

## 300-410 Dumps

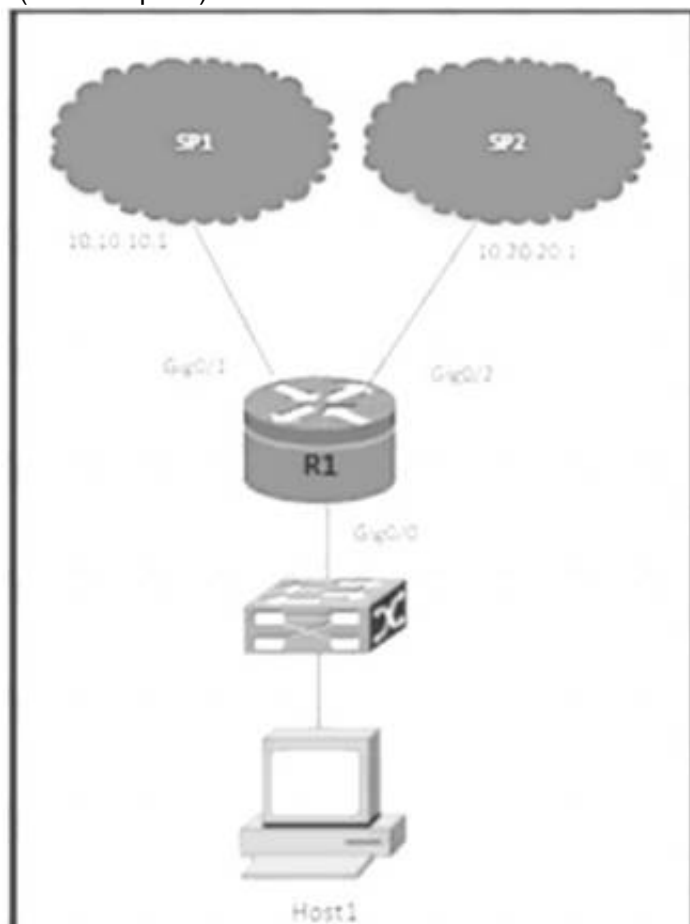
# Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

<https://www.certleader.com/300-410-dumps.html>



**NEW QUESTION 1**

- (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)

```

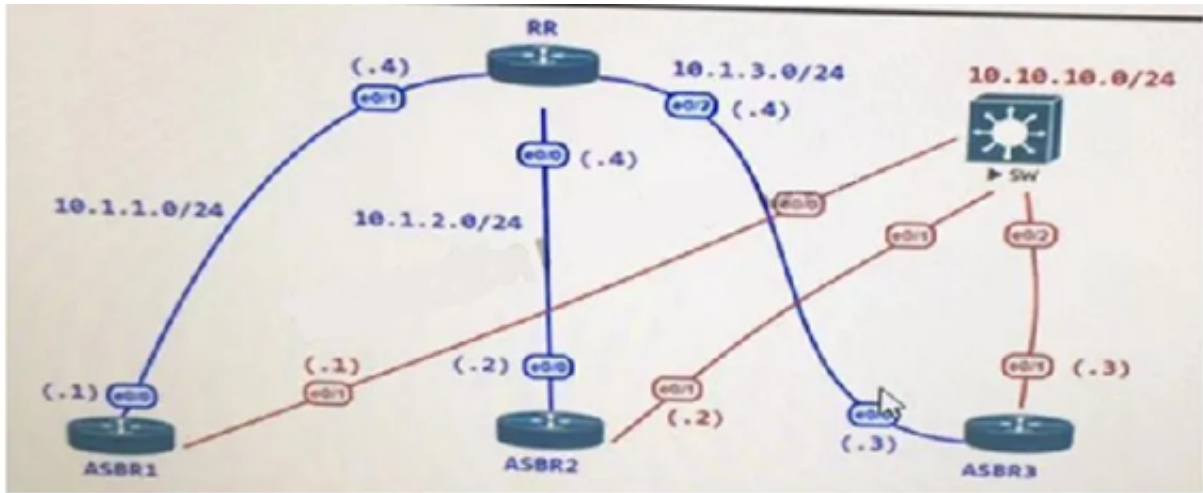
ip access-list extended match_SSH
 permit tcp any any eq 22
!
route-map PBR_SSH permit 10
 match ip address match_SSH
 set ip next-hop 10.20.20.1
!
interface Gig0/1
 ip policy route-map PBR_SSH
  
```

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

Answer: C

NEW QUESTION 2

- (Exam Topic 3)  
Refer to the exhibit.



```
RR
router bgp 100
neighbor 10.1.1.1 remote-as 100
neighbor 10.1.2.2 remote-as 100
neighbor 10.1.3.3 remote-as 100

ASBR2
router bgp 100
neighbor 10.1.1.4 remote-as 100

ASBR3
router bgp 100
neighbor 10.1.2.4 remote-as 100

ASBR4
router bgp 100
neighbor 10.1.3.4 remote-as 100
```

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 3

- (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 4**

- (Exam Topic 3)

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

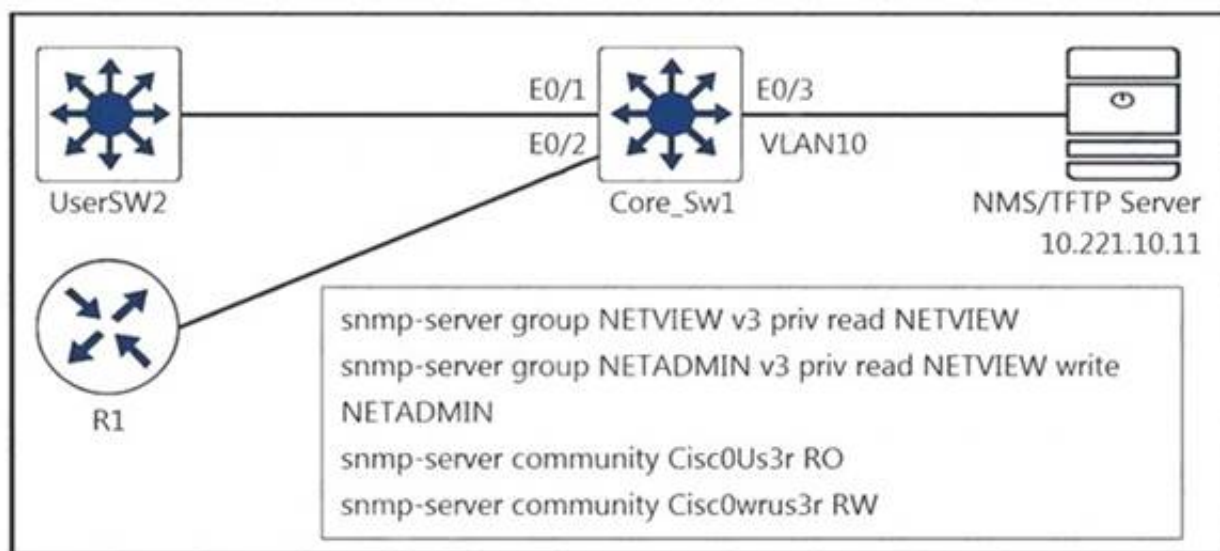
- A. Use pseudowire for Layer 2 routes
- B. Use MP-BGP for customer routes
- C. Use OSPF between PE and CE
- D. Use a unique RD per customer VRF
- E. Use LDP for customer routes

**Answer:** CD

**NEW QUESTION 5**

- (Exam Topic 3)

Refer to the exhibit.



A junior engineer configured SNMP to network devices. Malicious users have uploaded different configurations to the network devices using SNMP and TFTP servers.

Which configuration prevents changes from unauthorized NMS and TFTP servers?

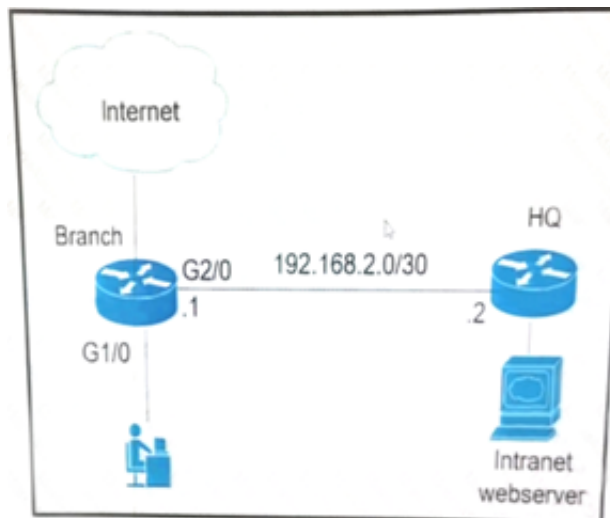
- A. access-list 20 permit 10.221.10.11 access-list 20 deny any log!snmp-server group NETVIEW v3 priv read NETVIEW access 20snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0Us3r RO 20snmp-server community Cisc0wrus3r RW 20snmp-server tftp-server-list 20
- B. access-list 20 permit 10.221.10.11 access-list 20 deny any log!snmp-server group NETVIEW v3 priv read NETVIEW access 20snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0wrus3r RO 20snmp-server community Cisc0Us3r RW 20 snmp-server tftp-server-list 20
- C. access-list 20 permit 10.221.10.11 access-list 20 deny any log
- D. access-list 20 permit 10.221.10.11

**Answer:** A

**NEW QUESTION 6**

- (Exam Topic 3)

Refer to the exhibit.



The branch router is configured with a default route toward the internet and has no routes configured for the HQ site that is connected through interface G2/0. The HQ router is fully configured and does not require changes. Which configuration on the branch router makes the intranet website (TCP port 80) available to the branch office users?



A)

```
access-list 100 permit tcp any host intranet-webserver-ip eq 80
|
route-map pbr permit 10
match ip address 100
set ip next-hop 192.168.2.2
|
interface G2/0
ip policy route-map pbr
```

B)

```
access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-webserver-ip
|
route-map pbr permit 10
match ip address 101 102
set ip next-hop 192.168.2.2
|
interface G1/0
ip policy route-map pbr
```

C)

```
access-list 101 permit tcp any any eq 80
access-list 102 permit tcp any host intranet-webserver-ip
|
route-map pbr permit 10
match ip address 101
set ip next-hop 192.168.2.2
route-map pbr permit 20
match ip address 102
set ip next-hop 192.168.2.2
|
interface G2/0
ip policy route-map pbr
```

D)

```
access-list 100 permit tcp host intranet-webserver-ip eq 80 any
|
route-map pbr permit 10
match ip address 100
set ip next-hop 192.168.2.2
|
interface G1/0
ip policy route-map pbr
```

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

**Answer:** B**Explanation:**

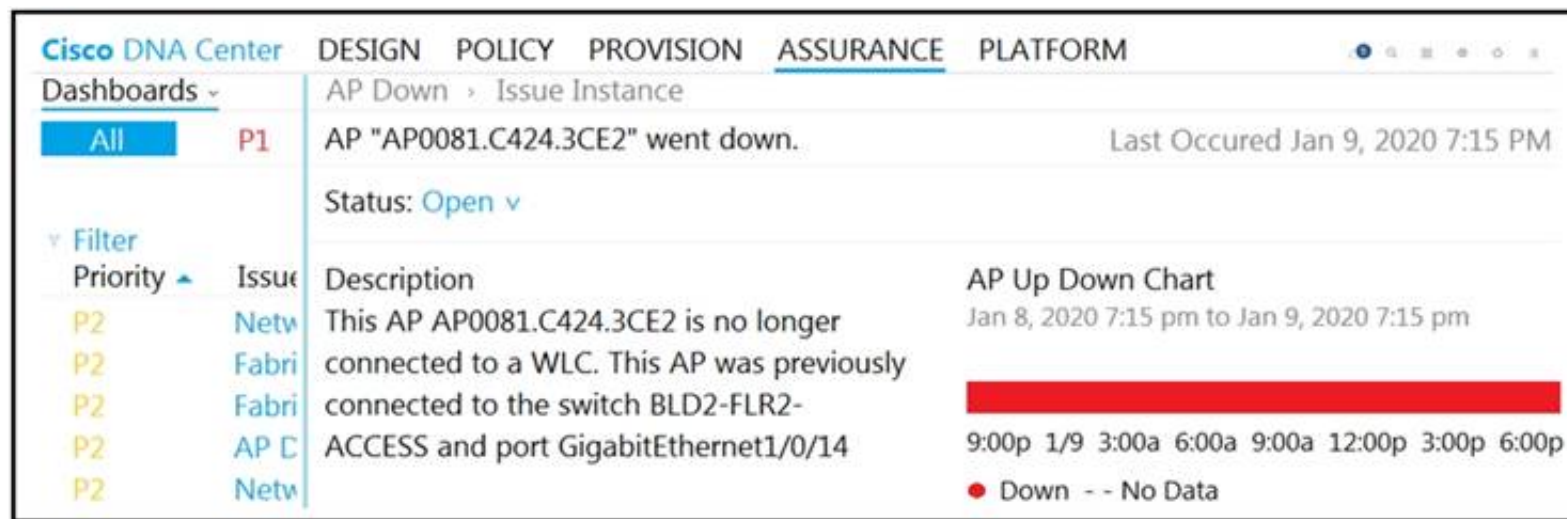
the ACL 101 matches all HTTP packets while the ACL 102 matches TCP packets destined to Intranet webserver. These packets will be sent to HQ router.

If a match command refers to several objects in one command, either of them should match (the logical OR algorithm is applied). For example, in the match ip address 101 102 command, a route is permitted if it is permitted by access list 101 or access list 102.

**NEW QUESTION 7**

- (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.

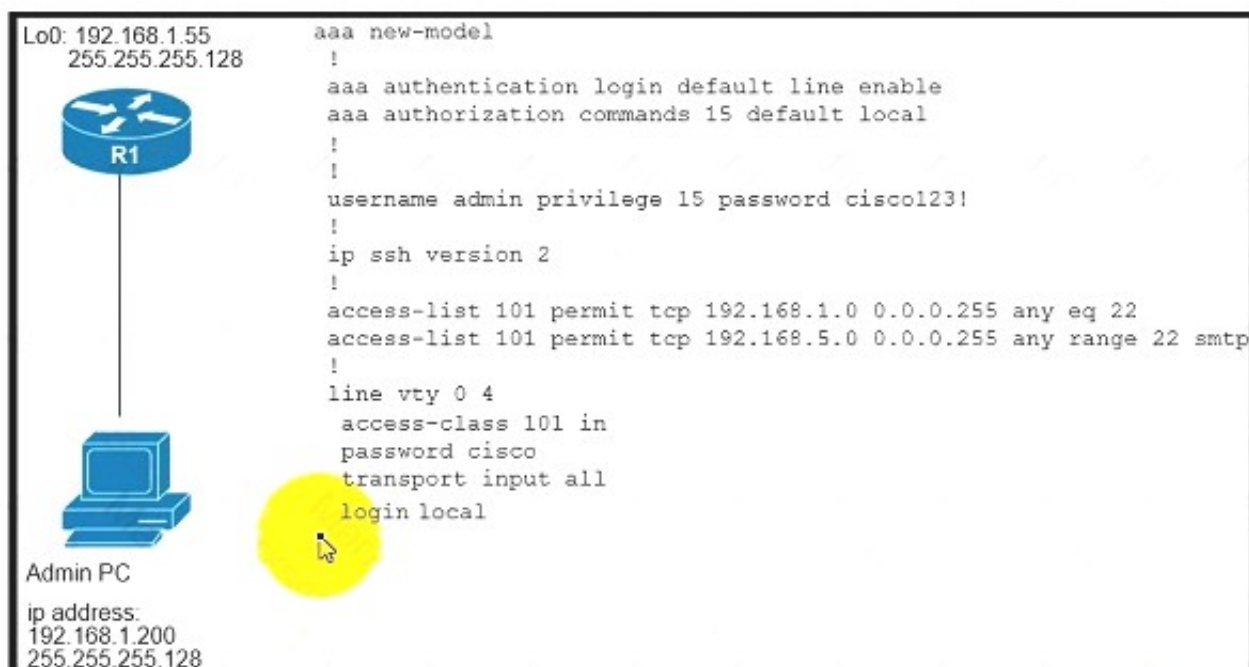
Wait 10 seconds and then issue the command to show the cable diagnostics result:

```
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 8**

- (Exam Topic 3)



Refer to the exhibit. An engineer configured user login based on authentication database on the router, but no one can log into the router. Which configuration resolves the issue?

- A. aaa authentication login default enable
- B. aaa authorization network default local
- C. aaa authentication login default local
- D. aaa authorization exec default local

**Answer:** C

#### NEW QUESTION 9

- (Exam Topic 3)

What is a characteristic of IPv6 RA Guard?

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

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 3)

An engineer configured a router with this configuration

```
ip access-hst DENY TELNET
```

```
10 deny tcp any any eq 23 log-input
```

The router console starts receiving log message :%SEC-6-IPACCESSLOGP: list DENY\_TELNET denied tcp 192.168.1.10(1022)(FastEthernet1/0 D508.89gb.003f) ->192.168.2.20(23), 1 packet"

Which action stops messages on the console while still denying Telnet?

- A. Configure a 20 permit ip any any command
- B. Remove log-Input keyword from the access list.
- C. Replace log-input keyword with the log keyword in the access list.
- D. Configure a 20 permit ip any any log-input command.

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

**Answer:** A

#### NEW QUESTION 14

- (Exam Topic 3)

The summary route is not shown in the RouterB routing table after this below configuration on Router\_A

```
interface ethernet 0
description location ID:S4289T9E09F39
ip address 192.168.3.1 255.255.255.0
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
```

Which Router\_A configuration resolves the issue by advertising the summary route to Router B?



- ☐ interface loopback 0  
ip address 172.16.96.1 255.255.255.0  
interface Ethernet 0  
ip address 192.168.3.1 255.255.255.0  
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
- ☐ interface loopback 0  
ip address 172.16.81.1 255.255.255.0  
interface Ethernet 0  
ip address 192.168.3.1 255.255.255.0  
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
- ☐ interface loopback 0  
ip address 172.16.79.1 255.255.255.0  
interface Ethernet 0  
ip address 192.168.3.1 255.255.255.0  
ip summary-address eigrp 1 172.16.80.0 255.255.240.0
- ☐ interface loopback 0  
ip address 172.18.81.1 255.255.255.0  
interface Ethernet 0  
ip address 192.168.3.1 255.255.255.0  
ip summary-address eigrp 1 172.16.80.0 255.255.240.0

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

**Answer:** B

#### NEW QUESTION 15

- (Exam Topic 3)

A newly Installed router starts establishing an LDP session from another MPLS router to which it is not directly connected. Which LDP message type responds by target router to the Initiating router using UDP protocol?

- A. notification message  
B. session message  
C. extended discovery message  
D. advertisement message

**Answer:** C

#### NEW QUESTION 19

- (Exam Topic 3)

The network administrator configured CoPP so that all HTTP and HTTPS traffic from the administrator device located at 172.16.1.99 toward the router CPU is limited to 500 kbps. Any traffic that exceeds this limit must be dropped.

```
access-list 100 permit ip host 172.16.1.99 any
!
class-map CM-ADMIN match access-group 100
!
policy-map PM-COPP class CM-ADMIN
police 500000 conform-action transmit
!
interface E0/0
service-policy input PM-COPP
```

CoPP failed to capture the desired traffic and the CPU load is getting higher. Which two configurations resolve the issue? (Choose two.)

- A. interface E0/0no service-policy input PM-COPP!control-planeservice-policy input PM-COPP  
B. policy-map PM-COPP class CM-ADMINno police 500000 conform-action transmit police 500 conform-action transmit!control-planeservice-policy input PM-COPP  
C. no access-list 100access-list 100 permit tcp host 172.16.1.99 any eq 80  
D. no access-list 100access-list 100 permit tcp host 172.16.1.99 any eq 80access-list 100 permit tcp host 172.16.1.99 any eq 443  
E. policy-map PM-COPP class CM-ADMINno police 500000 conform-action transmit police 500 conform-action transmit

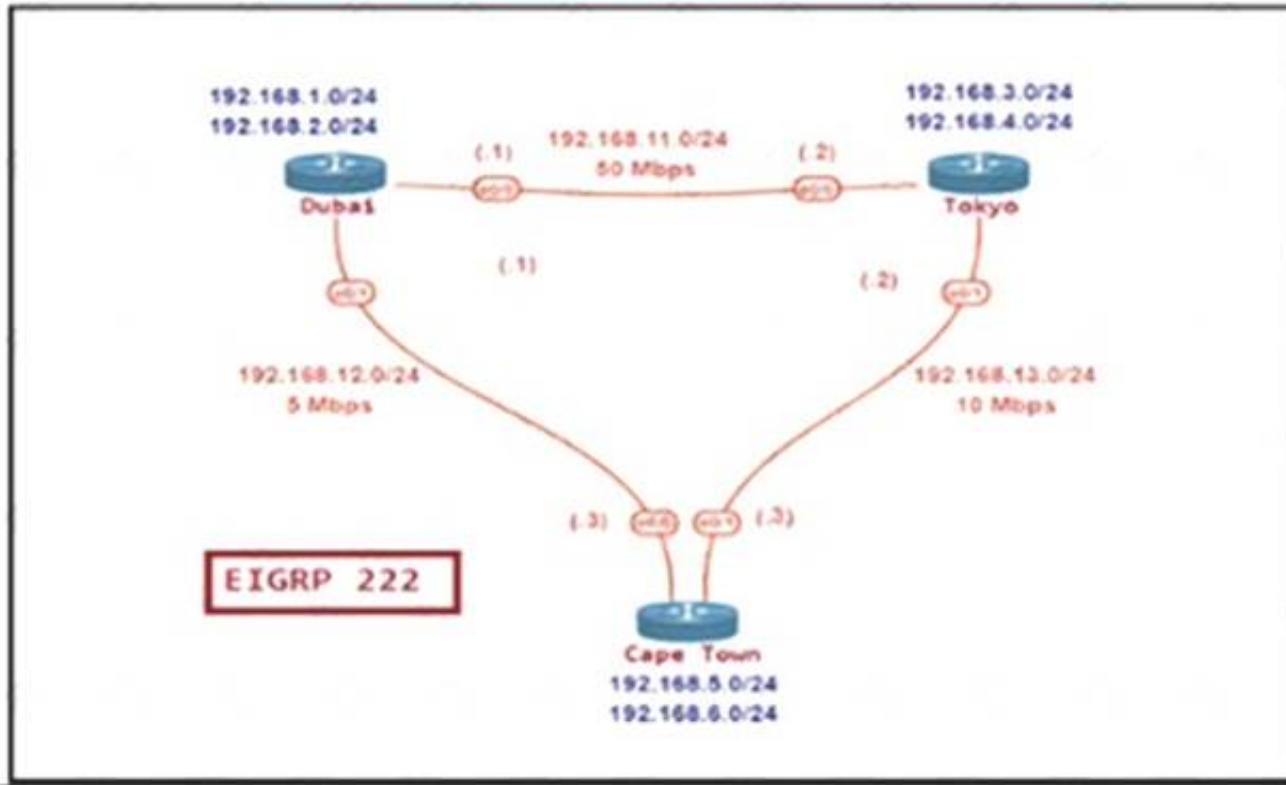
**Answer:** A

#### NEW QUESTION 24

- (Exam Topic 3)

Refer to the exhibit.





```

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

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

A)

Dubai

```

router eigrp 100
 variance 2
    
```

B)

CapeTown

```

router eigrp 100
 variance 2
    
```

C)

CapeTown

```

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

D)

**Cape Town**

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

**Dubai**

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

**Tokyo**

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

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

**Answer:** D

**NEW QUESTION 27**

- (Exam Topic 3)

Refer to the exhibit.

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

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

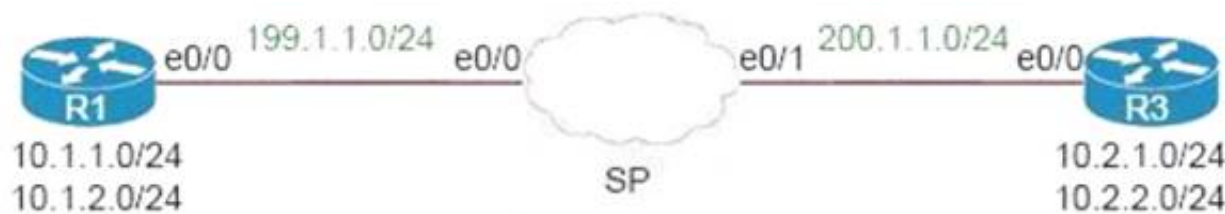
- A. access-class INTERNET in
- B. ip access-group INTERNET in
- C. ipv6 traffic-filter INTERNET in
- D. ipv6 access-class INTERNET in

**Answer:** D

**NEW QUESTION 30**

- (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 3deshash sha group 2!crypto isakmp key cisco123 address 200.1.1.3
- B. crypto isakmp policy 5 authentication pre-share encryption 3deshash md5 group 2!crypto isakmp key cisco123 address 200.1.1.3
- C. crypto isakmp policy 5 authentication pre-share encryption 3deshash md5 group 2!crypto isakmp key cisco123 address 199.1.1.1
- D. crypto isakmp policy 5 authentication pre-share encryption 3deshash 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 34**

- (Exam Topic 3)

What are the two goals of micro BFD sessions? (Choose two.)

- A. The high bandwidth member link of a link aggregation group must run BFD
- B. Run the BFD session with 3x3 ms hello timer
- C. Continuity for each member link of a link aggregation group must be verified
- D. Eny member link on a link aggregation group must run BFD
- E. Each member link of a link aggregation group must run BFD.

**Answer:** CE

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bfd/configuration/xe-16-8/irb-xe-16-8-book/irb-micr](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-16-8/irb-xe-16-8-book/irb-micr)

**NEW QUESTION 38**

- (Exam Topic 3)

Refer to the exhibit.

```
R2(config)# int tun0

*Feb 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

*Feb 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

*Feb 23 00:43:05.730: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.12.1 (Tunnel0) is up: new adjacency
*Feb 23 00:43:05.993: %ADJ-5-PARENT: Midchain parent maintenance
for IP midchain out of Tunnel0 - looped chain attempting to
stack
*Feb 23 00:43:15.193: %TUN-5-RECURDOWN: Tunnel0 temporarily
disabled due to recursive routing
*Feb 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. Stop sending a route matching the tunnel destination across the tunnel.
- B. Modify the network command to use the Tunne10 Interface netmask.
- C. Advertise the Loopback0 interface from R2 across the tunnel.
- D. Readdress the IP network on the Tunne10 on both routers using the /31 netmask.

**Answer:** A

**NEW QUESTION 42**

- (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 46**

- (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  0x00275C
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  0x001CBC
0

*Feb 22 22:50:39.523: %OSPF-4-FLOOD_WAR: 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 48

- (Exam Topic 3)

Which router attaches the VPN label to incoming packets from CE routing?

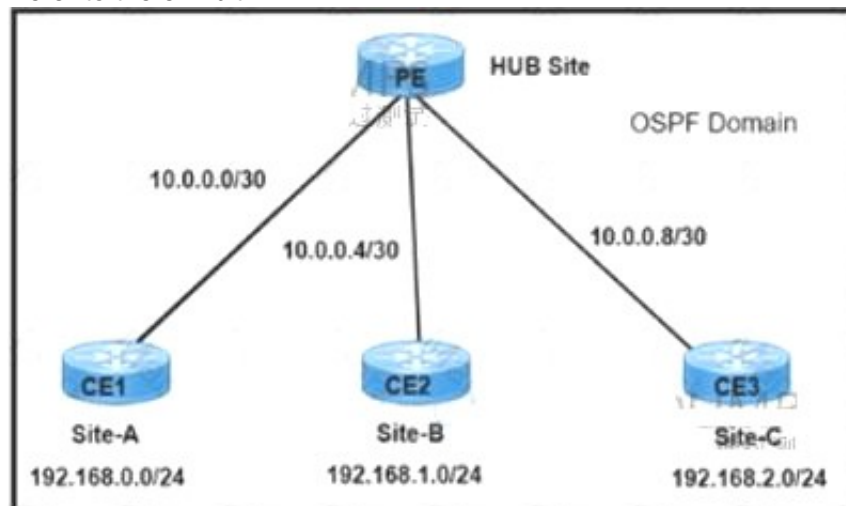
- A. CE router
- B. core router
- C. P router
- D. PE router

**Answer: D**

#### NEW QUESTION 50

- (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 52

- (Exam Topic 3)

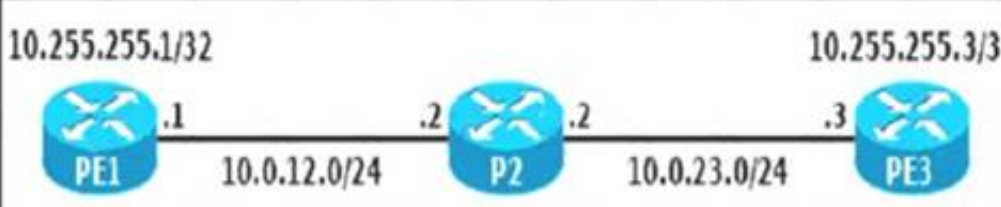
What is considered the primary advantage of running BFD?

- A. reduction in time needed to detect Layer 2 switched neighbor failures  
B. reduction in time needed to detect Layer 3 routing neighbor failures  
C. reduction in CPU needed to detect Layer 2 switch neighbor failures  
D. reduction in CPU needed to detect Layer 3 routing neighbor failures

**Answer: B**

#### NEW QUESTION 57

- (Exam Topic 3)



```

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

1/1/1 ms

```

PE1# debug ip tcp transactions
PE1# debug ip icmp

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

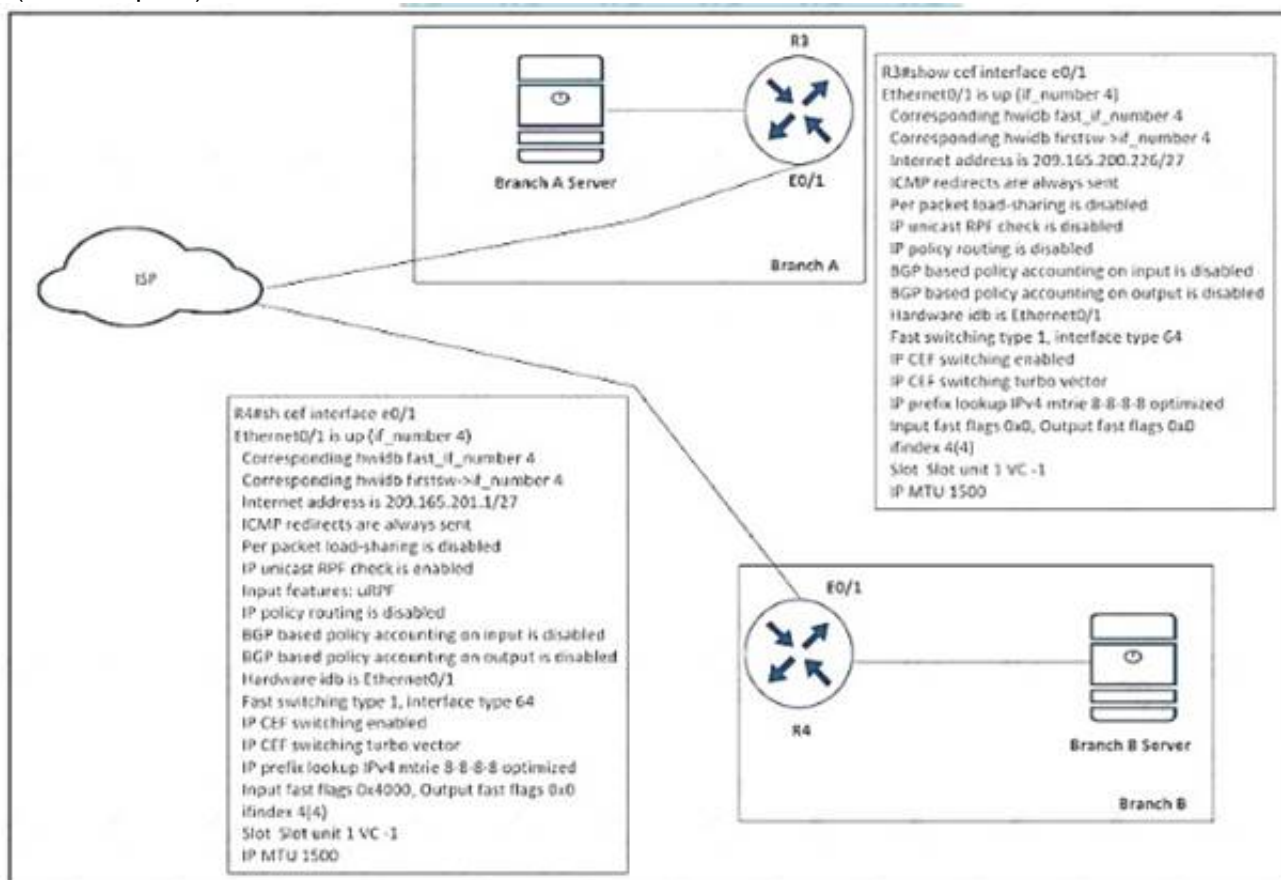
Refer to the exhibit. The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish Which action resolves the issue?

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

Answer: C

### NEW QUESTION 59

- (Exam Topic 3)



Refer to the exhibit.

A shoe retail company implemented the uRPF solution for an antispoofing attack. A network engineer received the call that the branch A server is under an IP spoofing attack. Which configuration must be implemented to resolve the attack?

A)

**R4**  
**interface ethernet0/1**  
**ip unicast RPF check reachable-via any allow-default allow-self-ping**

B)

**R4**  
**interface ethernet0/1**  
**ip verify unicast source reachable-via any allow-default allow-self-ping**

C)

**R3**  
**interface ethernet0/1**  
**ip verify unicast source reachable-via any allow-default allow-self-ping**

D)

**R3**  
**interface ethernet0/1**  
**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: C

### NEW QUESTION 63

- (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

```

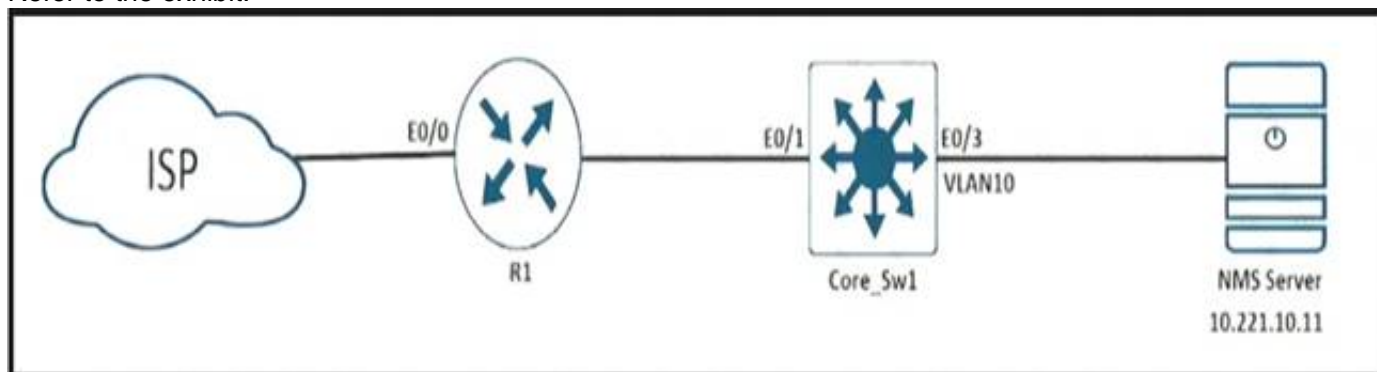
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 65

- (Exam Topic 3)

Refer to the exhibit.



During ISP router maintenance, the network produced many alerts because of the flapping interface. Which configuration on R1 resolves the issue?

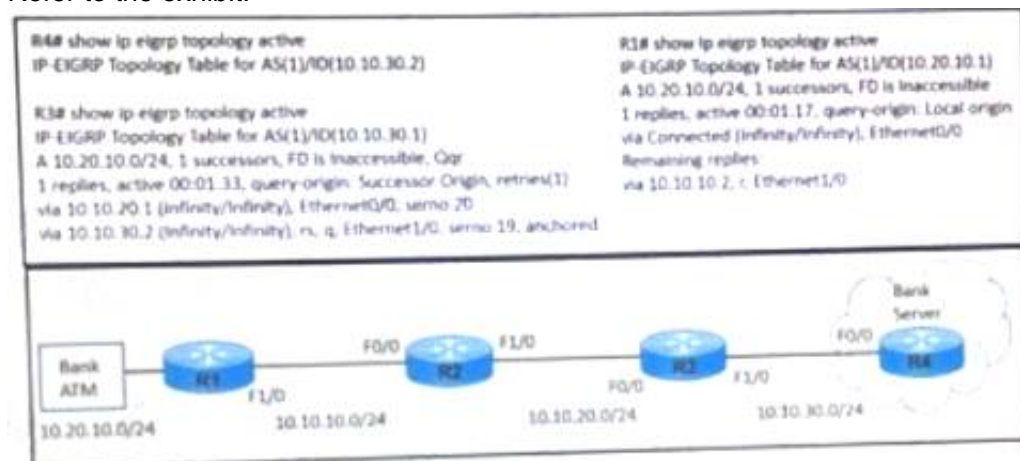
- A. no snmp trap link-status
- B. snmp trap link-status down
- C. snmp trap ip verify drop-rate
- D. ip verify drop-rate notify hold-down 60

**Answer: D**

#### NEW QUESTION 68

- (Exam Topic 3)

Refer to the exhibit.



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

- A. Advertise 10.10.30.0/24 subnet in R1 EIGRP AS.
- B. EIGRP peering between R3 and R4 to be fixed.
- C. EIGRP peering between R1 and R2 to be fixed.
- D. Advertise 10.10.30.0/24 subnet in R3 EIGRP AS.

**Answer: D**

#### NEW QUESTION 73

- (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 74

- (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 78

- (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 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 172.20.1.2 255.255.255.0R2(config-if)# ip mtu 1400 R2(config-if)# ip tcp adjust-mss 1360R2(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 10.10.2.2 R2(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 85

- (Exam Topic 3)

```
*Sep 3 23:18:21.264: EIGRP: Neighbor (10.1.2.192) not yet found
*Sep 3 23:19:18.675: Going down: Peer 10.1.2.1 total=2 stub 0, iadb-stub=0 iid-all=0
*Sep 3 23:19:18.675: EIGRP: Handle deallocation failure [1]
*Sep 3 23:19:18.675: EIGRP: Neighbor 10.1.2.1 went down on Tunnel1.
*Sep 3 23:19:22.943: EIGRP: New peer 10.1.2.1.
*Sep 3 23:19:22.943: %DUAL-5-NBRCHANGE: EIGRP-IPv4 3111: Neighbor 10.1.2.1 (Tunnel1) is up: new adjacency
```

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**

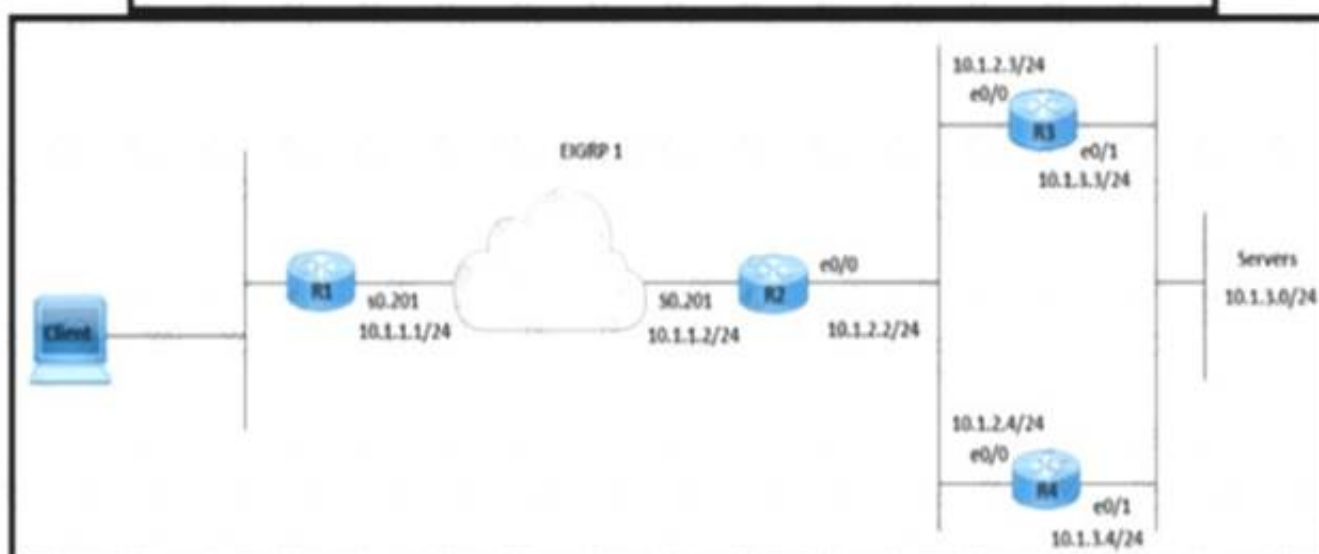
### NEW QUESTION 86

- (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 89

- (Exam Topic 3)

Refer to the exhibit.



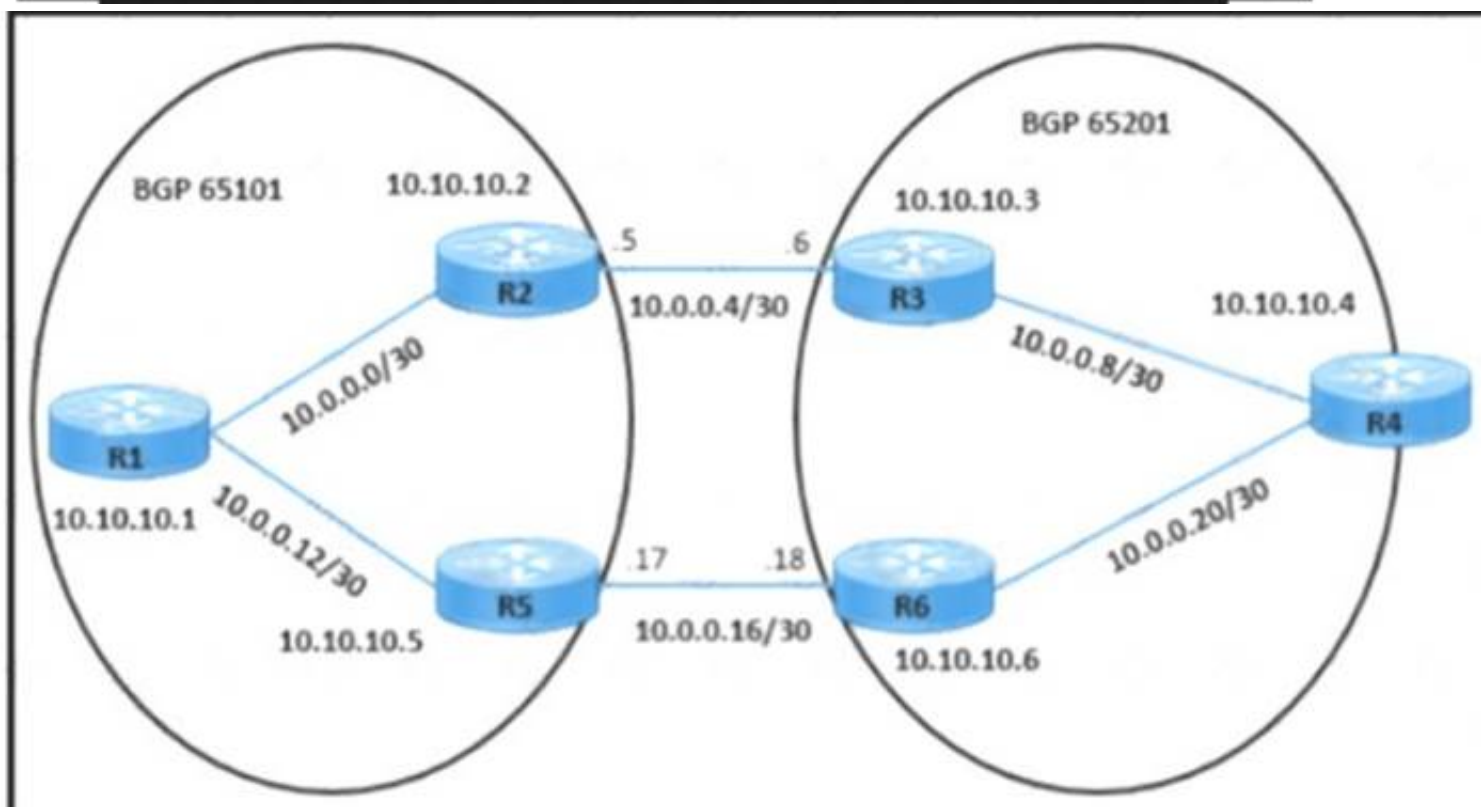
```

R3#
*Sep  5 07:29:34.031: %TCP-6-BADAUTH: No MD5 digest from 10.10.10.2(179) to
10.10.10.3(60942) (RST)
R2# show ip bgp neighbors 10.10.10.3
BGP neighbor is 10.10.10.3, remote AS 65201, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 00:02:19, last write 00:02:19, hold time is 180, keepalive interval is
60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

      Sent      Rcvd
Opens:          2         2
Notifications:  0         0
Updates:        5         6
Keepalives:     10        9
Route Refresh:  0         0
Total:         17        17

Default minimum time between advertisement runs is 30 seconds
Address tracking is enabled, the RIB does have a route to 10.10.10.3
Connections established 2; dropped 2
Last reset 00:11:58, due to Peer closed the session
External BGP neighbor not directly connected.
Transport(tcp) path-mtu-discovery is enabled
No active TCP connection

```



The network operation team observes a traffic forwarding issue between R2 and R3:

- Ping and traceroute of loopback IP address from R2 to R3 is successful.
- iBGP peering in AS 65101 and AS 65201 is up. Which configuration resolves the issue?

- A. Configure MD5 password authentication on R2.
- B. Advertise R2 and R3 loopback IPs in AS 65101 and AS 65201.
- C. Remove MD5 password authentication on R3.
- D. Set up eBGP multihop on R2 and R3 routers.

**Answer: D**

#### NEW QUESTION 90

- (Exam Topic 3)

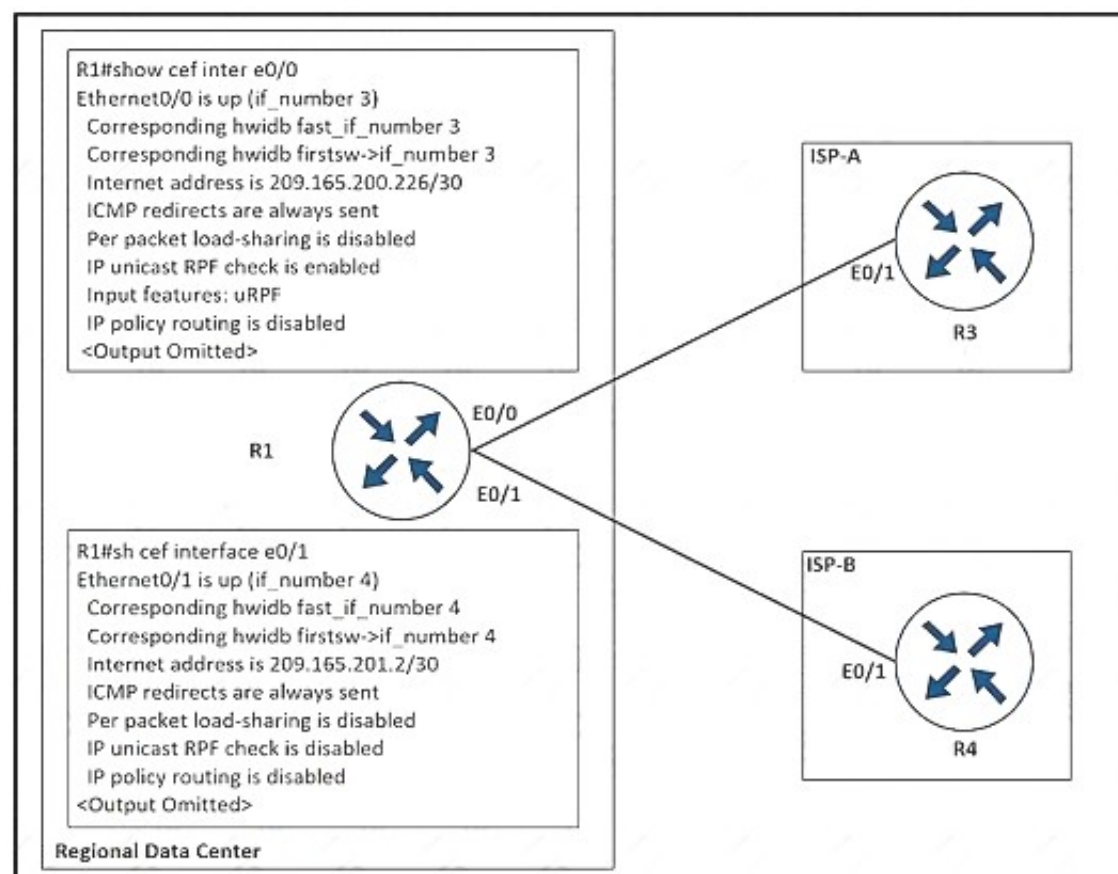
An engineer received a ticket about a router that has reloaded. The monitoring system graphs show different traffic patterns between logical and physical interfaces when the router is rebooted. Which action resolves the issue?

- A. Configure the snmp ifindex persist command globally.
- B. Clear the logical interfaces with snmp ifindex clear command
- C. Configure the snmp ifindex persist command on the physical interfaces.
- D. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs

**Answer: A**

#### NEW QUESTION 95

- (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?

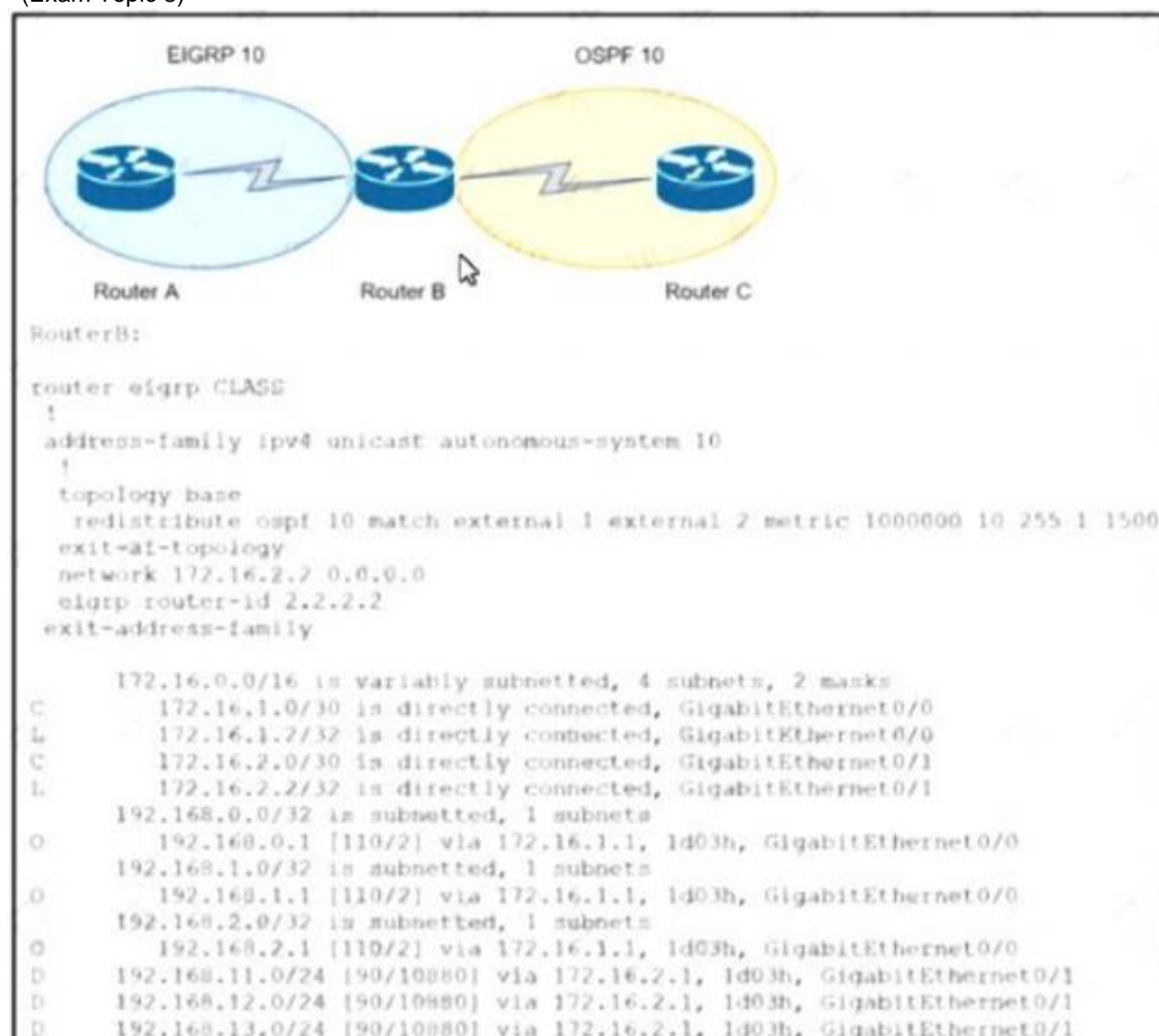
- ☐ interface ethernet0/0  
ip verify unicast reverse-path
- ☐ interface ethernet0/1  
ip verify unicast reverse-path
- ☒ interface ethernet0/1  
ip unicast RPF check reachable-via any allow-default allow-self-ping
- ☐ interface ethernet0/0  
ip unicast RPF check reachable-via any allow-default allow-self-ping

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

**Answer: B**

#### NEW QUESTION 99

- (Exam Topic 3)



Refer to the exhibit. An engineer configured route exchange between two different companies for a migration project EIGRP routes were learned in router C but no OSPF routes were learned in router A. Which configuration allows router A to receive OSPF routes?

- A. (config-router-af)#redistribute ospf 10 1000000 10 255 1 1500
- B. (config-router-af-topology)#redistribute ospf 10 metric 1000000 10 255 1 1500
- C. (config-router-af-topology)#redistribute connected
- D. (config-router-af-topology)#no redistribute ospf 10 match external 1 external 2 metric 1000000 10 255 1 1500

**Answer: B**

#### NEW QUESTION 103

- (Exam Topic 3)

Which two technologies optimize MPLS infrastructure using bandwidth protection services when experiencing slow response? (Choose two.)

- A. IPLFA
- B. MPLS OAM
- C. VPLS
- D. SO-MPLS
- E. Fast-Rwroute

**Answer: AE**

#### NEW QUESTION 104

- (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 108

- (Exam Topic 3)

What are two characteristics of a VRF instance? (Choose two)

- A. It is defined by the VPN membership of a customer site attached to a P device.



- B. Each VRF has a different set of routing and CEF tables.
- C. All VRFS share customers routing and CEF tables.
- D. An interface must be associated to one VRF
- E. A customer site can be associated to different VRFs.

**Answer:** BD

#### NEW QUESTION 111

- (Exam Topic 3)

Which method provides failure detection in BFD?

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

**Answer:** B

#### NEW QUESTION 113

- (Exam Topic 3)

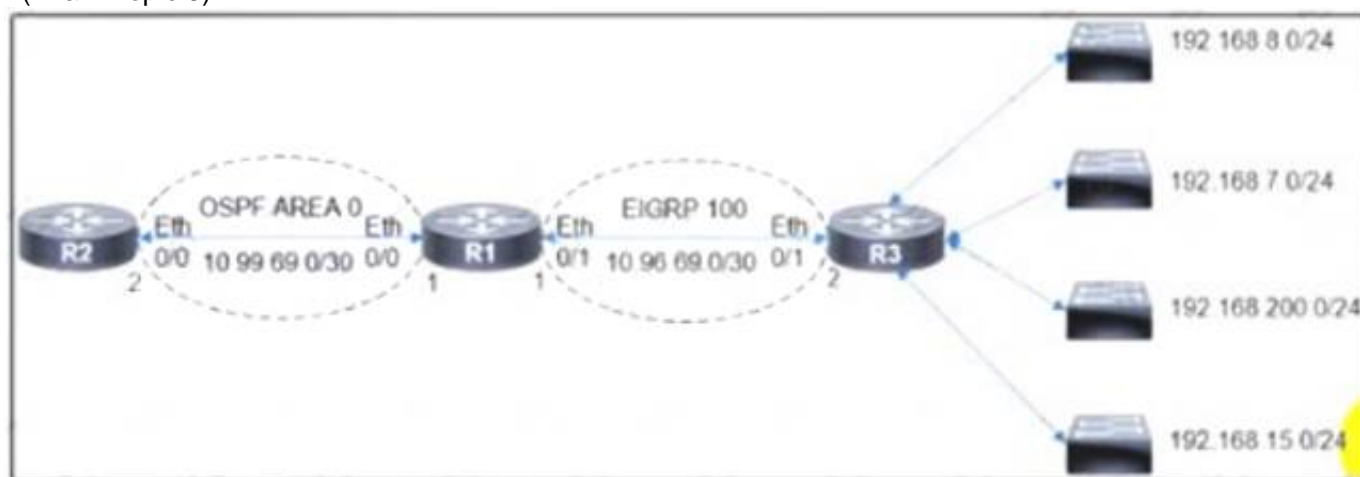
Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?

- A. RA Throttling
- B. Source or Destination Guard
- C. ND Multicast Suppression
- D. IPv6 Snooping

**Answer:** D

#### NEW QUESTION 115

- (Exam Topic 3)



```
R1#show route-map
route-map FROM->EIGRP, permit, sequence 10
  Match clauses:
    ip address (access-lists): 10
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
R1#show run | sec router
router eigrp 100
 network 10.96.69.0 0.0.0.3
 no auto-summary
 eigrp router-id 1.1.1.1
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute eigrp 100 subnets route-map FROM->EIGRP
 network 10.99.69.0 0.0.0.3 area 0
R1#show ip access-list
Standard IP access list 10
 10 permit 192.168.16.0, wildcard bits 0.0.3.255
 11 permit 192.168.0.0, wildcard bits 0.0.7.255
 20 deny any
```

Refer to the exhibit The engineer configured route redistribution in the network but soon received reports that R2 cannot access 192.168.7.0/24 and 192.168.15.0/24 subnets Which configuration resolves the issue?

- ☒ R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.3.255  
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.3.255
- ☐ R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.7.255  
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.3.255
- ☐ R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.0.0 0.0.3.255  
R1(config-std-nacl)#11 permit 192.168.8.0 0.0.7.255
- ☒ R1(config)#ip access-list standard 10  
R1(config-std-nacl)#no 10 permit  
R1(config-std-nacl)#no 11 permit  
R1(config-std-nacl)#10 permit 192.168.4.0 0.0.3.255  
R1(config-std-nacl)#11 permit 192.168.12.0 0.0.3.255

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

**Answer: D**

#### NEW QUESTION 119

- (Exam Topic 3)

What must be configured by the network engineer to circumvent AS\_PATH prevention mechanism in IP/VPN Hub and Spoke deployment scenarios?

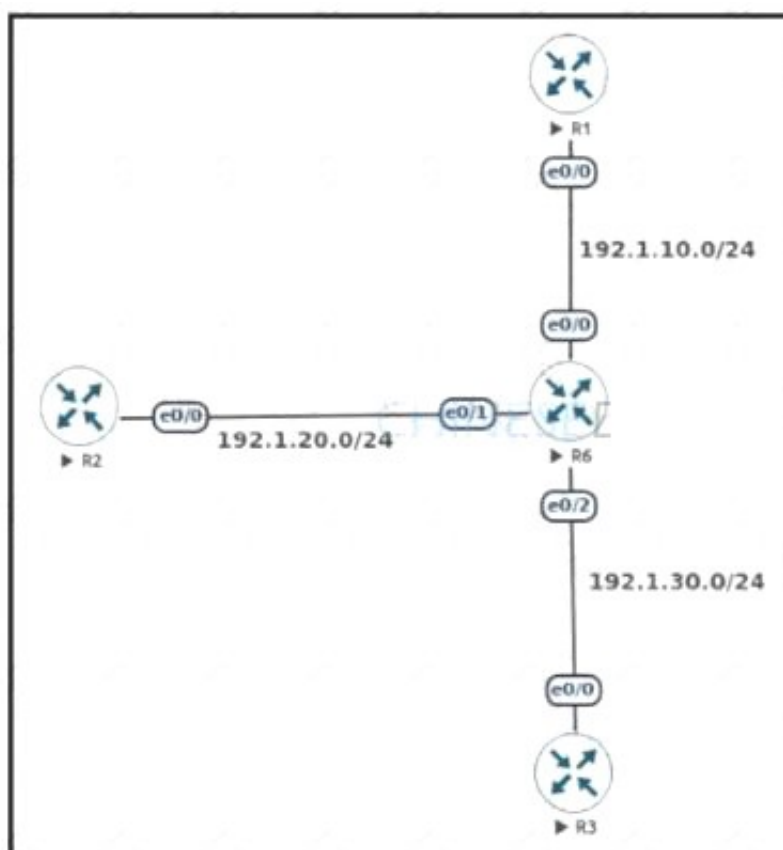
- A. Use allows in and as-override at all Pes.  
B. Use allows in and as-override at the PE-Hub.  
C. Use Allowas-in the PE\_Hub  
D. Use as-override at the PE\_Hub

**Answer: D**

#### NEW QUESTION 121

- (Exam Topic 3)

Refer to the exhibit.



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

Interface Tunnel1  
ip address 192.168.1.1 255.255.255.0  
tunnel source e 0/0  
tunnel mode gre multipoint  
ip nhrp network-id 1

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

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

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

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

**Answer:** B

#### NEW QUESTION 125

- (Exam Topic 3)

Users report issues with reachability between areas as soon as an engineer configured summary routes between areas in a multiple area OSPF autonomous system. Which action resolves the issue?

- A. Configure the summary-address command on the ASBR.
- B. Configure the summary-address command on the ABR.
- C. Configure the area range command on the ABR.
- D. Configure the area range command on the ASBR.

**Answer:** C

#### Explanation:

For OSPF, we can only summary at the ABR with the command "area range" or at the ASBR with the command "summary-address" -> Therefore answer A and answer B are not correct.

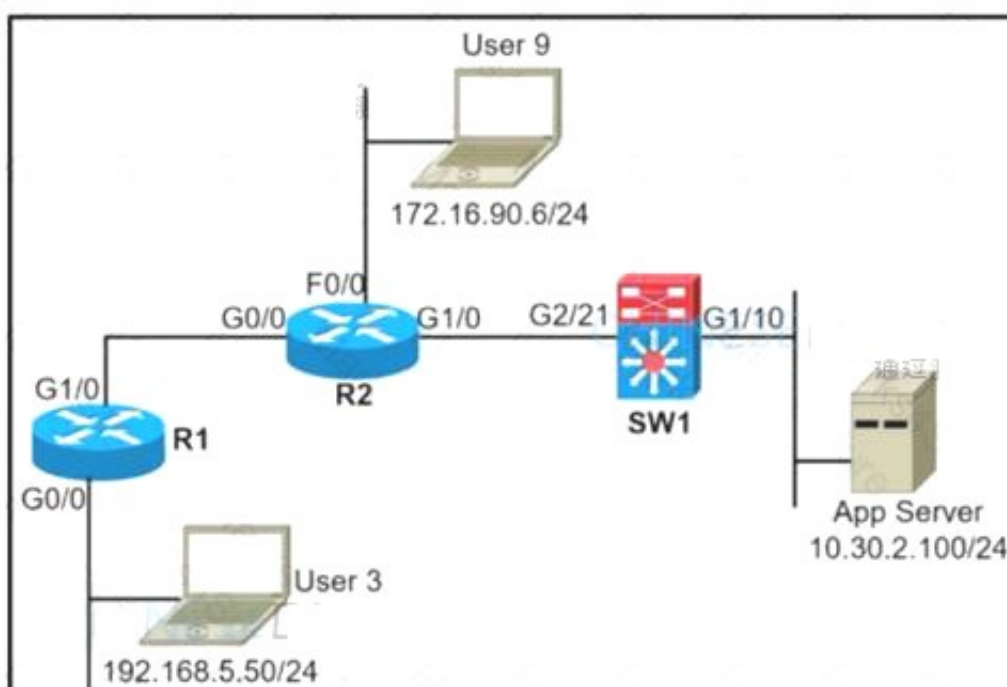
In this question, the most likely problem is that when doing summarization, the network mask is configured wrong and summarization doesn't work because of the misconfiguration. When configuring the area range command, make sure that the summarization mask is in the form of a prefix mask rather than a wildcard mask (that is, 255.255.255.0 instead of 0.0.0.255).

Good reference: <https://www.configrouter.com/troubleshooting-route-summarization-ospf-14082/>

#### NEW QUESTION 130

- (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?



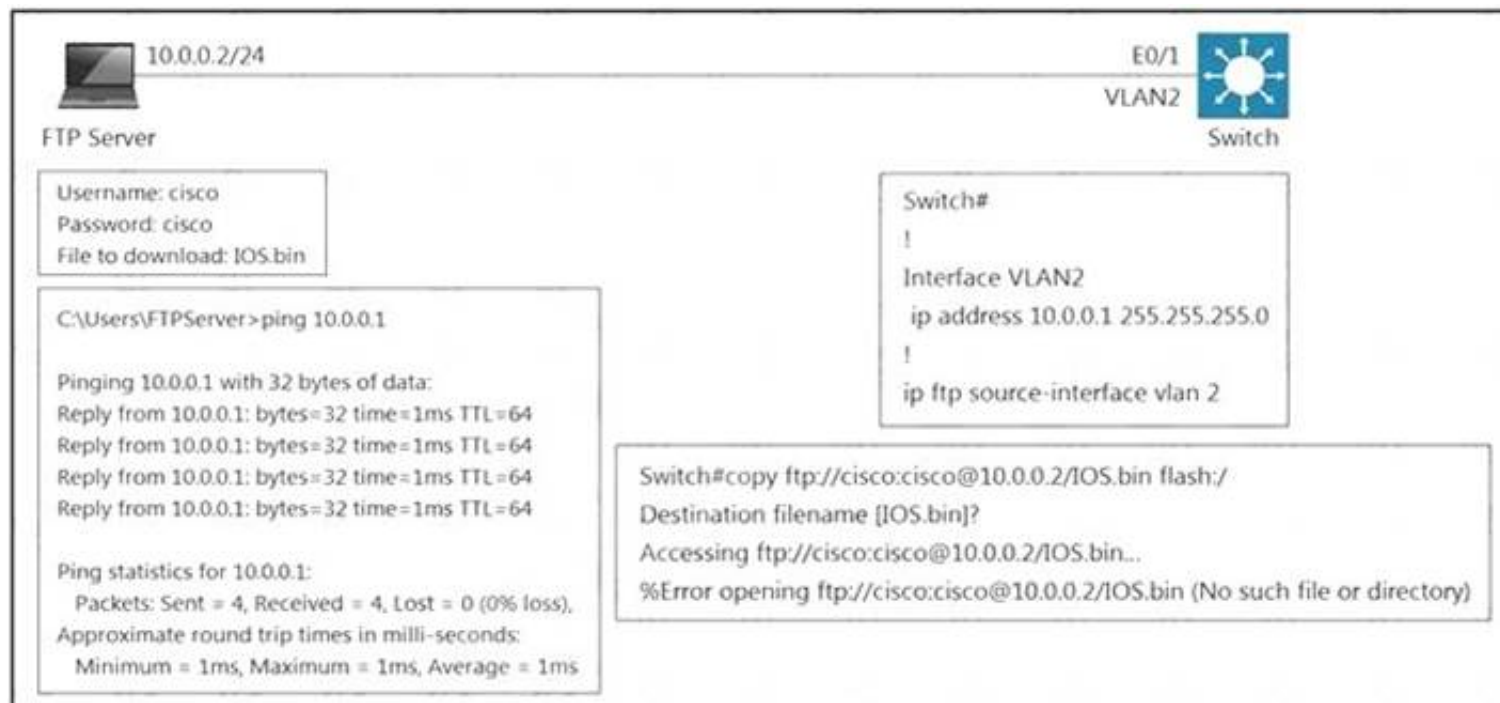
- A. R2 interface G1/0
- B. R2 interface G0/0
- C. SW1 interface G1/10
- D. SW1 interface G2/21

**Answer: D**

#### NEW QUESTION 135

- (Exam Topic 3)

Refer to the exhibit.



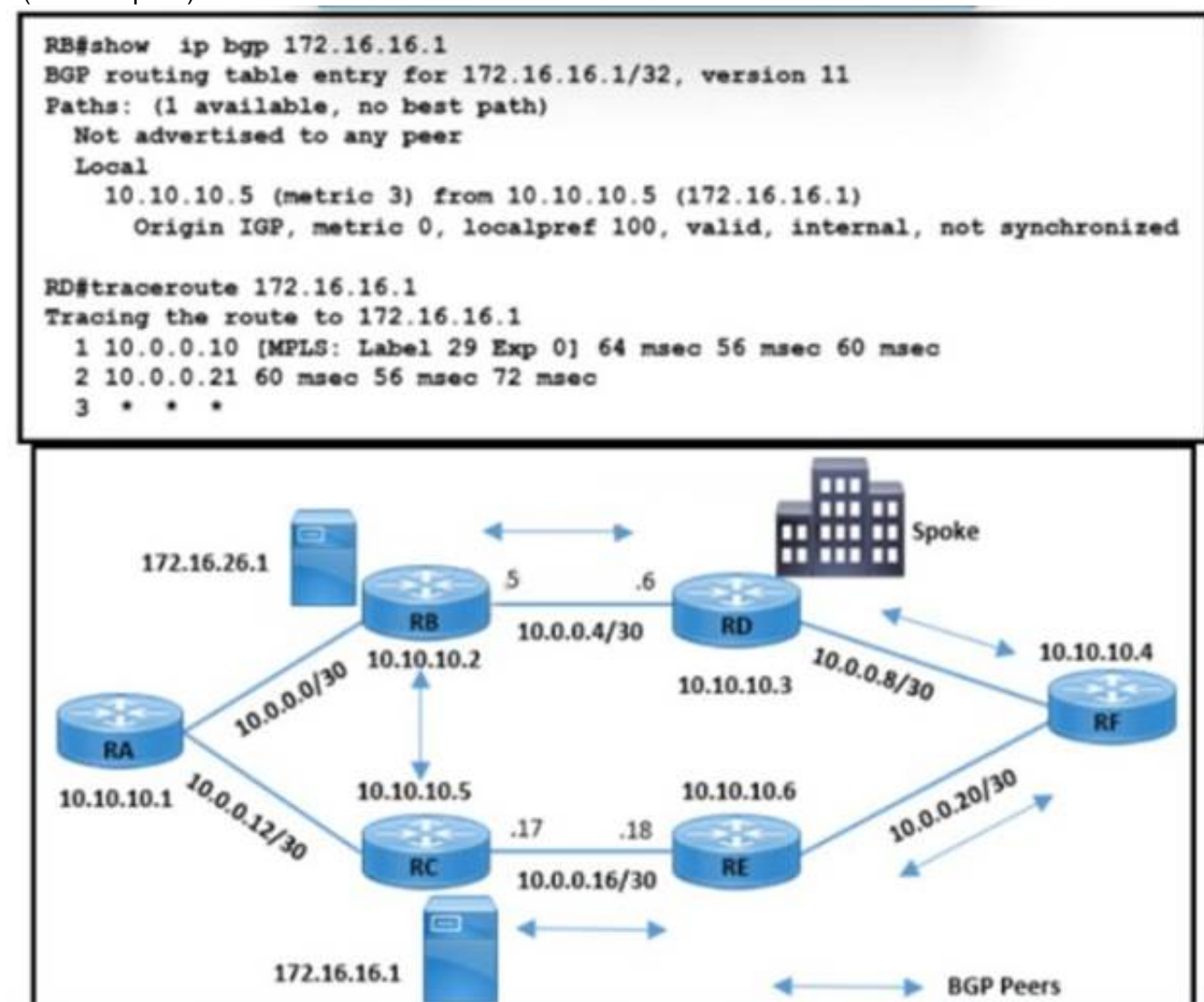
An engineer cannot copy the IOS.bin file from the FTP server to the switch.  
Which action resolves the issue?

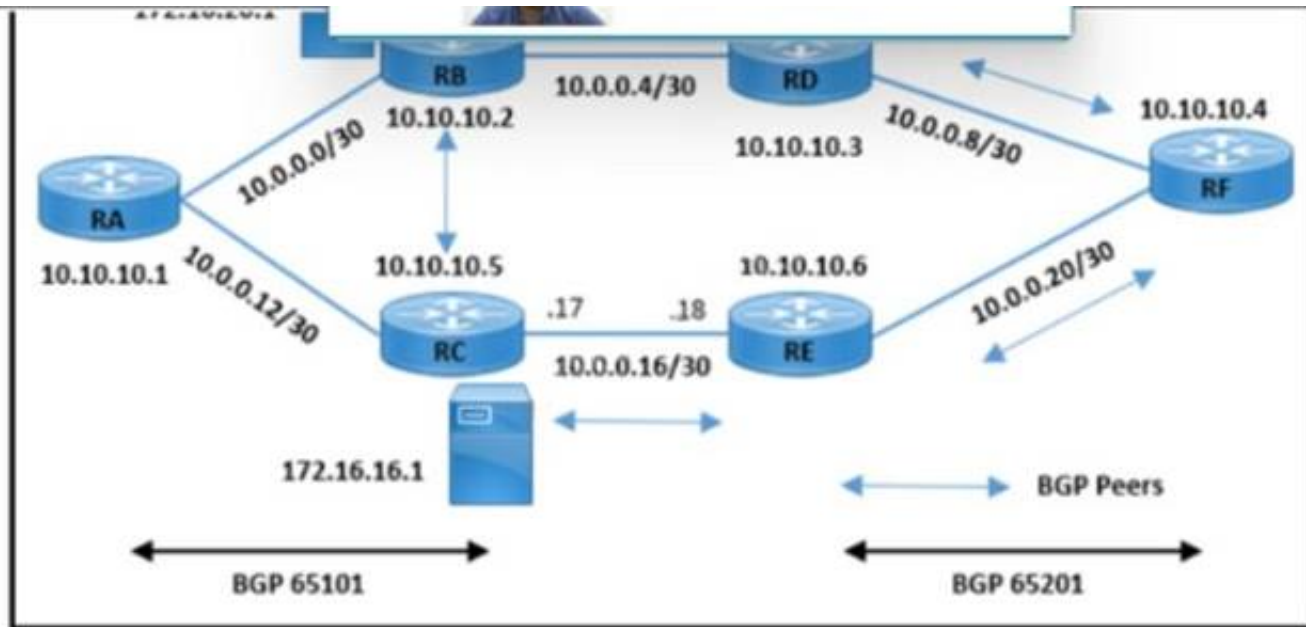
- A. Allow file permissions to download the file from the FTP server.
- B. Add the IOS.bin file, which does not exist on FTP server.
- C. Make memory space on the switch flash or USB drive to download the file.
- D. Use the copy flash:/ ftp://cisco@10.0.0.2/IOS.bin command.

**Answer: B**

#### NEW QUESTION 137

- (Exam Topic 3)





Refer to the exhibit A customer reported an issue with a fiber link failure between RC and RE Users connected through the spoke location face disconnection and packet drops with the primary email server (172.16.16.1) but have no issues with the backup email server (172.16.26.1). All the router loopback IPs are advertised through the OSPF protocol. Which configuration resolves the issue?

- ☐ RB(config)#router bgp 65101  
RB(config-router)#no synchronization
- ☐ RC(config)#router bgp 65101  
RC(config-router)#neighbor 10.10.10.2 next-hop-self
- ☐ RB(config)#router bgp 65101  
RB(config-router)#neighbor 10.10.10.5 next-hop-self
- ☐ RC(config)#router bgp 65101  
RC(config-router)#no synchronization

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

**Answer: B**

#### NEW QUESTION 138

- (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

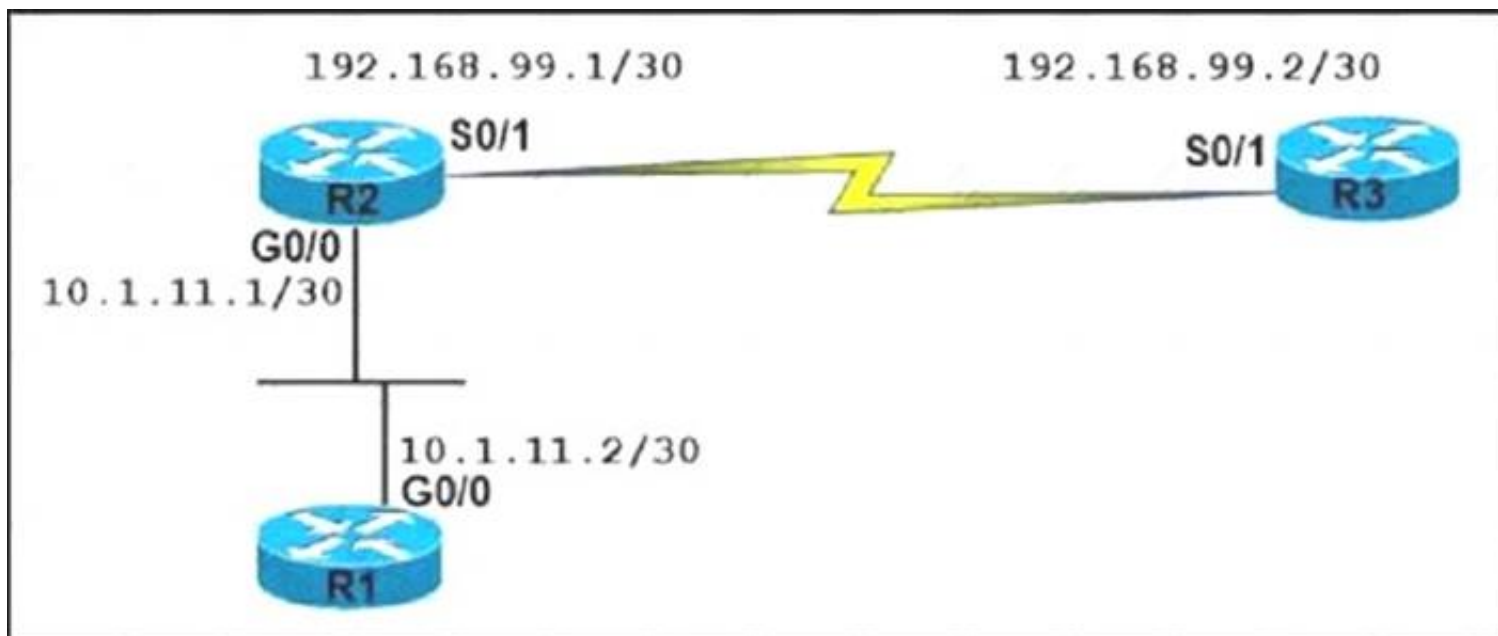
#### NEW QUESTION 139

- (Exam Topic 3)

Refer to the exhibit.

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

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



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

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

**Answer: B**

**Explanation:**

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

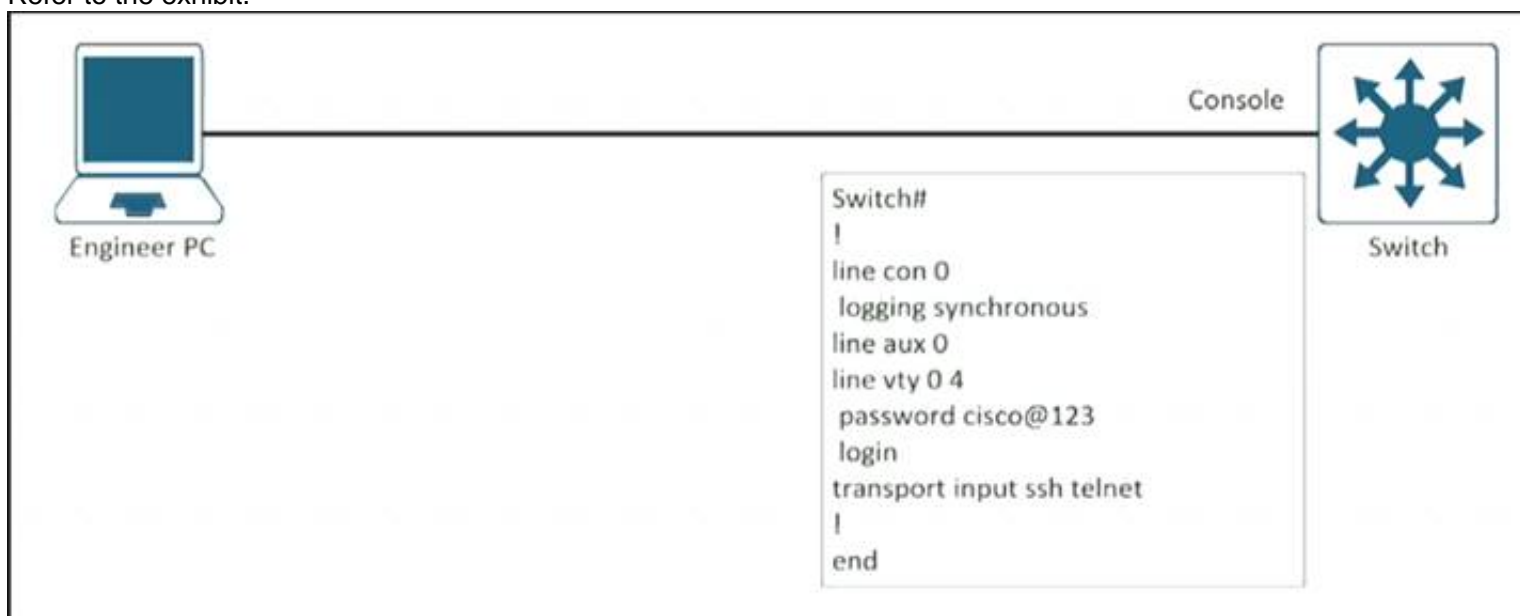
Neighbors Stuck in Exstart/Exchange State

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

**NEW QUESTION 144**

- (Exam Topic 3)

Refer to the exhibit.



An engineer must block access to the console ports for all corporate remote Cisco devices based on the recent corporate security policy but the security team still can connect through the console port. Which configuration on the console port resolves the issue?

- A. transport input telnet
- B. login and password
- C. no exec
- D. exec 0.0

**Answer: C**

**Explanation:**

"no exec" will disable access to a line. It is used if we want to allow only outgoing session (and disable incoming session) so this command will block all console port access.

There is no "exec 0 0" command. We can only find the "exec prompt" command in IOS Version 15.4(2)T4.



```
Router(config-line)#exec ?
prompt EXEC prompt
<cr>

Router(config-line)#exec pro
Router(config-line)#exec prompt ?
timestamp Print timestamps for show commands

Router(config-line)#exec prompt █
```

The most similar command is “exec-timeout 0 0” command, which is used to prevent Telnet/SSH sessions from timing out.

**NEW QUESTION 145**

- (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 150**

- (Exam Topic 3)

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

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

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

- A. control-planeno service-policy input PM-CoPP!interface Ethernet 0/0service-policy input PM-CoPP
- B. control-planeno service-policy input PM-CoPPservice-policy input PM-CoPP
- C. no access-list 101access-list 101 deny tcp host 10,1,1.1 any eq 23access-list 101 deny tcp host 172,16.1.1 any eq 23 access-list 101 permit ip any any
- D. no access-list 101access-list 101 deny tcp host 10,1.1.1 any eq 23access-list 101 deny tcp host 172.16.1.1 any eq 23 access-list 101 permit ip any any!interface E0/0service-policy input PM-CoPP

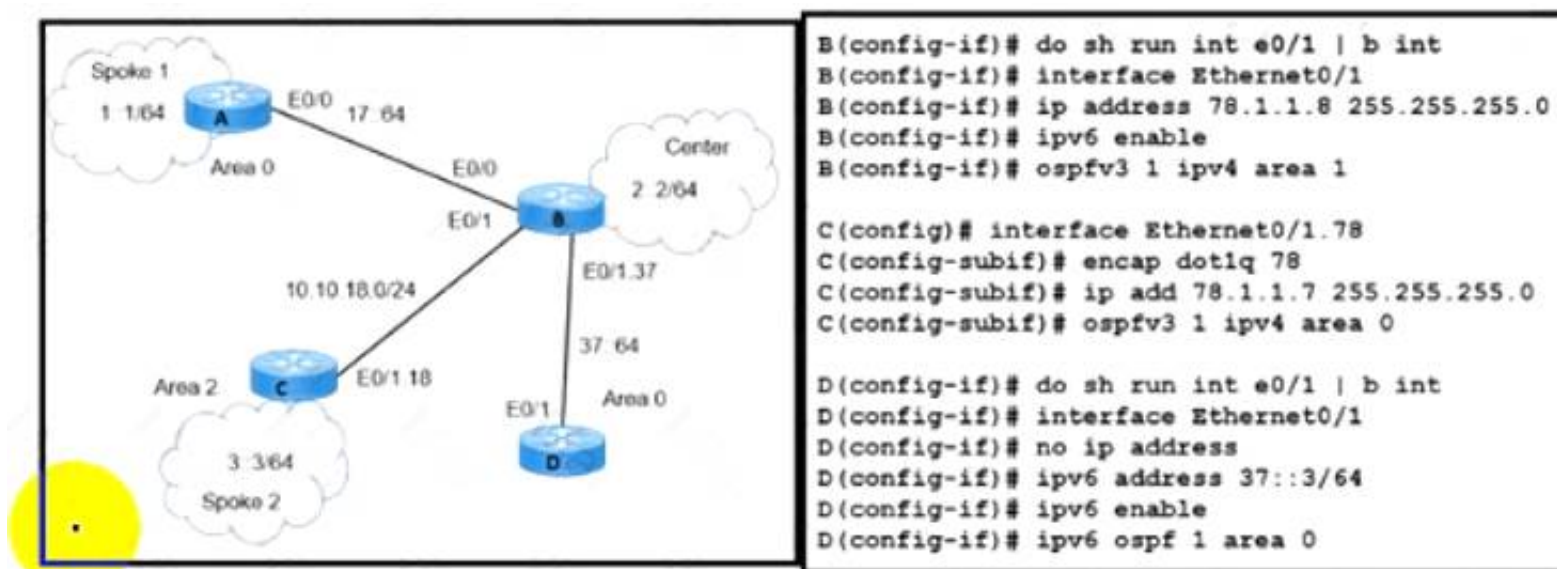
**Answer:** C

**Explanation:**

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

**NEW QUESTION 151**

- (Exam Topic 3)



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

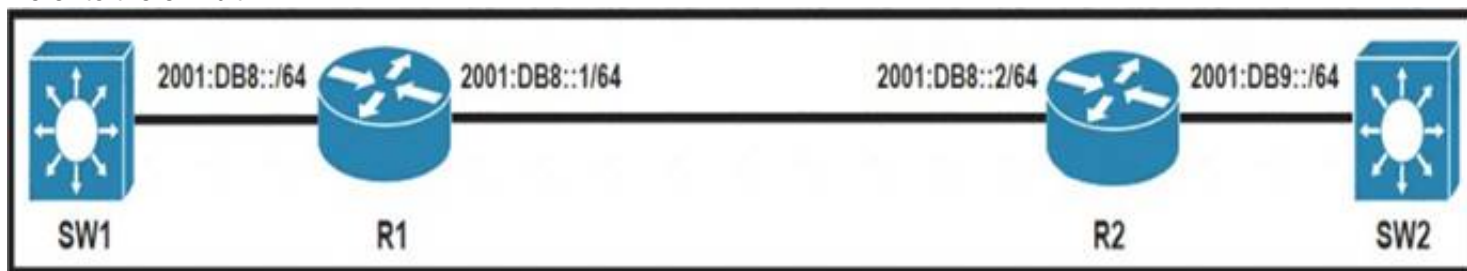
- A. Configure the Spoke 2 users IP on the router B OSPF domain
- B. Configure encapsulation dot1q 78 on the router C interface.
- C. Configure IPv6 on the routers B and C interfaces
- D. Configure OSPFv2 on the routers B and C interfaces

**Answer: C**

#### NEW QUESTION 156

- (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?

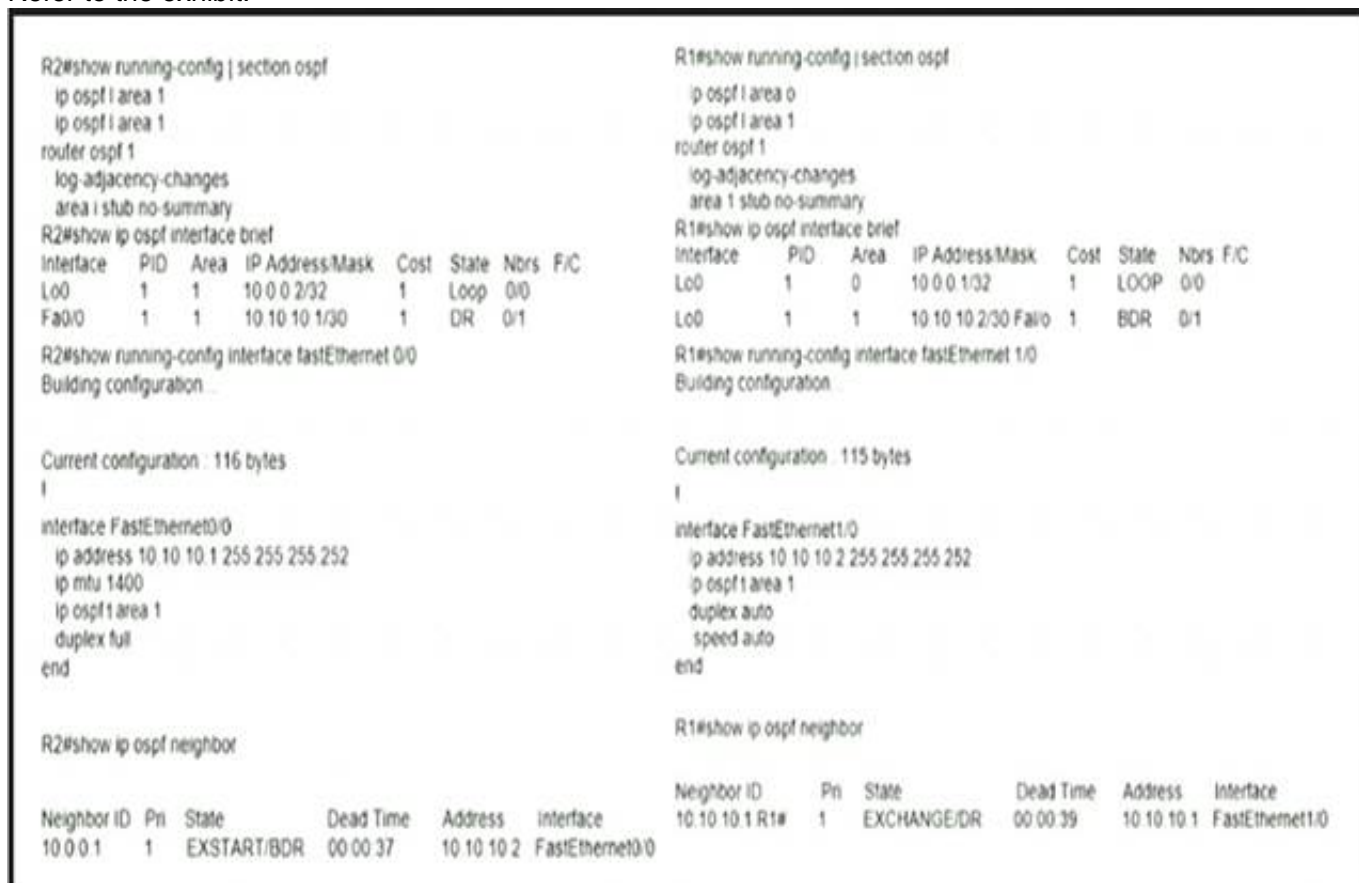
- A. router bgp 65000no bgp default ipv4-unicast address-family ipv6 multicast network 2001:DB8::/64
- B. router bgp 65000no bgp default ipv4-unicast address-family ipv6 unicast network 2001:DB8::/64
- C. router bgp 64900no bgp default ipv4-unicast address-family ipv6 unicast network 2001:DB8::/64
-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

**Answer: B**

#### NEW QUESTION 159

- (Exam Topic 3)

Refer to the exhibit.



Which action restores OSPF adjacency between R1 and R2?

- A. Change the IP MTU of R1 Fa1/0 to 1300
- B. Change the IP MTU of R2 Fa0/0 to 1300
- C. Change the IP MTU of R1 Fa1/0 to 1500

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

**Answer:** D

#### NEW QUESTION 163

- (Exam Topic 3)

A network engineer must configure a DMVPN network so that a spoke establishes a direct path to another spoke if the two must send traffic to each other. A spoke must send traffic directly to the hub if required Which configuration meets this requirement?

☐ At the hub router:  
interface tunnel10  
ip nhrp nhs multicast dynamic  
ip nhrp nhs shortcut  
tunnel mode gre multipoint

On the spokes router:  
interface tunnel10  
ip nhrp nhs multicast dynamic  
ip nhrp nhs redirect  
tunnel mode gre multipoint

☒ At the hub router:  
interface tunnel10  
ip nhrp map multicast dynamic  
ip nhrp redirect  
tunnel mode gre multipoint

On the spokes router:  
interface tunnel10  
ip nhrp map multicast dynamic  
ip nhrp shortcut  
tunnel mode gre multipoint

☐ At the hub router:  
interface tunnel10  
ip nhrp nhs dynamic multipoint  
ip nhrp nhs shortcut  
tunnel mode gre multicast

On the spokes router:  
interface tunnel10  
ip nhrp nhs multicast dynamic  
ip nhrp nhs redirect  
tunnel mode gre multicast

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

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

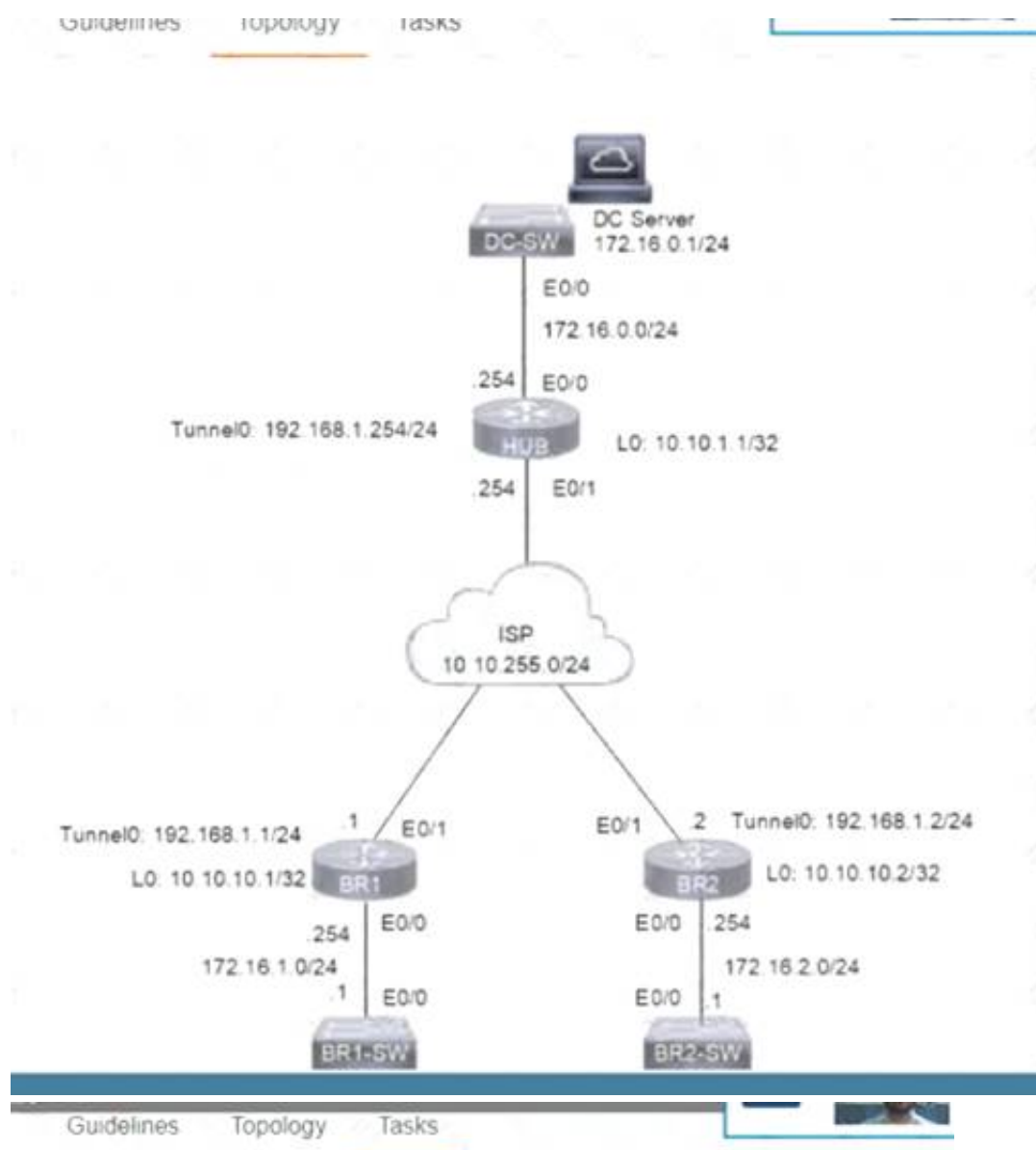
**Answer:** B

#### NEW QUESTION 164

- (Exam Topic 3)

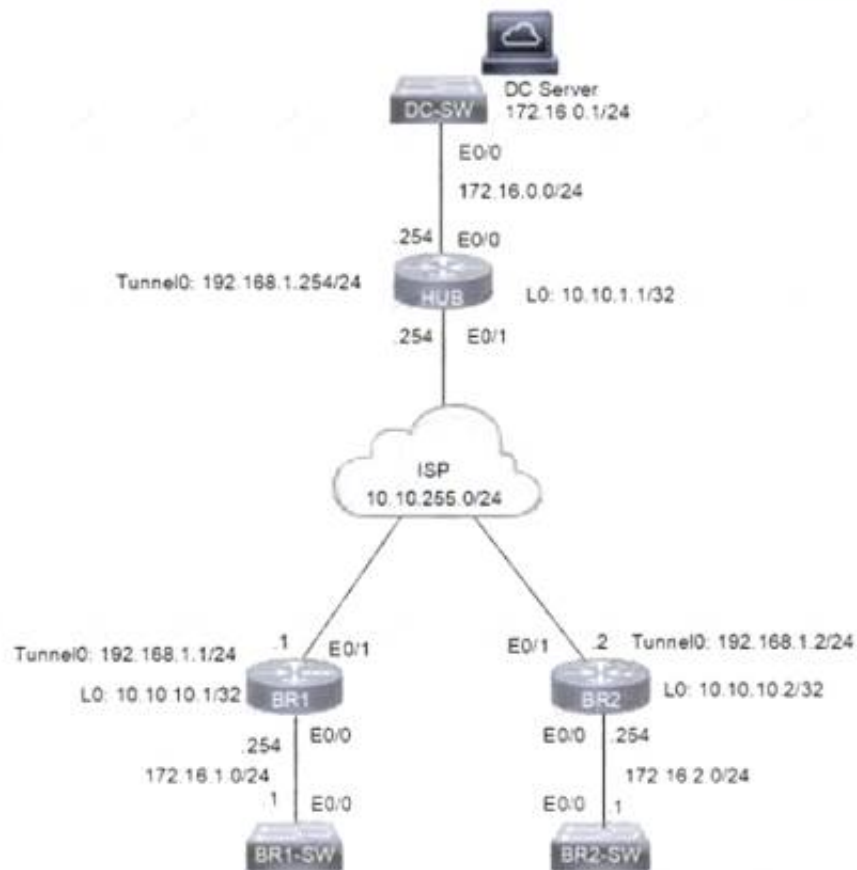
A DMVPN network is preconfigured with tunnel 0 IP address 192.168.1.254 on the HUB, IP connectivity, crypto policies, profiles, and EIGRP AS 100. The NHRP password is ccnp123, and the network ID and tunnel key is EIGRP ASN Do not introduce a static route. Configure DMVPN connectivity between routers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





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

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



Topology Diagram

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

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

Submit feedback about this item

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

ON BR1

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

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

ON BR2

```
DC-SW  HUB  BR1  BR1-SW  BR2  BR2-SW

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

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

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

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

Current configuration : 404 bytes
!
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication ccmp123
 ip nhrp map 192.168.1.254 10.10.255.254
 ip nhrp map multicast 10.10.255.254
 ip nhrp network-id 100
 ip nhrp holdtime 5
 ip nhrp nhs 192.168.1.254
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source 10.10.10.2
 tunnel destination 10.10.255.254
 tunnel key 100
end
```

**NEW QUESTION 165**

- (Exam Topic 3)

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

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

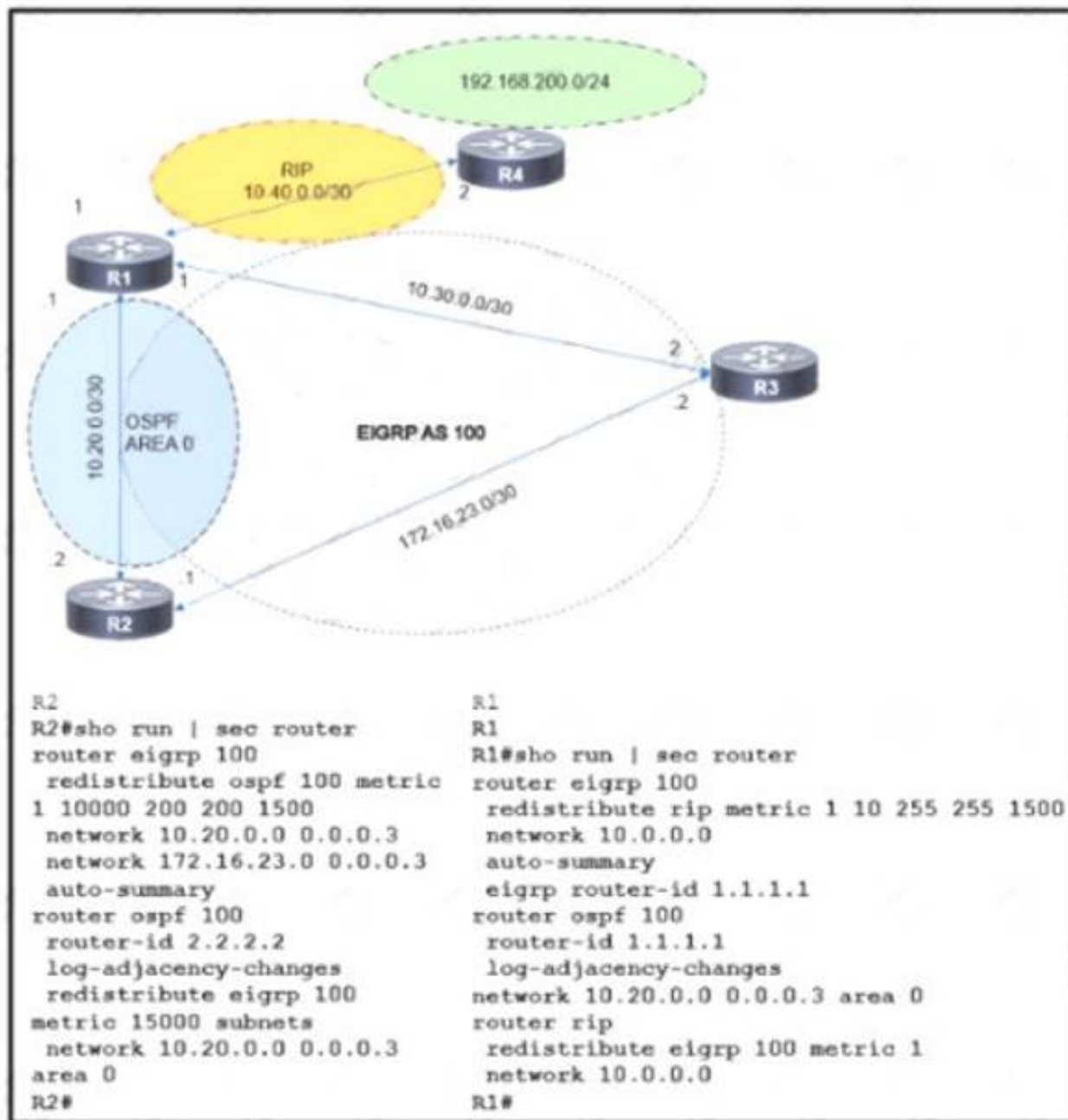
- A. Rediscover all the router interfaces through SNMP after the router is reloaded
- B. Save the router configuration to startup-config before reloading the router
- C. Configure SNMP to use static OIDs referring to individual router interfaces
- D. Configure SNMP interface index persistence on the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

Answer: D

**NEW QUESTION 166**

- (Exam Topic 3)





Refer to the exhibit The route to 192 168 200 0 is flapping between R1 and R2 Which set of configuration changes resolves the flapping route?

- ☐ R2(config)#router ospf 100  
R2(config-router)#no redistribute eigrp 100  
R2(config-router)#redistribute eigrp 100 metric 1 subnets
- ☐ R1(config)#no router rip  
R1(config)#ip route 192.168.200.0 255.255.255.0 10.40.0.2
- ☐ R2(config)#router eigrp 100  
R2(config-router)#no redistribute ospf 100  
R2(config-router)#redistribute rip
- ☒ R1(config)#router ospf 100  
R1(config-router)#redistribute rip metric 1 metric-type 1 subnets

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

Answer: D

#### NEW QUESTION 167

- (Exam Topic 3)

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

The administrator has configured the following on R1:

```

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

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

- ☐ line vty 0 4  
login authentication RAD-LOCAL
- ☐ line vty 0 4  
login authentication default
- ☐ line vty 0 4  
login authentication RAD-SERV
- ☐ aaa authentication login RAD-SERV group RAD-LOCAL local
- ☐ aaa authentication login RAD-LOCAL group RAD-SERV local

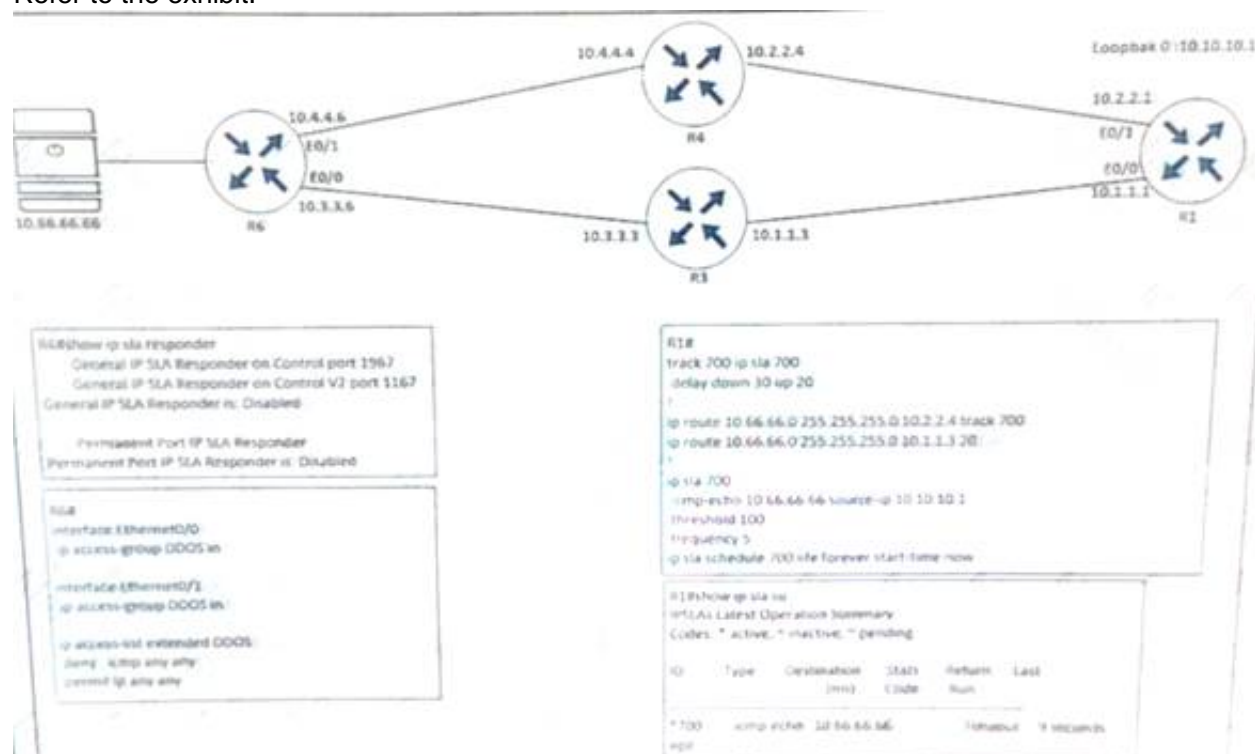
- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: CE

### NEW QUESTION 172

- (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(config ext-nacl)# 5 permit icmp host 10.66.66.66 host 10.10.10.1
- D. R6(config)# ip access-list extended DDOSR6(config ext-nacl)# 5 permit icmp host 10.10.10.1 host 10.66.66.66

Answer: D

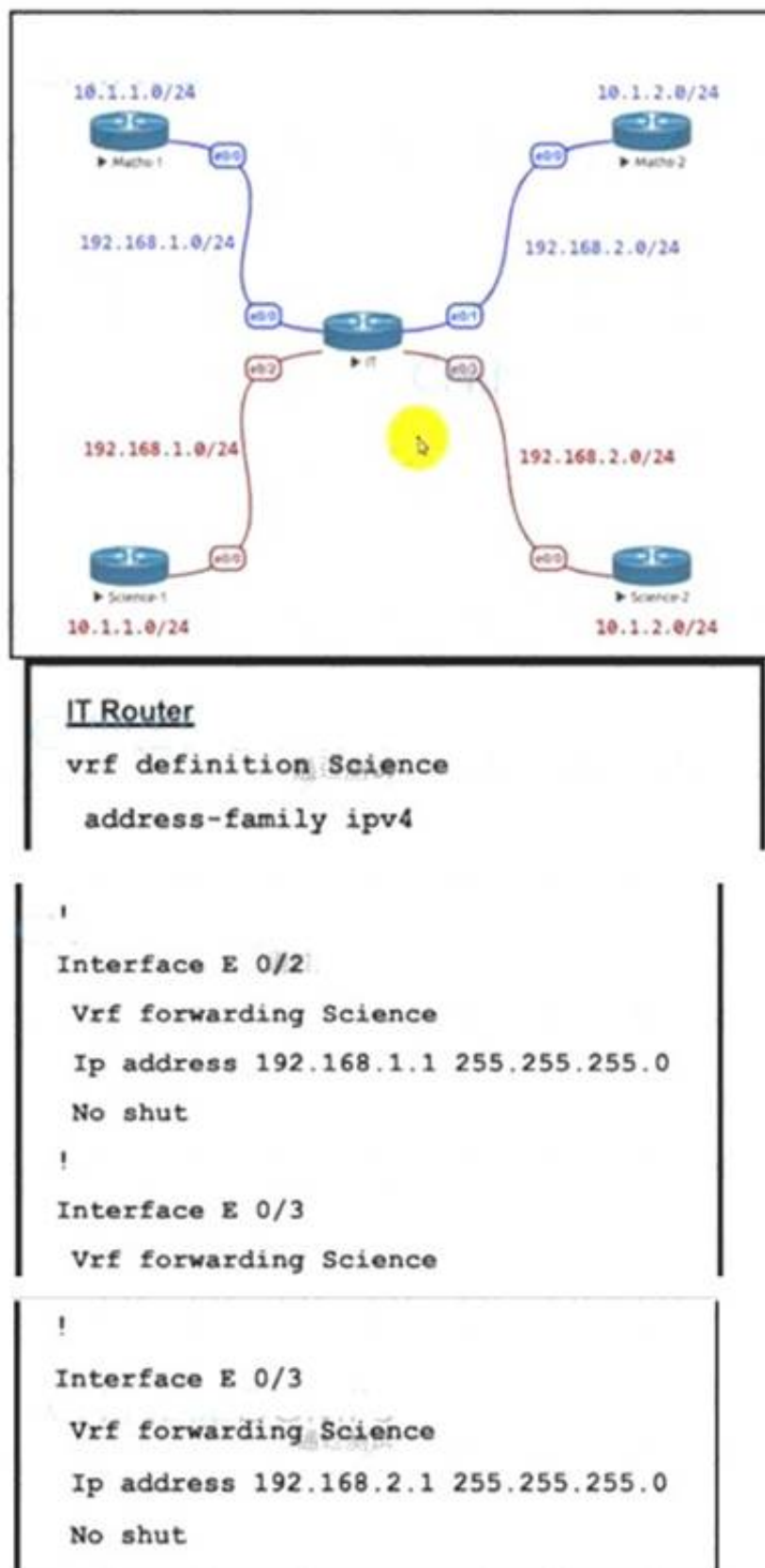
### Explanation:

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 176

- (Exam Topic 3)



Refer to the exhibit. The IT router has been configured with the Science VRF and the interfaces have been assigned to the VRF. Which set of configurations advertises Science-1 and Science-2 routes using EIGRPAS 111?

- ☐ router eigrp 111
  - address-family ipv4 vrf Science autonomous-system 1
  - network 192.168.1.0
  - network 192.168.2.0
- ☐ router eigrp 111
  - address-family ipv4 vrf Science
  - network 192.168.1.0
  - network 192.168.2.0
- ☐ router eigrp 111
  - network 192.168.1.0
  - network 192.168.2.0
- ☐ router eigrp 1
  - address-family ipv4 vrf Science autonomous-system 111
  - network 192.168.1.0
  - network 192.168.2.0

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

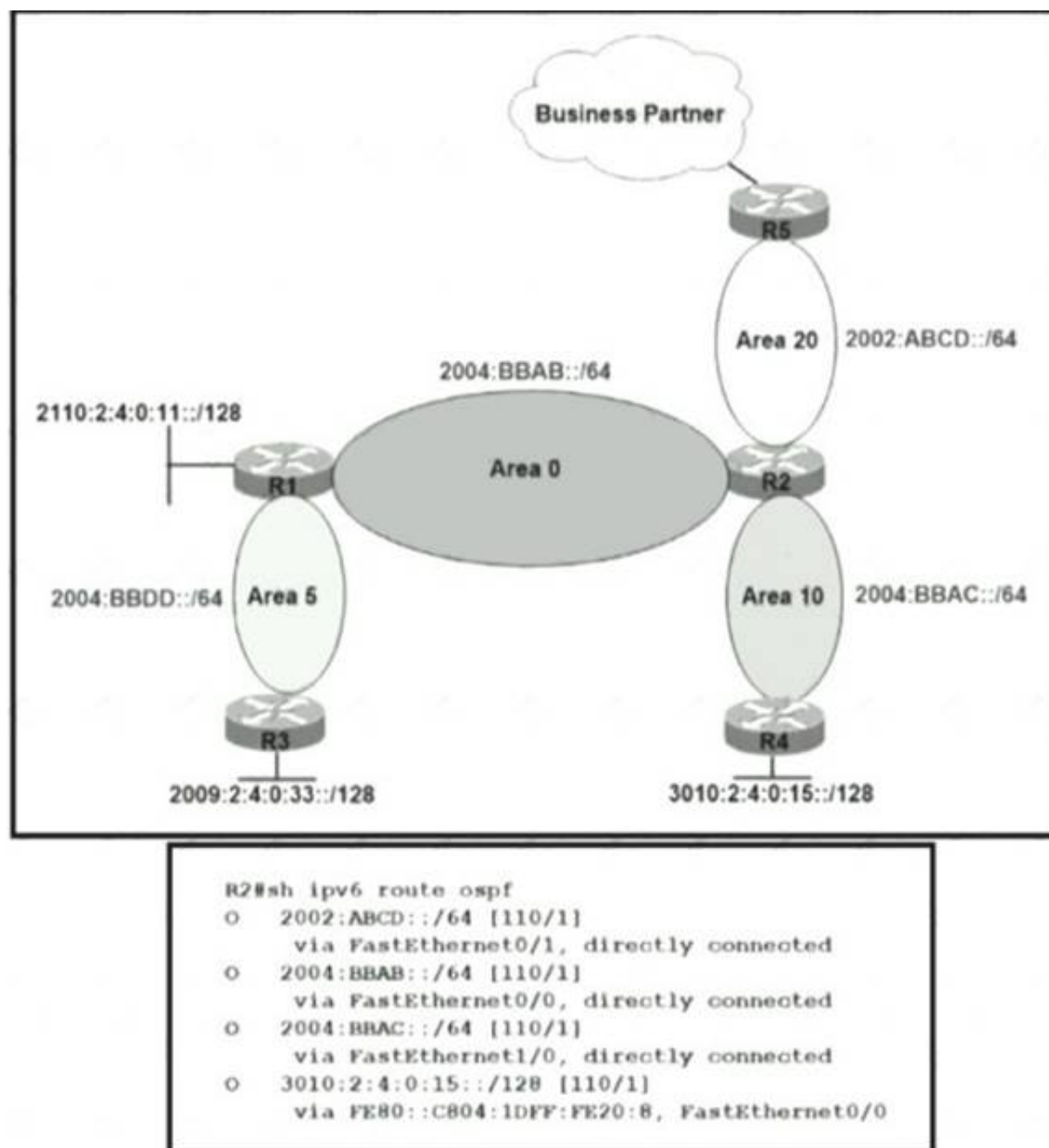
**Answer: D**

#### NEW QUESTION 180

- (Exam Topic 3)

Refer to the exhibit.





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

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

**Answer:** D

#### NEW QUESTION 183

- (Exam Topic 3)

What is a function of an end device configured with DHCPv6 guard?

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

**Answer:** C

#### Explanation:

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.

Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).

If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

#### NEW QUESTION 184

- (Exam Topic 3)

Refer to the exhibit.

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

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

- A. Configure two static routes for the 8.8.8.8/32 destination to match the IP SLA probe for each ISP.
- B. Associate every IP SLA probe with the proper WAN address of the router.
- C. Reference the proper exit interfaces along with the next hops in both static default routes.
- D. Use a separate track object to reference the existing IP SLA 1 probe for every static route.
- E. Use a separate IP SLA probe and track object for every static route

**Answer:** AE

#### NEW QUESTION 187

- (Exam Topic 3)

What are the two reasons for RD and VPNv4 addresses in an MPLS Layer 3 VPN? (Choose two.)

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

**Answer:** AC

#### NEW QUESTION 191

- (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?

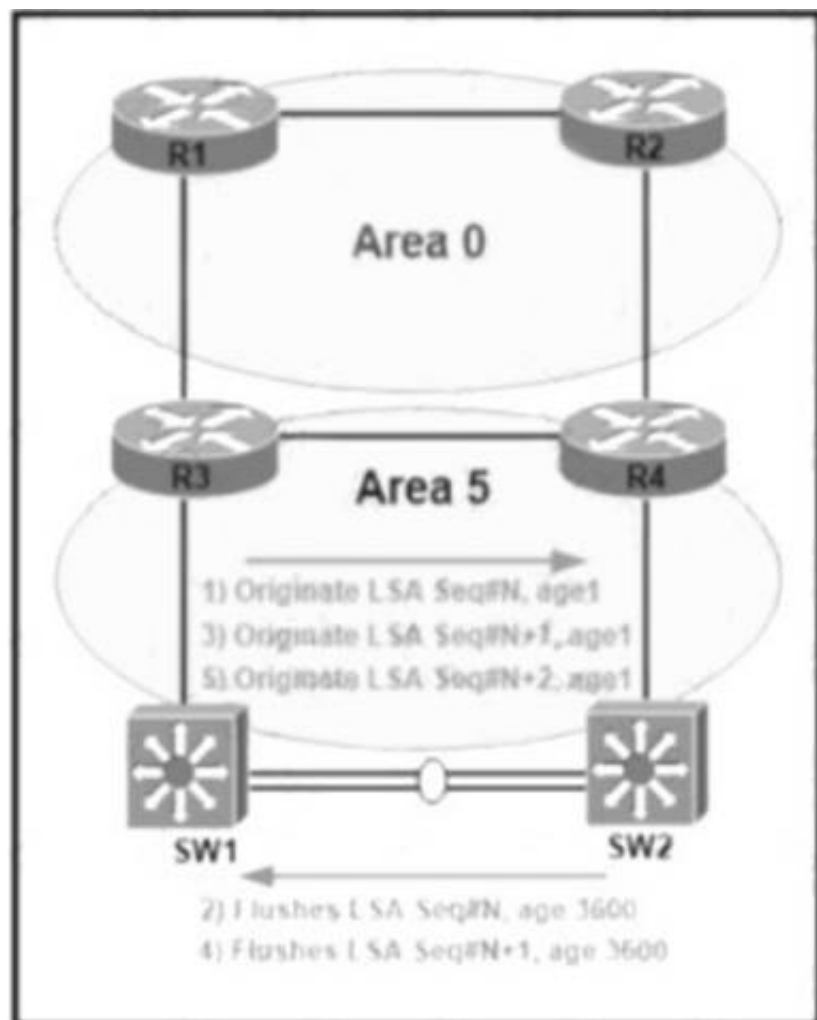
- A. Change the R1 dead timer to 20.
- B. Change the R2 dead timer to 20.
- C. Change the R2 hello timer to 20.
- D. Change the R1 hello timer to 20.

**Answer:** A

#### NEW QUESTION 193

- (Exam Topic 3)

Refer to the exhibit.



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

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

**Answer: D**

#### NEW QUESTION 197

- (Exam Topic 3)

What is the function of BFD?

- A. It provides uniform failure detection regardless of media type.
- B. It creates high CPU utilization on hardware deployments.
- C. It negotiates to the highest version if the neighbor version differs.
- D. It provides uniform failure detection on the same media type.

**Answer: A**

#### NEW QUESTION 201

- (Exam Topic 3)

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

```
interface GigabitEthernet2
description Migration ID: B410A60D0806G06
vrf forwarding RED
ip address 10.0.0.0 255.255.255.254
negotiation auto
```

Which configuration completes the change?

- A. interface GigabitEthernet2 no ip addressvrf forwarding BLUE
- B. interface GigabitEthernet2 no vrf forwarding RED vrf forwarding BLUEip address 10.0.0.0 255.255.255.254
- C. interface GigabitEthernet2 no vrf forwarding RED vrf forwarding BLUE
- D. interface GigabitEthernet2 no ip addressip address 10.0.0.0 255.255.255.254vrf forwarding BLUE

**Answer: B**

#### Explanation:

When assigning an interface to a VRF, the IP address will be removed so we have to reassign the IP address to that interface.

#### NEW QUESTION 203

- (Exam Topic 3)

What action is performed for untagged outgoing labels in an MPLS router?

- A. Convert the incoming MPLS packet to an untagged packet and then do a FIB lookup

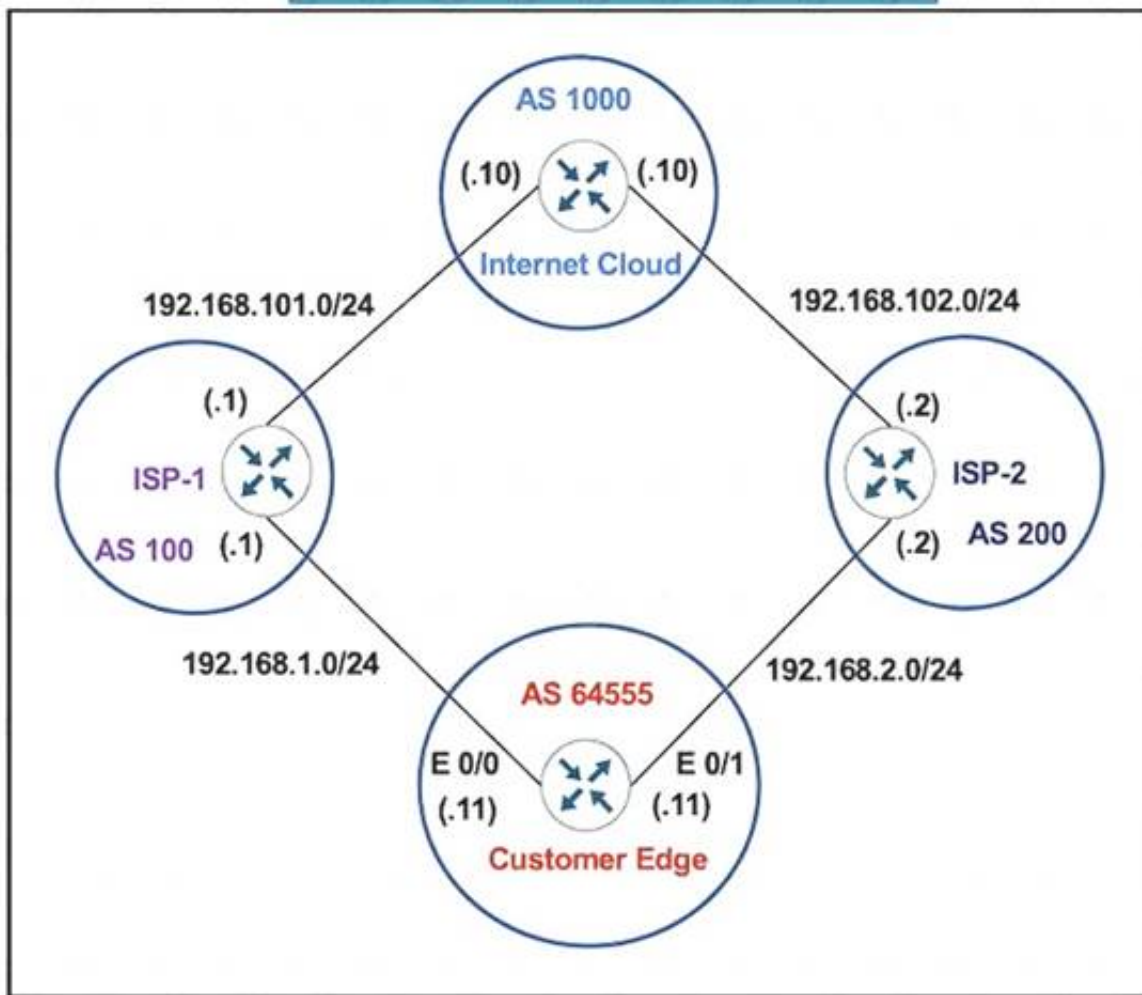


- B. Convert the incoming MPLS packet to an untagged packet and then do a RIB lookup.
- C. Convert the untagged packet to a labeled packet and forward it to the next router
- D. Convert the incoming MPLS packet to an IP packet and forward it to the next router.

**Answer: C**

**NEW QUESTION 206**

- (Exam Topic 3)



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

**Customer-Edge**

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

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

A)

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

B)

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

C)

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

D)

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

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

**Answer: C**

#### NEW QUESTION 207

- (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?

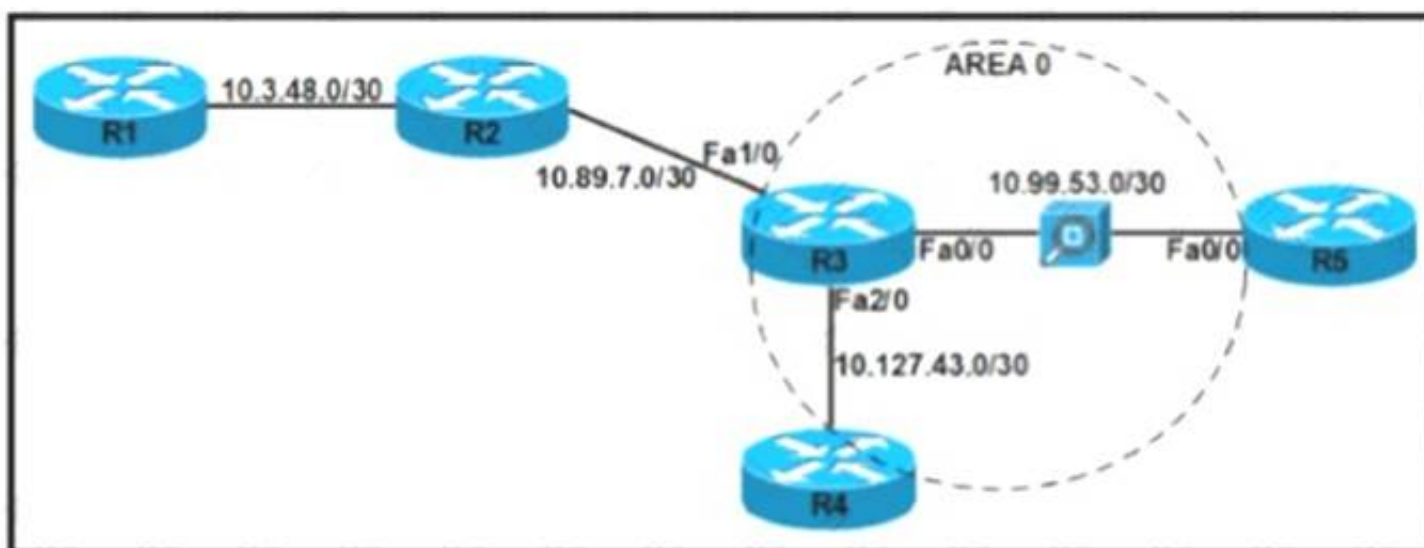
- A. Configure the logging synchronous command on line vty.
- B. Configure the exec command on line vty.
- C. Configure the login local command on line vty
- D. Configure the enable password command on line vty.

**Answer: C**

#### NEW QUESTION 208

- (Exam Topic 3)

Refer to the exhibit.



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

A)



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

B)

```
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network non-broadcast
ip ospf priority 0
!
router ospf 10
router-id 10.10.3.255
network 10.99.53.0 0.0.0.3 area 0
neighbor 10.99.53.2
!
access-list 122 permit 89 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 89 any any
access-list 122 permit tcp any any
access-list 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 88 host 10.99.53.2 host 10.99.53.1
access-list 122 deny 88 any any
!
```

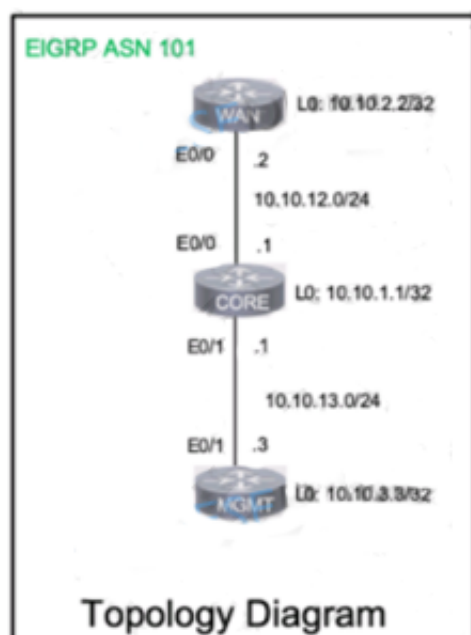
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** C

#### NEW QUESTION 212

- (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
```

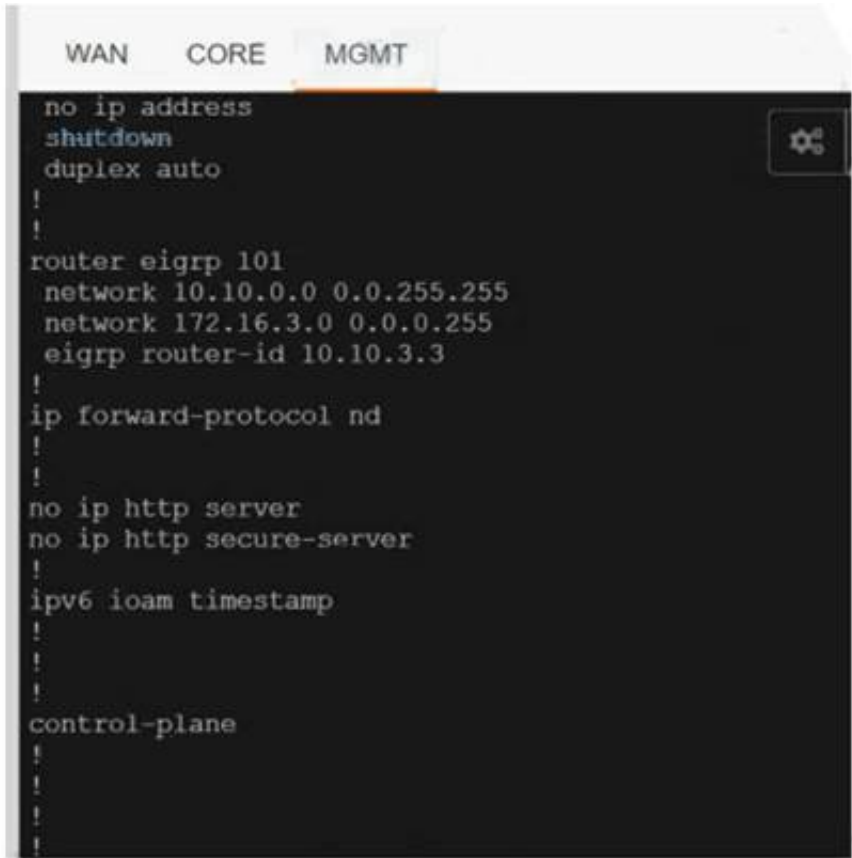
```
!
!
access-list 120 remark *** ACL for CoPP-Critical ***
access-list 121 remark *** ACL for CoPP-IMPORTANT
access-list 122 remark *** ACL for CoPP-NORMAL
!
control-plane
 service-policy input CoPP
!
!
```

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
```



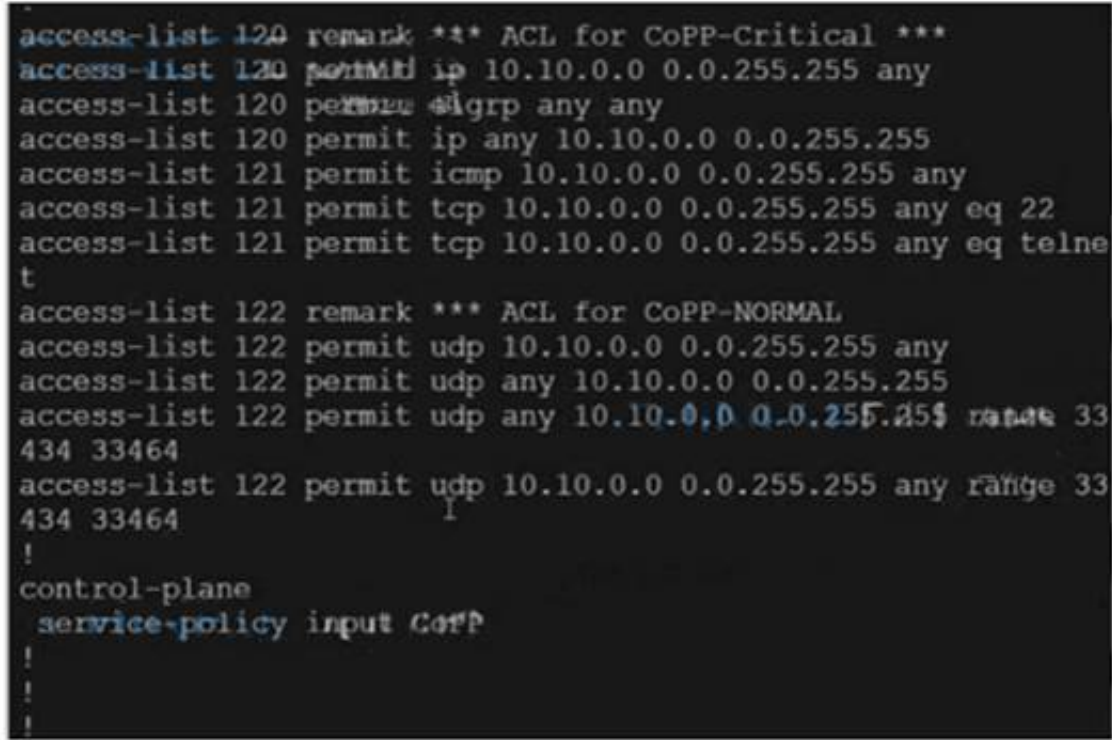


- A. Mastered
- B. Not Mastered

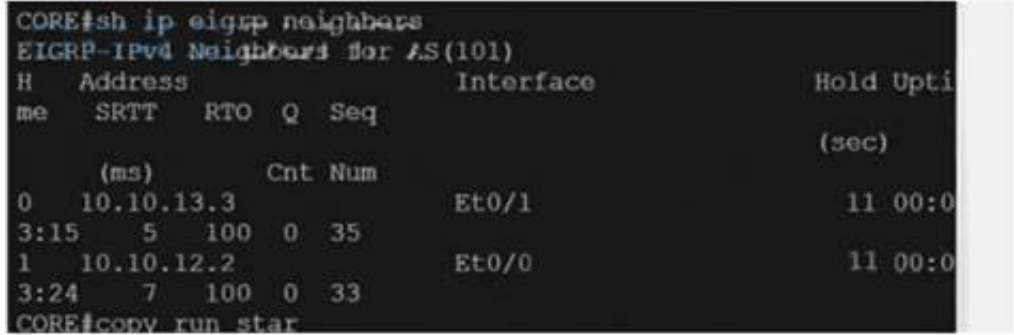
Answer: A

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



CORE# Copy run start TESTING: CORE  
 Graphical user interface Description automatically generated with medium confidence



MGMT  
 Graphical user interface, text Description automatically generated

```

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

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open

Password required, but none set
[Connection to 10.10.13.1 closed by foreign host]
MGMT#

```

#### NEW QUESTION 214

- (Exam Topic 3)

Refer to the exhibit.

```

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

```

When the 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 216

- (Exam Topic 3)

Refer to the exhibit.

```

RtrA#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(1)/ID(10.1.6.1)
... snip ...
P 10.200.1.0/24, 1 successors, FD is 21026560
  via 10.1.1.2 (21026560/20514560), Serial1/0
  via 10.1.2.2 (46740736/20514560), Serial1/1
  via 10.1.3.2 (46740736/46228736), Serial1/2

```

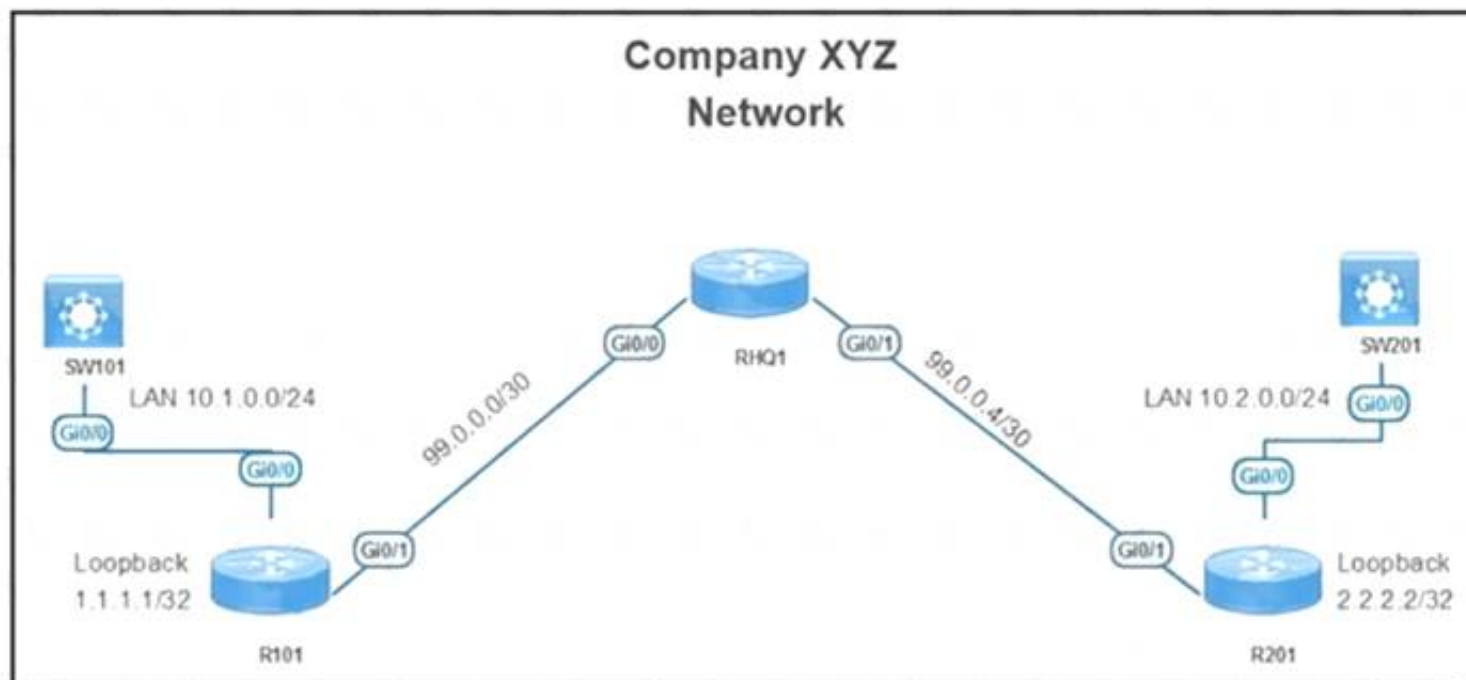
Which action makes 10.1.3.2 the feasible successor to reach 10.200.1.0/24 for location S42T447E33F95?

- A. Increase path bandwidth lower than 1011.2 and lower than 1012.2 between RtrA and the destination
- B. Increase path bandwidth higher than 10.1.2.2 and lower than 101.1.2 between RtrA and the destination.
- C. Increase path bandwidth higher than 1011.2 and lower than 1012.2 between RtrA and the destination
- D. Increase path bandwidth higher than 10.1.2.2 and higher than 10.1.1.2 between RtrA and the destination

**Answer: A**

#### NEW QUESTION 217

- (Exam Topic 3)



```
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

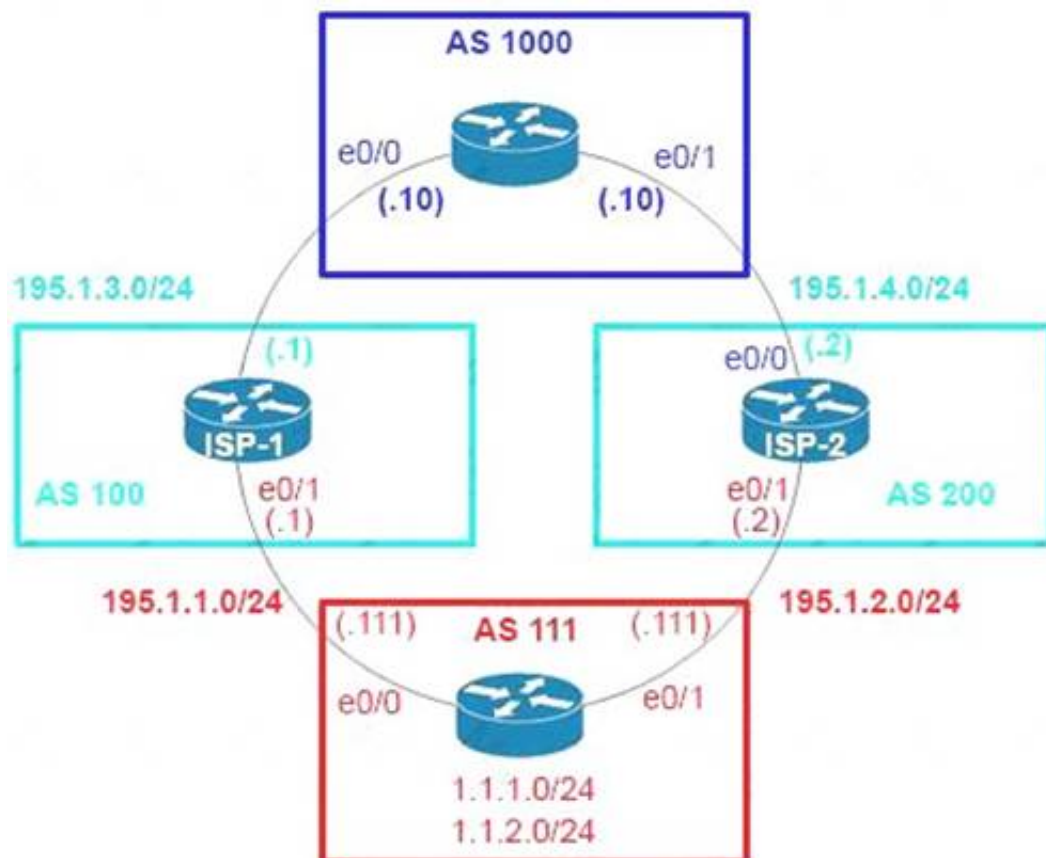
**Answer: A**

#### NEW QUESTION 218

- (Exam Topic 3)

Refer to the exhibit.





### AS111

Router bgp 111

Neighbor 195.1.1.1 remote-as 100

Neighbor 195.1.1.1 allowas-in

Neighbor 195.1.2.2 remote-as 200

Neighbor 195.1.2.2 allowas-in

AS111 is receiving its own routes from AS200 causing a loop in the network. Which configuration provides loop prevention?

- A)
- ```

router bgp 111
 neighbor 195.1.1.1 as-override
 neighbor 195.1.2.2 as-override
    
```
- B)
- ```

router bgp 111
 neighbor 195.1.1.1 as-override
 no neighbor 195.1.2.2 allowas-in
    
```
- C)
- ```

router bgp 111
 no neighbor 195.1.1.1 allowas-in
 no neighbor 195.1.2.2 allowas-in
    
```
- D)
- ```

router bgp 111
 neighbor 195.1.2.2 as-override
 no neighbor 195.1.1.1 allowas-in
    
```

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

**Answer:** C

#### **Explanation:**

A router discards BGP network prefixes if it sees its ASN in AS-Path as a loop prevention mechanism. The “allowas-in” feature allows routes to be received and processed even if router detects its own ASN in AS-Path.

#### **NEW QUESTION 223**

- (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
```

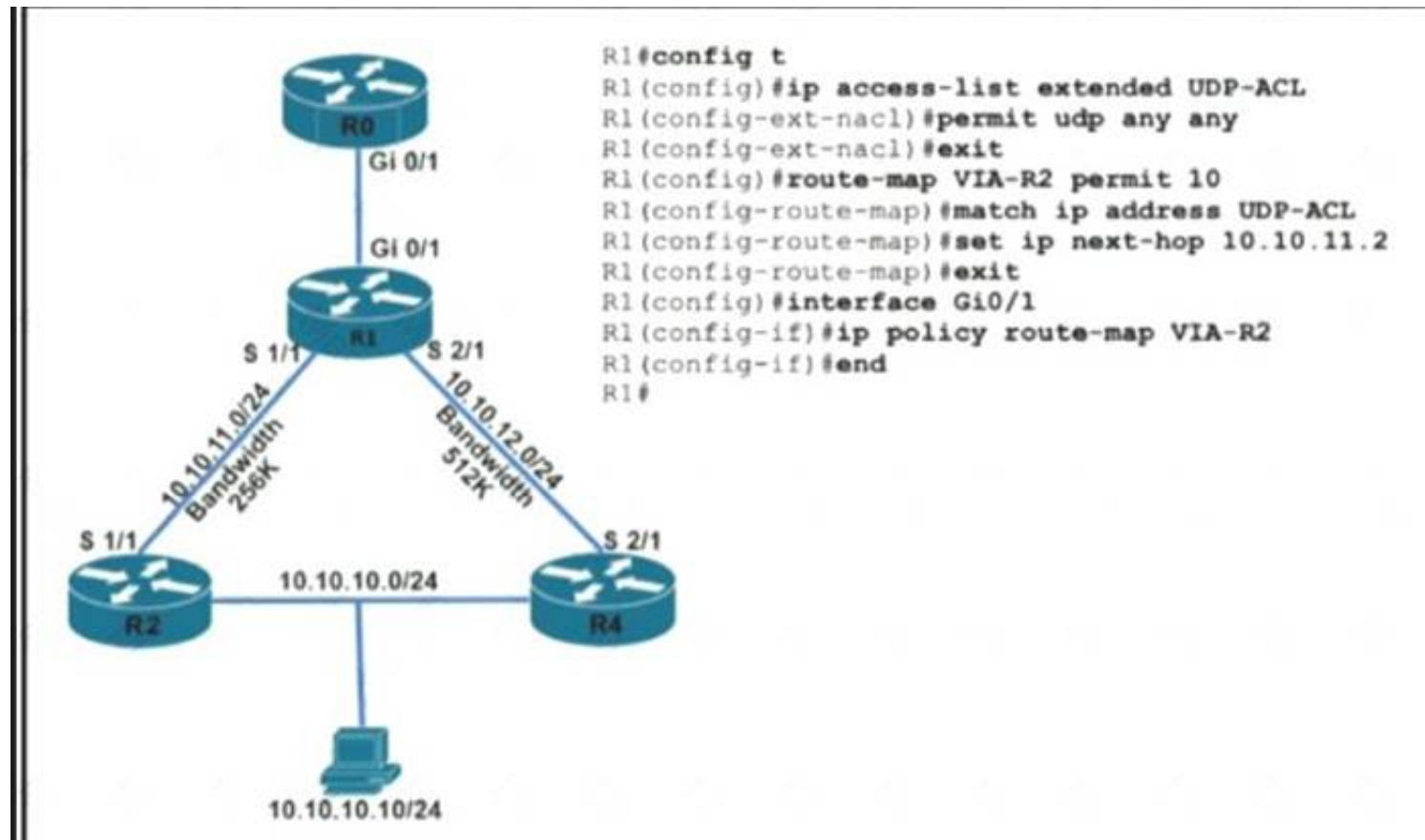
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/34/56 ms
```

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 226

- (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?

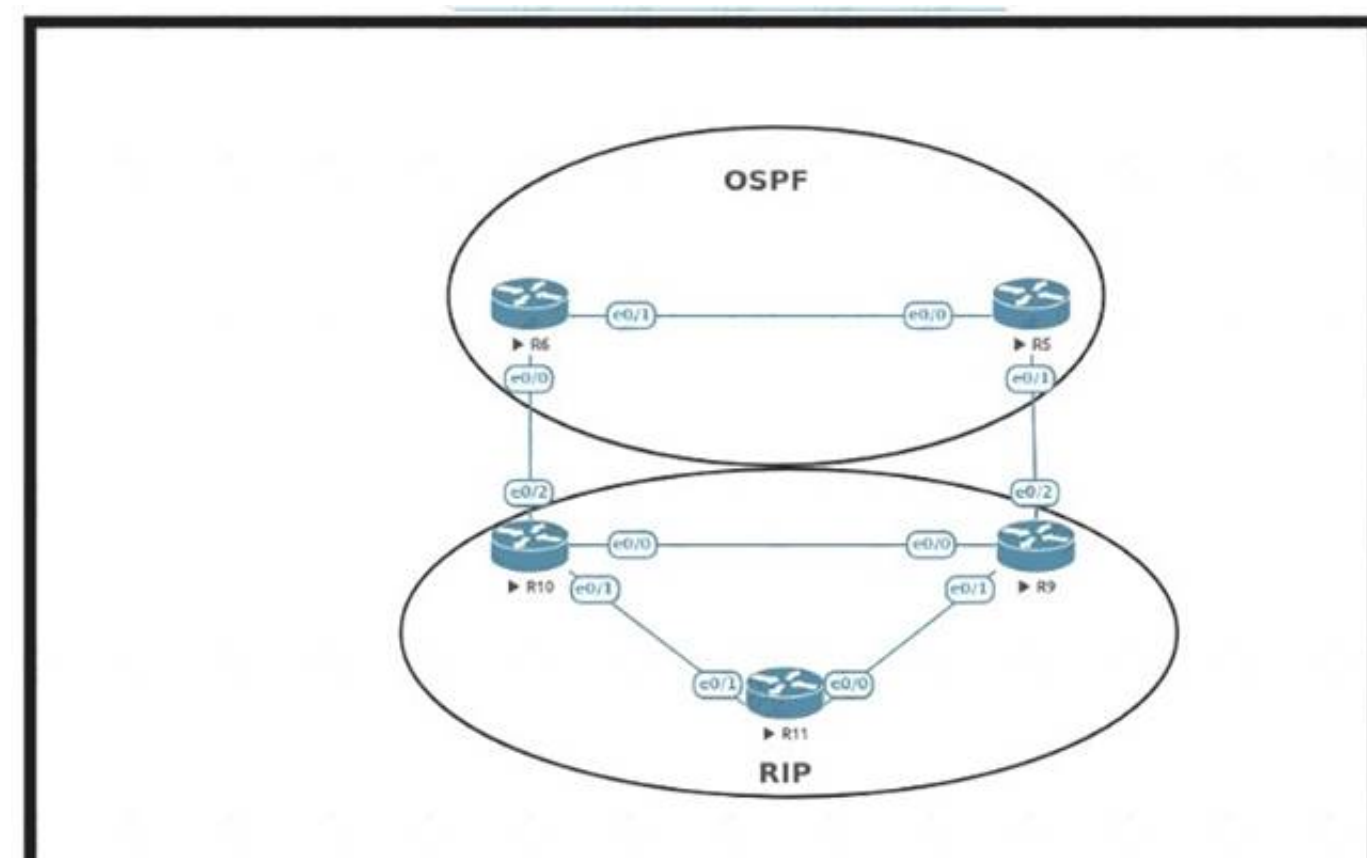
- A. TCP traffic will reach the destination via R2 without any changes
- B. Add a permit 20 statement in the route map to allow TCP traffic
- C. Allow TCP in the access list with no changes to the route map
- D. Set IP next-hop to 10.10.12.2 under the route-map permit 10 to allow TCP traffic.

Answer: C

#### NEW QUESTION 227

- (Exam Topic 3)

Refer to the exhibit.





An engineer must configure OSPF with R9 and R10 and configure redistribution between OSPF and RIP causing a routing loop Which configuration on R9 and R10 meets this objective?

A)

```
router ospf 1
 redistribute rip subnets tag 20
 !
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 permit 20
 !
router ospf 1
 distribute-list route-map deny_tag20 in
```

B)

```
router ospf 1
 redistribute rip subnets tag 20
 !
route-map deny_tag20 permit 10
 match tag 20
route-map deny_tag20 permit 20
 !
router ospf 1
 distribute-list route-map deny_tag20 in
```

C)

```
router ospf 1
 redistribute rip subnets tag 20
 !
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 deny 20
 !
router ospf 1
 distribute-list route-map deny_tag20 in
```

D)

```
router ospf 1
 redistribute rip subnets tag 20
 !
route-map deny_tag20 deny 10
 match tag 20
route-map deny_tag20 permit 20
 !
router rip 1
 distribute-list route-map deny_tag20 in
```

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

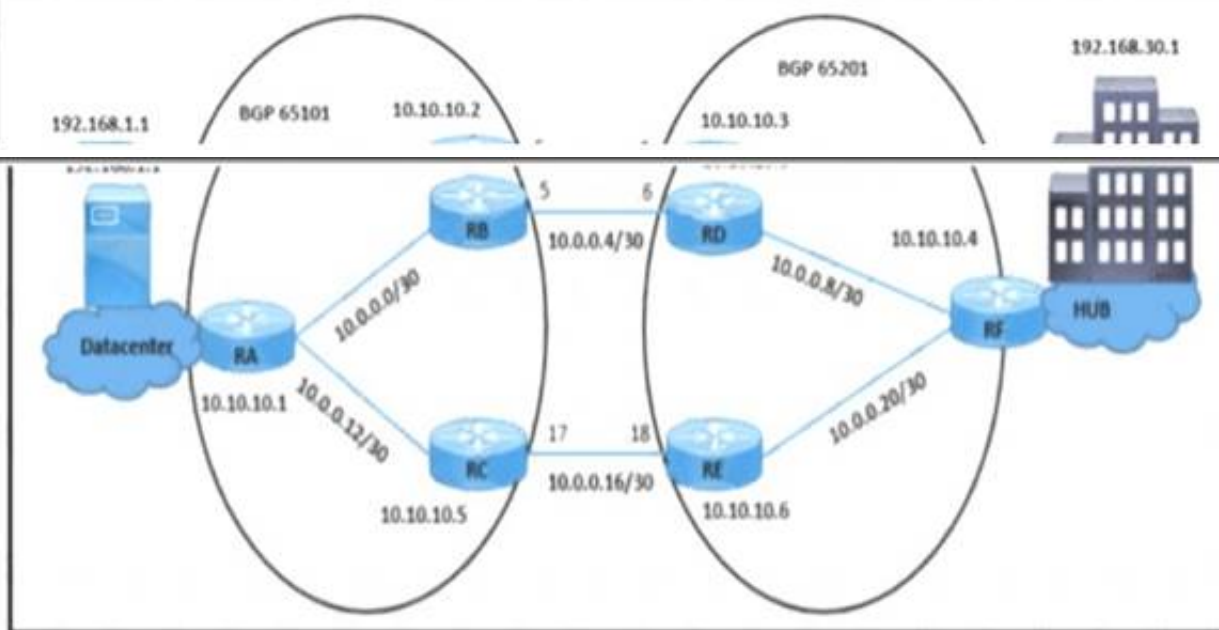
**Answer:** A

#### **NEW QUESTION 232**

- (Exam Topic 3)

```
RD#show ip bgp 192.168.1.1
Advertised to update-groups:
  3
 65101
 10.10.10.2 (metric 2) from 10.10.10.2 (10.10.10.2)
  Origin IGP, metric 100, localpref 100, weight 65535, valid, external,
best
 65101
 10.0.0.17 (metric 2) from 10.10.10.6 (172.16.20.1)
  Origin IGP, metric 0, localpref 100, valid, internal

RB#show ip bgp 192.168.1.1
BGP routing table entry for 192.168.1.1/32, version 10
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Advertised to update-groups:
  2
Local
 10.10.10.1 (metric 2) from 10.10.10.1 (192.168.1.1)
  Origin IGP, metric 0, localpref 100, valid, internal, best
```



Refer to the exhibit. A customer finds that traffic from the application server (192.168.1.1) to the HUB site passes through a congested path that causes random packet drops. The NOC team influences the BGP path with MED on RB, but RD still sees that traffic coming from RA is not taking an alternate route. Which configuration resolves the issue?

A)

```
RD(config)#router bgp 65201
RD(config-router)#no neighbor 10.10.10.2 weight 65535
```

B)

```
RB(config)#router bgp 65101
RB(config-router)#no neighbor 10.10.10.3 route-map HIGH-LP out
```

C)

```
RB(config)#router bgp 65101
RB(config-router)#neighbor 10.10.10.3 weight 50
```

D)

```
RC(config)#router bgp 65101
RC(config-router)#neighbor 10.10.10.6 route-map HIGH-LP out
```

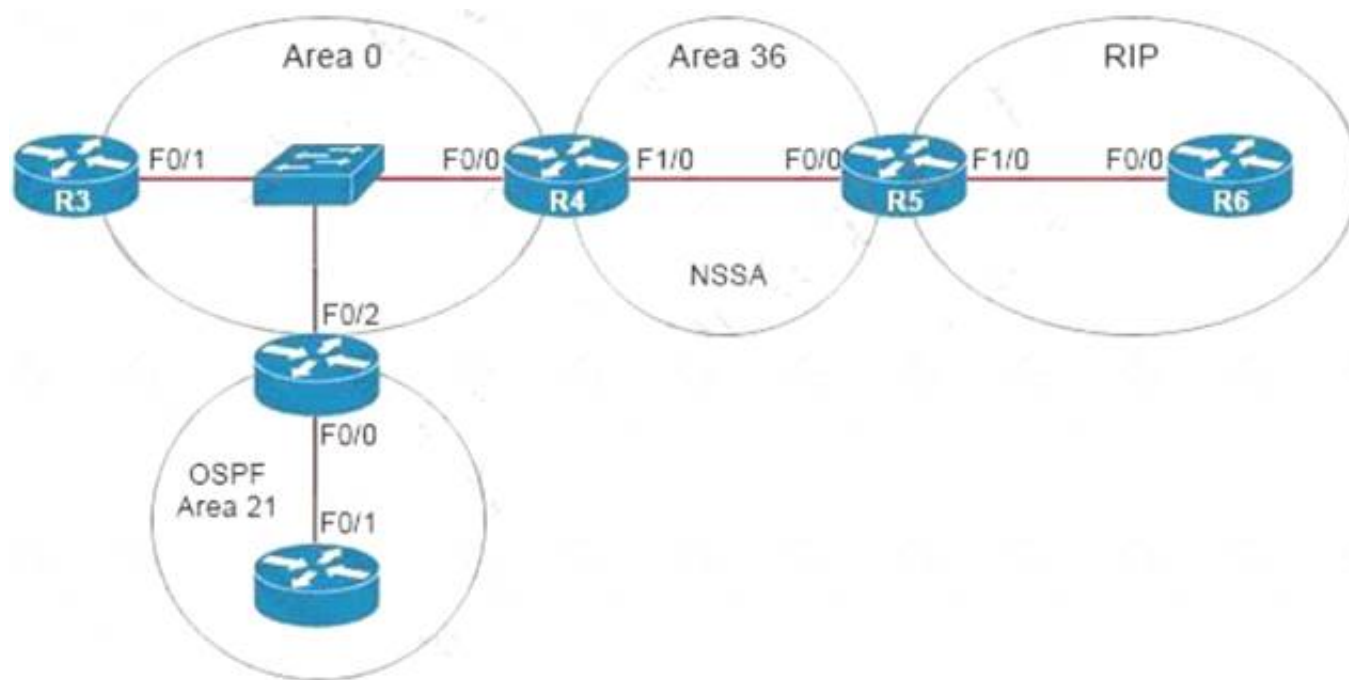
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

#### NEW QUESTION 237

- (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 areaR5(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 areaR4(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 238

- (Exam Topic 3)

```
100.0.0.0/32 is subnetted, 3 subnets
C 100.1.1.1 is directly connected, Loopback0
D 100.2.2.2 [90/156160] via 10.1.1.2, 00:00:46, FastEthernet0/0
D 100.3.3.3 [90/158720] via 10.1.1.14, 00:00:44, FastEthernet1/0
  [90/158720] via 10.1.1.2, 00:00:44, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 13 subnets, 4 masks
D 10.1.1.8/30 [90/30720] via 10.1.1.14, 00:00:44, FastEthernet1/0
C 10.1.1.12/30 is directly connected, FastEthernet1/0
C 10.1.1.0/30 is directly connected, FastEthernet0/0
D 10.1.1.4/30 [90/30720] via 10.1.1.2, 00:00:45, FastEthernet0/0
C 10.100.1.40/32 is directly connected, Loopback40
D EX 10.1.1.80/29 [170/33280] via 10.1.1.14, 00:00:45, FastEthernet1/0
  [170/33280] via 10.1.1.2, 00:00:45, FastEthernet0/0
C 10.100.1.50/32 is directly connected, Loopback50
C 10.100.1.10/32 is directly connected, Loopback10
S 10.100.1.0/24 is a summary, 00:00:48, Null0
C 10.100.1.30/32 is directly connected, Loopback30
C 10.100.1.20/32 is directly connected, Loopback20
C 10.200.1.0/24 is directly connected, FastEthernet0/1
D EX 10.247.10.0/30 [170/2174976] via 10.1.1.14, 00:00:46, FastEthernet1/0
  [170/2174976] via 10.1.1.2, 00:00:46, FastEthernet0/0
```

Refer to the exhibit. R1 must advertise all loopback interfaces IP addresses to neighbors, but EIGRP neighbors receive a summary route. Which action resolves the issue?

- A. Redistribute connected routes into EIGRP Enable
- B. EIGRP on loopback Interfaces.
- C. Disable auto summarization on R1.
- D. Remove the 10.100.1.0/24 static route.

**Answer: D**

#### NEW QUESTION 240

- (Exam Topic 3)

Refer to the exhibit. An engineer is trying to log in to R1 via R3 loopback address. Which action resolves the issue?

- A. Add transport input SCP
- B. Add transport input none



- C. Remove the IPv6 traffic filter from R1, which is blocking the Telnet.
- D. Remove the IPv6 traffic from R1, which is blocking the SSH

**Answer: C**

#### NEW QUESTION 243

- (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 vrf
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 247

- (Exam Topic 3)

Which table is used to map the packets in an MPLS LSP that exit from the same interface, via the same next hop, and have the same queuing policies?

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

**Answer: B**

#### NEW QUESTION 248

- (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 253

- (Exam Topic 3)

```
admin@linux:~$ telnet 198.51.100.64
Trying 198.51.100.64...
Connected to 198.51.100.64.
Escape character is '^]'.

User Access Verification

Password: admin
CPE> exit
Connection closed by foreign host.
admin@linux:~$ ssh 198.51.100.64
admin@198.51.100.64's password: admin
Permission denied, please try again.
admin@198.51.100.64's password: admin
Permission denied, please try again.
admin@198.51.100.64's password: admin
Connection closed by 198.51.100.64 port 22
admin@linux:~$
```

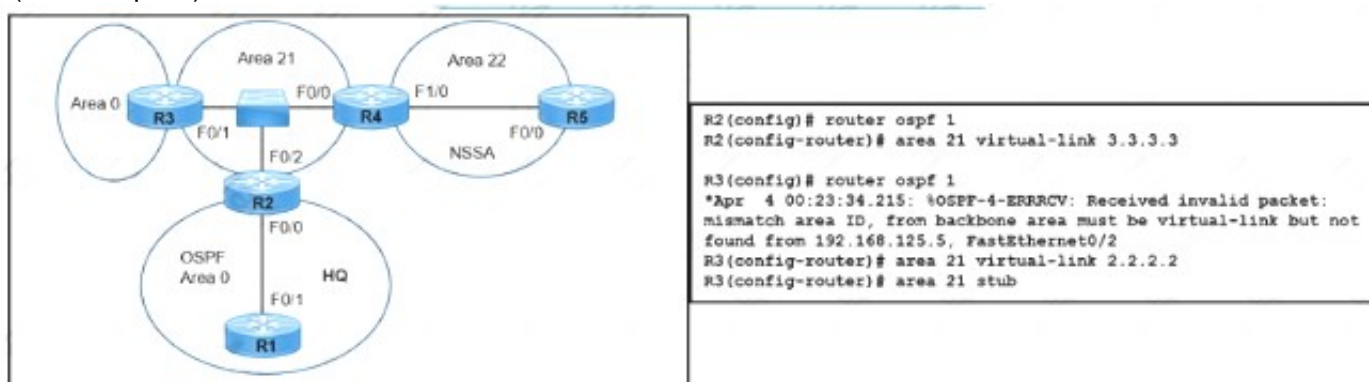
Refer to the exhibit. An administrator can log in to the device using Telnet but the attempts to log in to the same device using SSH with the same credentials fail. Which action resolves this issue?

- A. Configure SSH service on the router
- B. Configure transport input all on the VTY lines to allow SSH
- C. Configure to use the Telnet user database for SSH as well
- D. Configure the VTY lines with login local

**Answer: A**

#### NEW QUESTION 258

- (Exam Topic 3)



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

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

**Answer: D**

#### NEW QUESTION 260

- (Exam Topic 3)

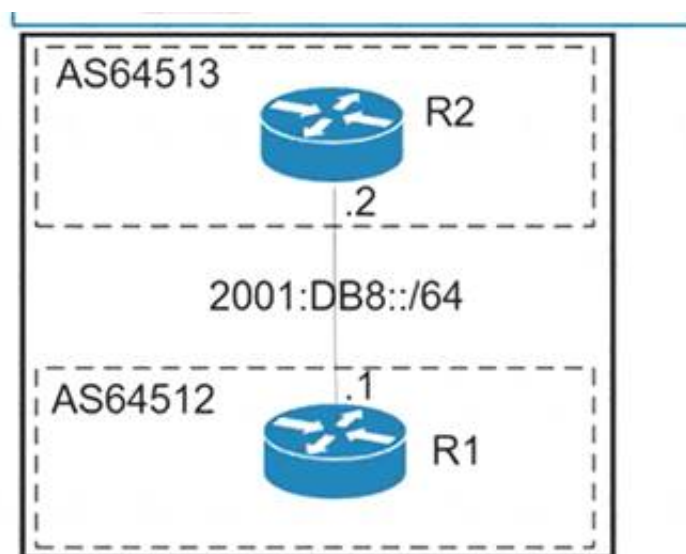
Which OSI model is used to insert an MPLS label?

- A. between Layer 5 and Layer 6
- B. between Layer 1 and Layer 2
- C. between Layer 3 and Layer 4
- D. between Layer 2 and Layer 3

**Answer: D**

#### NEW QUESTION 262

- (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 265

- (Exam Topic 3)

Refer to the exhibit.

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

An engineer must establish a point-to-point GRE VPN between R1 and the remote site. Which configuration accomplishes the task for the remote site?

- A. Interface Tunnel1 tunnel source 199.1.1.1 tunnel destination 200.1.1.3 ip address 192.168.1.3 255.255.255.0
- B. Interface Tunnel1 tunnel source 200.1.1.3 tunnel destination 199.1.1.1 ip address 192.168.1.1 255.255.255.0
- C. Interface Tunnel1 tunnel source 200.1.1.3 tunnel destination 199.1.1.1 ip address 192.168.1.3 255.255.255.0
- D. Interface Tunnel1 tunnel source 199.1.1.1 tunnel destination 200.1.1.3 ip address 192.168.1.1 255.255.255.0



**Answer:** C

**NEW QUESTION 268**

- (Exam Topic 3)

What is a MPLS PHP label operation?

- A. Downstream node signals to remove the label.
- B. It improves P router performance by not performing multiple label lookup.
- C. It uses implicit-NULL for traffic congestion from source to destination forwarding
- D. PE removes the outer label before sending to the P router.

**Answer:** A

**NEW QUESTION 269**

- (Exam Topic 3)

What are the two prerequisites to enable BFD on Cisco routers? (Choose two)

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

**Answer:** CE

**NEW QUESTION 270**

- (Exam Topic 3)

Which mechanism must be chosen to optimize the reconvergence time for OSPF at company location 407173257 that is less CPU-intensive than reducing the hello and dead timers?

- A. BFD
- B. Dead Peer Detection keepalives
- C. SSO
- D. OSPF demand circuit

**Answer:** A

**NEW QUESTION 274**

- (Exam Topic 3)

Refer to the exhibit.

```
ip address 4.4.4.4 255.255.255.0
!
interface FastEthernet1/0
Description **** WAN link ****
ip address 10.0.0.1 255.255.255.0
!
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
!
```

A)

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

B)

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

C)

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

D)

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

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

**Answer:** A

#### NEW QUESTION 279

- (Exam Topic 3)

What is a characteristic of Layer 3 MPLS VPNs?

- A. LSP signaling requires the use of unnumbered IP links for traffic engineering.
- B. Traffic engineering supports multiple IGP instances
- C. Traffic engineering capabilities provide QoS and SLAs.
- D. Authentication is performed by using digital certificates or preshared keys.

**Answer:** C

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_te\\_diffserv/configuration/15-mt/mp-te-diffserv-15-mt-bo](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_diffserv/configuration/15-mt/mp-te-diffserv-15-mt-bo)

MPLS traffic engineering supports only a single IGP process/instance

The MPLS traffic engineering feature does not support routing and signaling of LSPs over unnumbered IP links.

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp\\_te\\_path\\_setup/configuration/xe-3s/mp-te-path-setup-xe-3s-book/mp-te-enhance-xe.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_setup/configuration/xe-3s/mp-te-path-setup-xe-3s-book/mp-te-enhance-xe.html)

#### NEW QUESTION 281

- (Exam Topic 3)

Which feature is used by LDP in the forwarding path within the MPLS cloud?

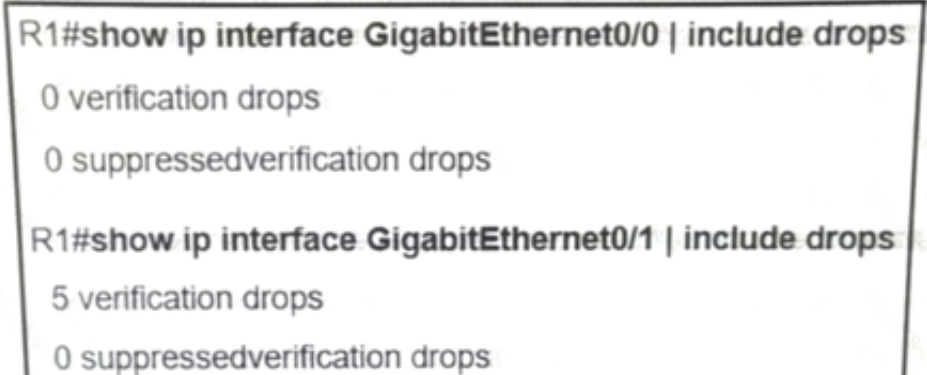
- A. IP forwarding
- B. TTL
- C. TDP
- D. LSP

**Answer:** D

#### NEW QUESTION 285

- (Exam Topic 3)

Refer to the exhibit.



```
R1#show ip interface GigabitEthernet0/0 | include drops
0 verification drops
0 suppressedverification drops

R1#show ip interface GigabitEthernet0/1 | include drops
5 verification drops
0 suppressedverification drops
```

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

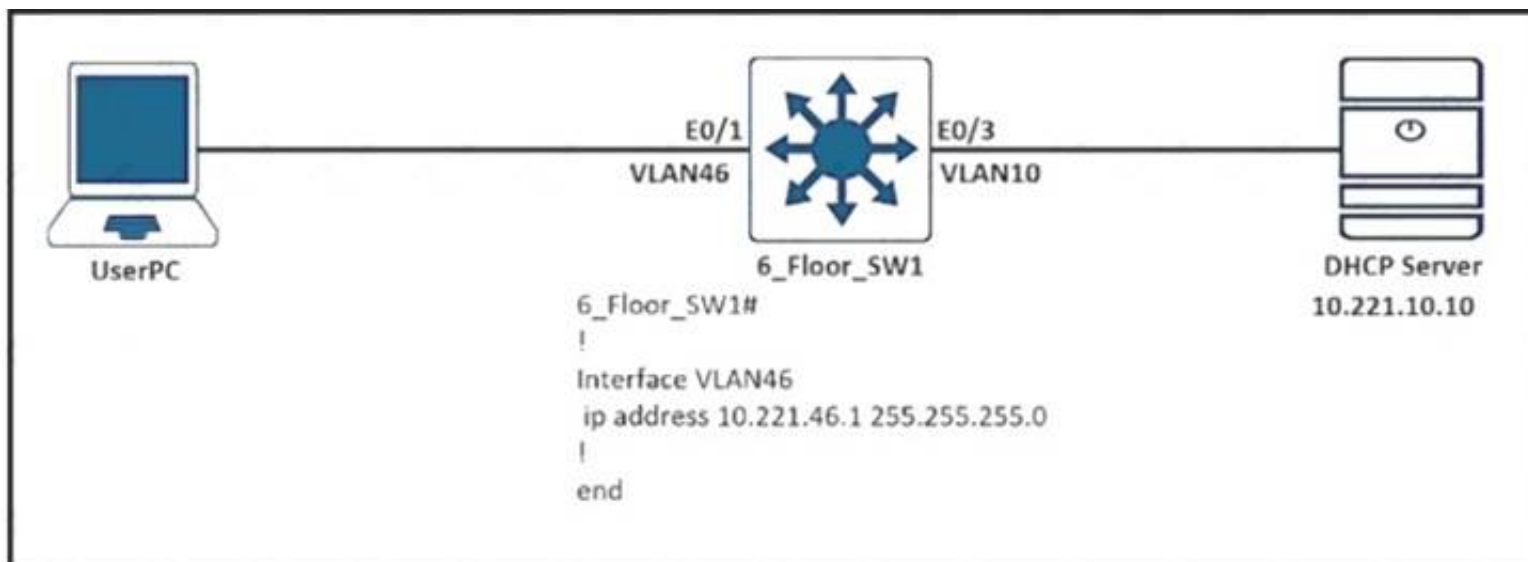
- A. Remove the access list from the interface GigabitEthernet 0/0
- B. Modify the uRPF mode from strict to loose
- C. Enable Cisco Express Forwarding to ensure that uRPF is functioning correctly
- D. Add a floating static route to the source on R1 to the GigabitEthernet 0/1 interface

**Answer:** B

#### NEW QUESTION 286

- (Exam Topic 3)

Refer to the exhibit.



Users in VLAN46 cannot get the IP from the DHCP server. Assume that all the parameters are configured properly in VLAN 10 and on the DHCP server Which command on interlace VLAN46 allows users to receive IP from the DHCP server?

- A. ip dhcp-addresses 10.221.10.10
- B. ip dhcp server 10.221.10.10
- C. ip helper-addresses 10.221.10.10
- D. ip dhcp relay information trust-all

**Answer: C**

### NEW QUESTION 290

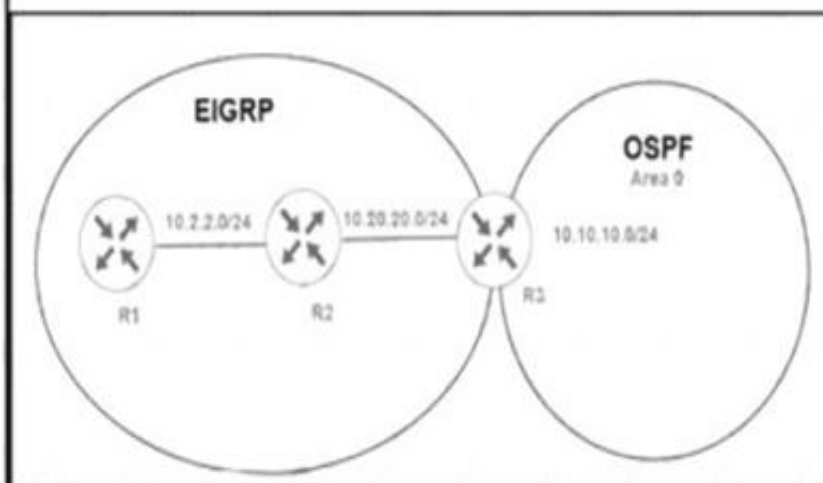
- (Exam Topic 3)

```

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 295

- (Exam Topic 3)

A newly installed spoke router is configured for DMVPN with the ip mtu 1400 command. Which configuration allows the spoke to use fragmentation with the maximum negotiated TCP MTU over GRE?

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

**Answer: A**

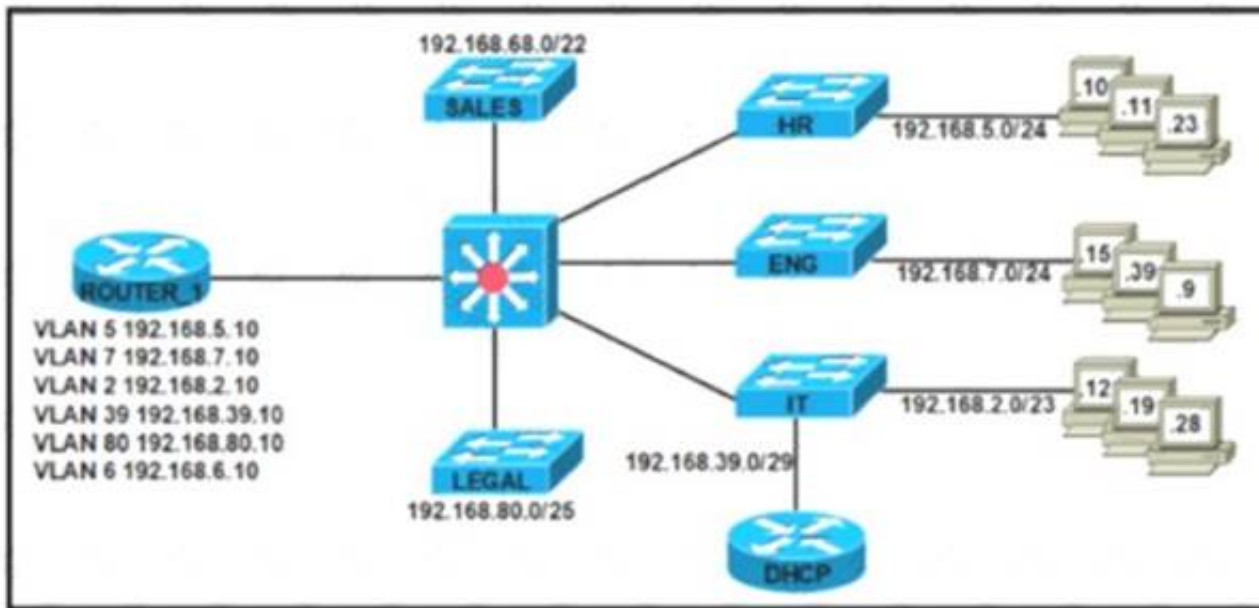
### Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot>



**NEW QUESTION 296**

- (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 299

- (Exam Topic 3)

Refer to the exhibit.

```

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

```

An administrator must configure the router with OSPF for IPv4 and IPv6 networks under a single process. The OSPF adjacencies are not established and did not

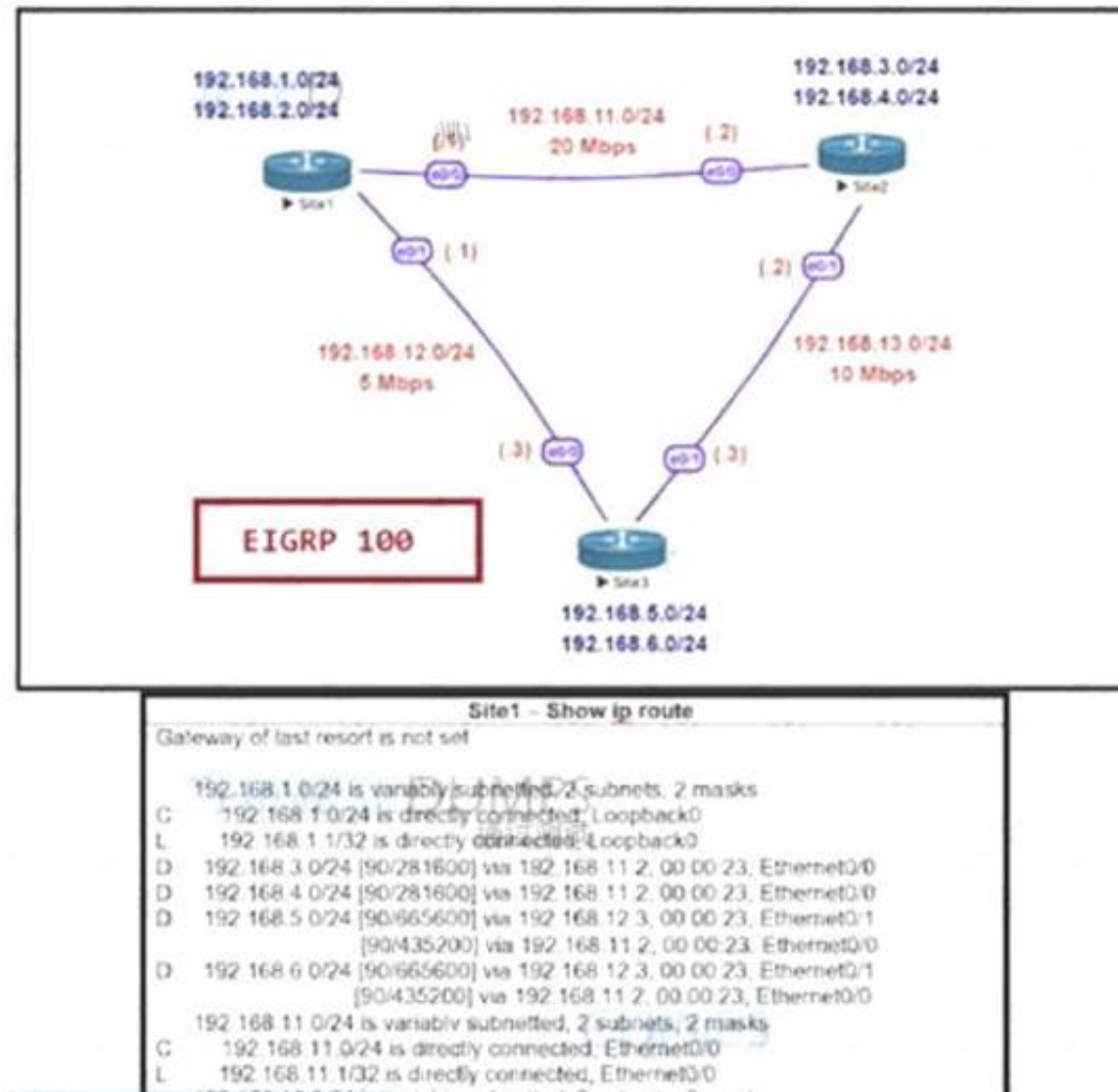
meet the requirement. Which action resolves the issue?

- A. Replace OSPF process 10 on the interface with OSPF process 1, and configure an additional router ID with IPv6 address.
- B. Replace OSPF process 10 on the interface with OSPF process 1, for the VpV6 addressma nd remove process route ID with IPv6 address.
- C. Replace OSPF process 10 on the interface with OSPF process 1, and remove process 10 from the global configuration.
- D. Replace OSPF process 10 on the interface with OSPF process 1 for the IPv4 address, and remove process 10 from the global configuration.

Answer: C

### NEW QUESTION 300

- (Exam Topic 3)



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 301

- (Exam Topic 3)

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

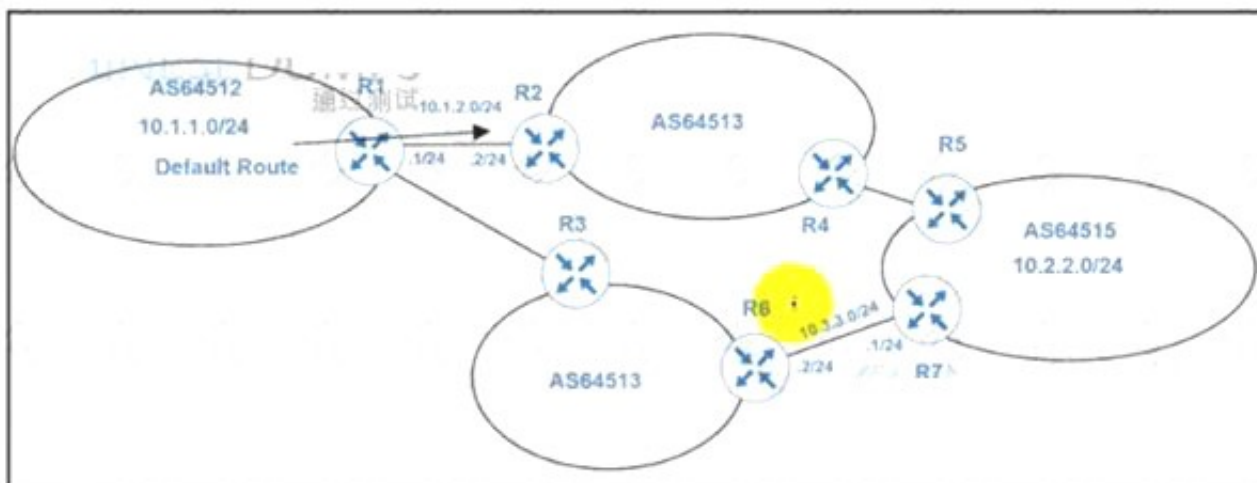
- A. label swap
- B. explicit-null
- C. label imposition
- D. PHP

**Answer:** D

### NEW QUESTION 305

- (Exam Topic 3)

Refer to the exhibit.



An engineer must configure PBR on R1 to reach to 10.2.2.0/24 via R3 AS64513 as the primary path and a backup route through default route via R2 AS64513. All BGP routes are in the routing table of R1, but a static default route overrides BGP routes. Which PBR configuration achieves the objective?

- ☒ access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255  
!  
route-map PBR permit 10  
match ip address 100  
set ip next-hop 10.3.3.1
- ☐ access-list 100 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255  
!  
route-map PBR permit 10  
match ip address 100  
set ip next-hop recursive 10.3.3.1
- ☐ access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0  
!  
route-map PBR permit 10  
match ip address 100  
set ip next-hop recursive 10.3.3.1
- ☐ access-list 100 permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0  
!  
route-map PBR permit 10  
match ip address 100  
set ip next-hop 10.3.3.1

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

**Answer:** B

#### NEW QUESTION 309

- (Exam Topic 3)

Refer to the exhibit.

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

R1 has a route map configured, which results in a loss of partial IPv6 prefixes for the BGP neighbor, resulting in service degradation. How can the full service be restored?

- A. The neighbor requires a soft reconfiguration, and this will clear the policy without resetting the BGP TCP connection.
- B. The prefix list requires all prefixes that R1 is advertising to be added to it, and this will allow additional prefixes to be advertised.
- C. The route map requires a deny 20 statement without set conditions, and this will allow additional prefixes to be advertised.
- D. The route map requires a permit 20 statement without set conditions, and this will allow additional prefixes to be advertised.

**Answer:** D

#### NEW QUESTION 311

- (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 315

- (Exam Topic 3)

```
Router#show ip bgp vpnv4 rd 1100:1001 10.30.116.0/23
BGP routing table entry for 1100:1001:10.30.116.0/23, version 26765275
Paths: (9 available, best #6, no table)
Advertised to update-groups:
 1      2      3
(65001 64955 65003) 65089, (Received from a RR-client)
 172.16.254.226 (metric 20645) from 172.16.224.236 (172.16.224.236)
  Origin IGP, metric 0, localpref 100, valid, confed-internal
  Extended Community: RT: 1100:1001
  mpls labels in/out 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-internal
  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-internal
  Extended Community: RT: 1100:1001
  mpls labels in/out no-label/278
```

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

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

**Answer: D**

#### NEW QUESTION 318

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

**Answer: D**



**NEW QUESTION 319**

- (Exam Topic 3)

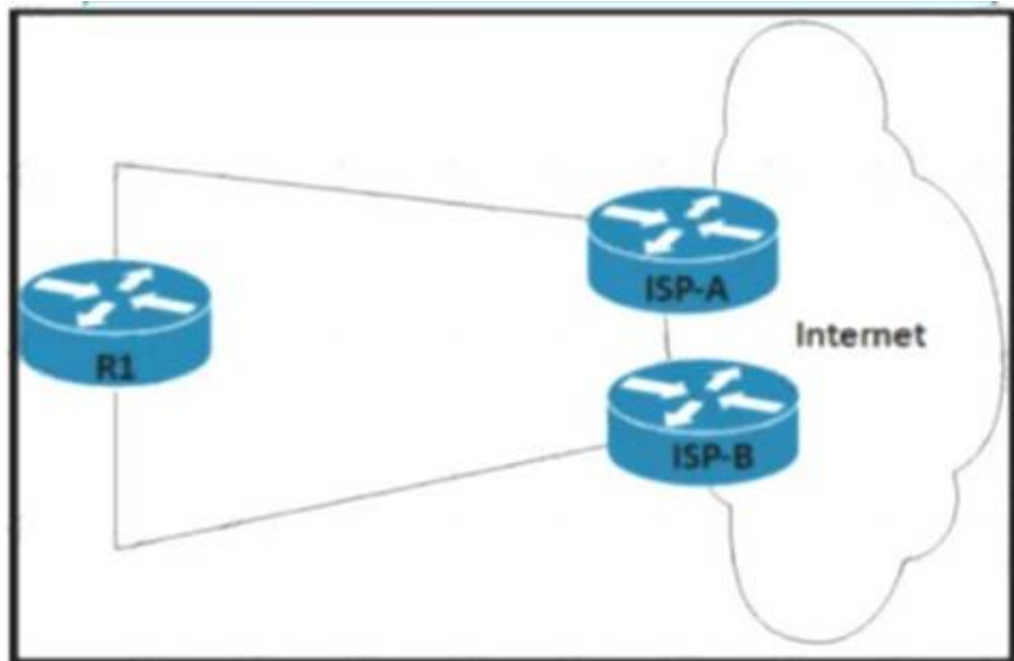
Which routing protocol is used by the PE router to advertise routes to a CE router without redistribution or static after removing the RD tag from the P router?

- A. IS-IS
- B. OSPF
- C. BGPIPV4
- D. MP-BGP

**Answer: C**

**NEW QUESTION 321**

- (Exam Topic 3)



Refer to the exhibit. Router R1 peers with two ISPs using static routes to get to the internet. The requirement is that R1 must prefer ISP-A under normal circumstances and failover to ISP-B if the connectivity to ISP-A is lost. The engineer observes that R1 is load balancing traffic across the two ISPs Which action resolves the issue by sending traffic to ISP-A only with failover to ISP-B?

- A. Configure OSPF between R1, ISP-
- B. and ISP-B for dynamic failover if any ISP link to R1 fails
- C. Configure two static routes on R1. one pointing to ISP-A and another pointing to ISP- B with 222 admin distance
- D. Change the bandwidth of the interface on R1 so that interface to ISP-A has a higher value than the interface to ISP-B
- E. Configure two static routes on R1. one pointing to ISP-B with more specific routes and another pointing to ISP-A with summary routes

**Answer: D**

**NEW QUESTION 322**

- (Exam Topic 3)

What does the MP-BGP OPEN message contain?

- A. MPLS labels and the IP address of the router that receives the message
- B. the version number and the AS number to which the router belongs
- C. IP routing information and the AS number to which the router belongs
- D. NLRI, path attributes, and IP addresses of the sending and receiving routers

**Answer: B**

**NEW QUESTION 323**

- (Exam Topic 3)

How is a preshared key "Test" for all the remote VPN routers configured In a DMVPN using GRE over IPsec set up?

- A. authentication pre-share Test address 0.0.0.0 0.0.0.0
- B. set pre-share Test address 0.0.0.0 0.0.0.0
- C. crypto Ipsec key Test address 0.0.0.0 0.0.0.0
- D. crypto isakmp key Test address 0.0.0.0 0.0.0.0

**Answer: D**

**NEW QUESTION 326**

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

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

**Answer:** C

#### NEW QUESTION 328

- (Exam Topic 3)

Refer to the exhibit.

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

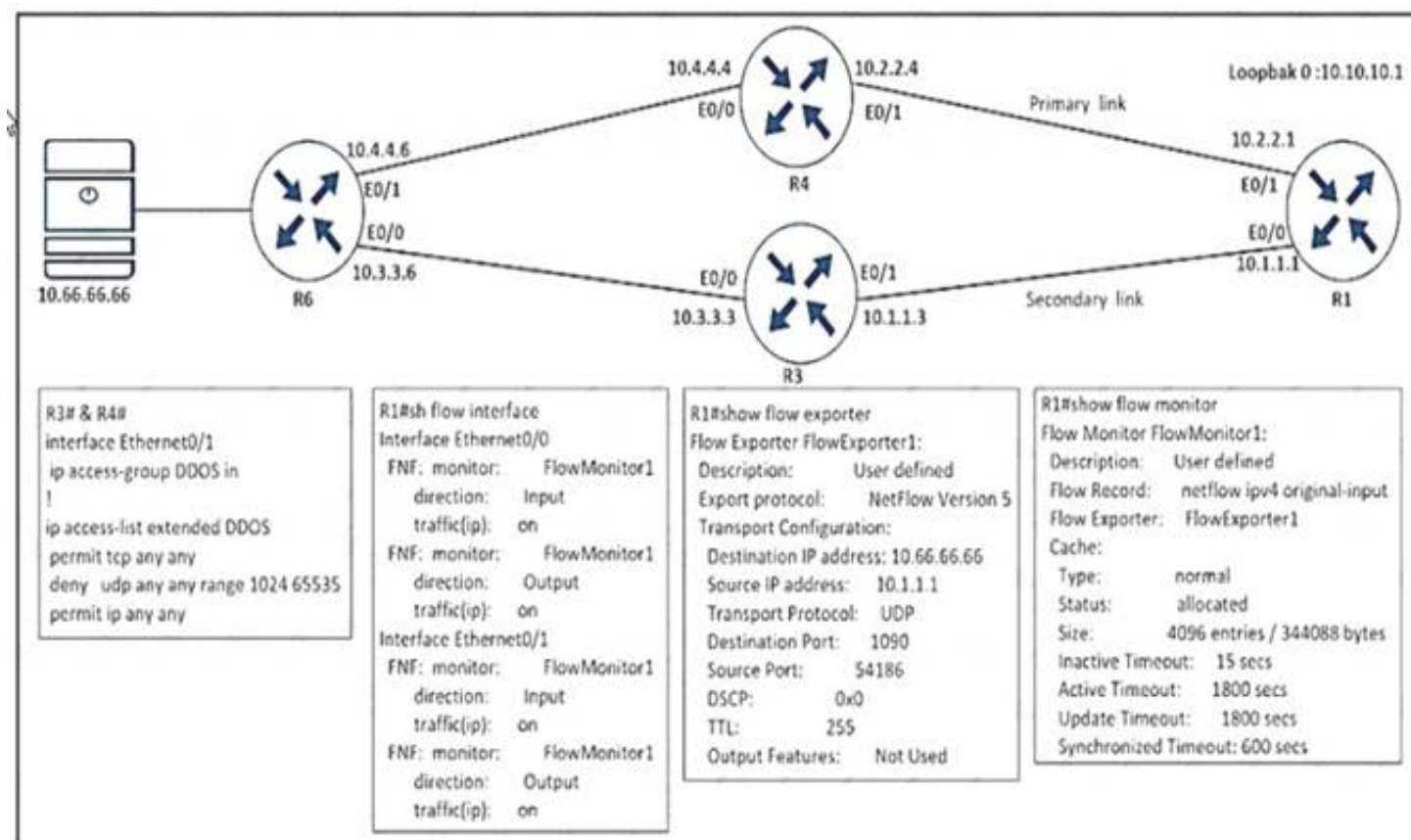
The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

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

**Answer:** D

#### NEW QUESTION 332

- (Exam Topic 3)



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

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

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

C)  
**R3(config)#flow exporter FlowExporter1**  
**R3(config-flow-exporter)#destination 10.66.66.66**

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

E)  
**R4(config)#flow exporter FlowExporter1**  
**R4(config-flow-exporter)#destination 10.66.66.66**

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

**Answer: BE**

#### NEW QUESTION 334

- (Exam Topic 3)

A network administrator is troubleshooting a high utilization issue on the route processor of a router that was reported by NMS The administrator logged into the router to check the control plane policing and observed that the BGP process is dropping a high number of routing packets and causing thousands of routes to recalculate frequently. Which solution resolves this issue?

- A. Police the cir for BGP, conform-action transmit, and exceed action transmit.
- B. Shape the pir for BGP, conform-action set-prec-transmit, and exceed action set-frde-transmit.
- C. Shape the cir for BG
- D. conform-action transmit, and exceed action transmit.
- E. Police the pir for BGP, conform-action set-prec-transmit, and exceed action set-clp-transmit.

**Answer: D**

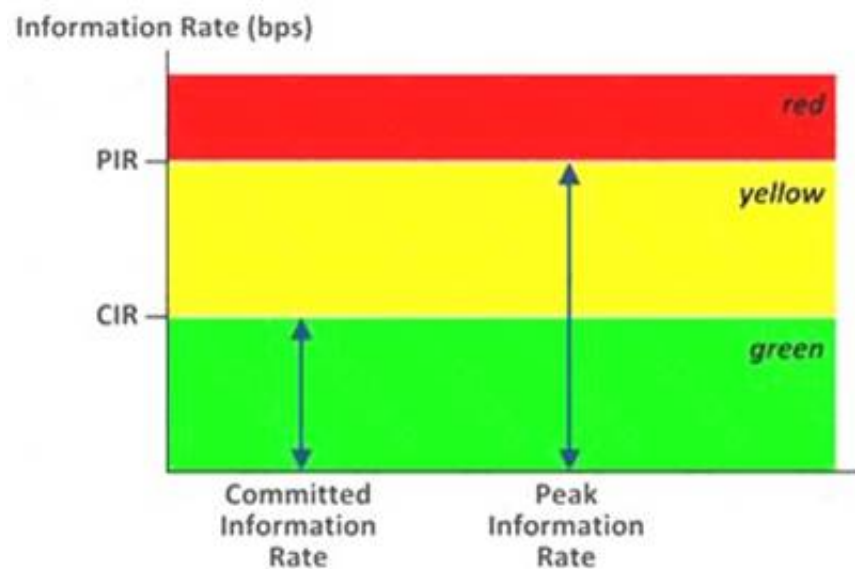
#### Explanation:

CIR (Committed Information Rate) is the minimum guaranteed traffic delivered in the network.

PIR (Peak Information Rate) is the top bandwidth point of allowed traffic in a non busy times without any guarantee.

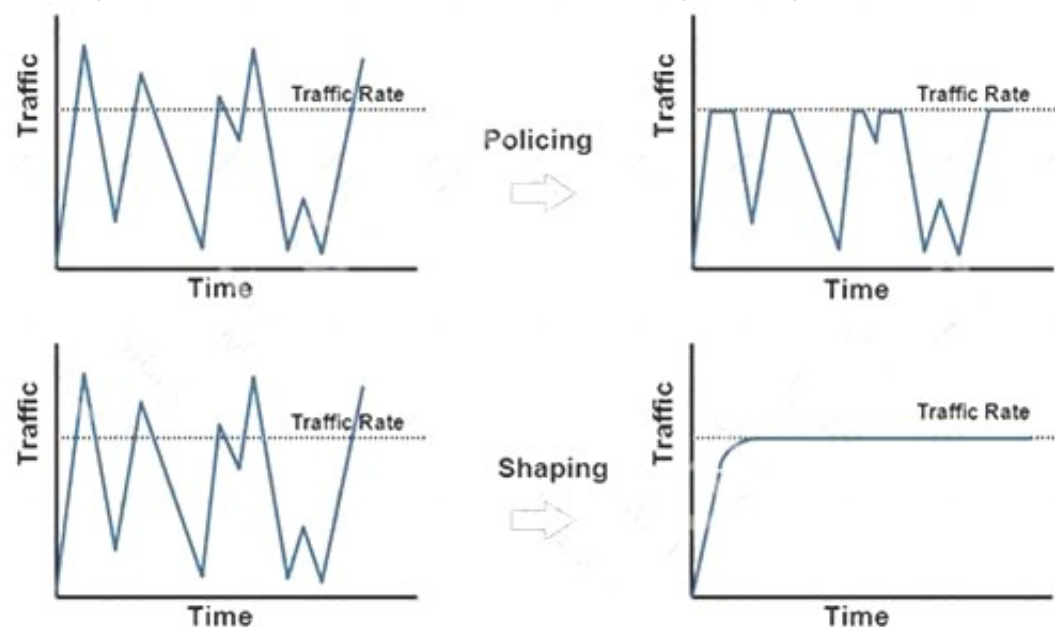


## Two Rates & Three Colors



+ Policing: is used to control the rate of traffic flowing across an interface. During a bandwidth exceed (crossed the maximum configured rate), the excess traffic is generally dropped or remarked. The result of traffic policing is an output rate that appears as a saw-tooth with crests and troughs. Traffic policing can be applied to inbound and outbound interfaces. Unlike traffic shaping, QoS policing avoids delays due to queuing. Policing is configured in bytes.

+ Shaping: retains excess packets in a queue and then schedules the excess for later transmission over increments of time. When traffic reaches the maximum configured rate, additional packets are queued instead of being dropped to proceed later. Traffic shaping is applicable only on outbound interfaces as buffering and queuing happens only on outbound interfaces. Shaping is configured in bits per second.



Therefore in this case we can only policing, not shaping as traffic shaping is applicable only on outbound interfaces as buffering and queuing happens only on outbound interfaces. Moreover, BGP traffic is not important so we can drop the excess packets without any problems.

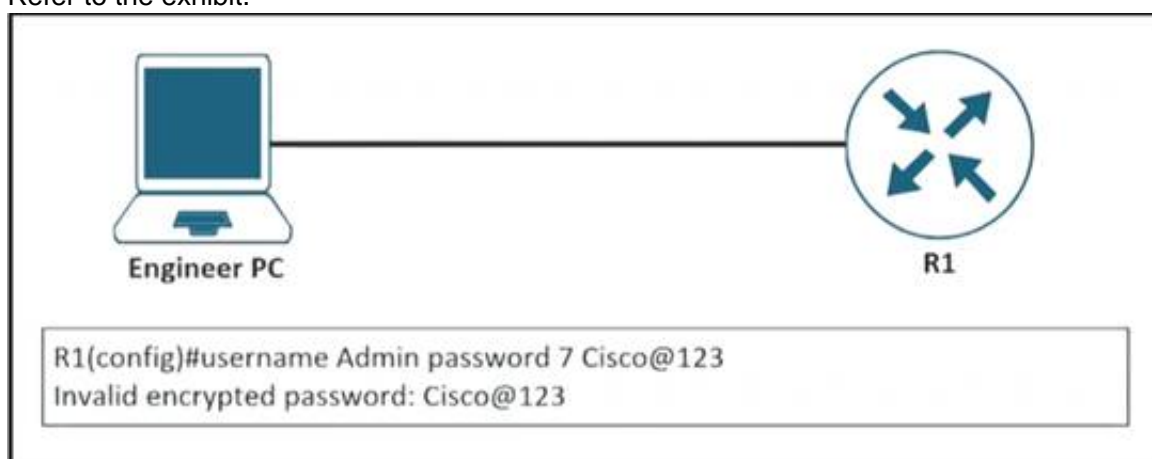
And we only policing the PIR traffic so that the route processor is not overwhelmed by BGP calculation.

Note: The "set-prec-transmit" is the same as "transmit" command except it sets the IP Precedence level as well. The "set-clp-transmit" sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet.

### NEW QUESTION 339

- (Exam Topic 3)

Refer to the exhibit.



An engineer is trying to add an encrypted user password that should not be visible in the router configuration. Which two configuration commands resolve the issue? (Choose two)

- A. password encryption aes
- B. username Admin password Cisco@maedeh motamedi
- C. username Admin password 5 Cisco@maedeh motamedi
- D. username Admin secret Cisco@maedeh motamedi
- E. no service password-encryption
- F. service password-encryption

**Answer:** DF

### NEW QUESTION 342

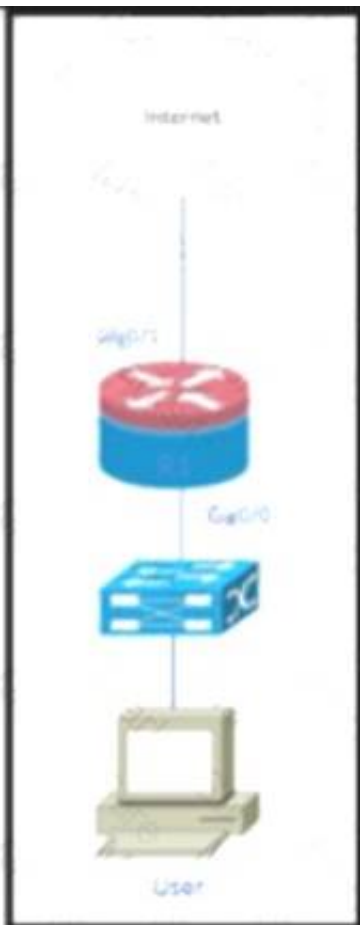
- (Exam Topic 3)

```
R1#show time-range

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

R1#show ip access-list interface gig0/0

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



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

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

B)

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

C)

```
no time-range timer
```

D)

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

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

**Answer: D**

#### NEW QUESTION 347

- (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 10.10.10.0/24 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
- B. Option
- C. Option
- D. Option



Answer: C

#### NEW QUESTION 348

- (Exam Topic 3)

Refer to the exhibit.

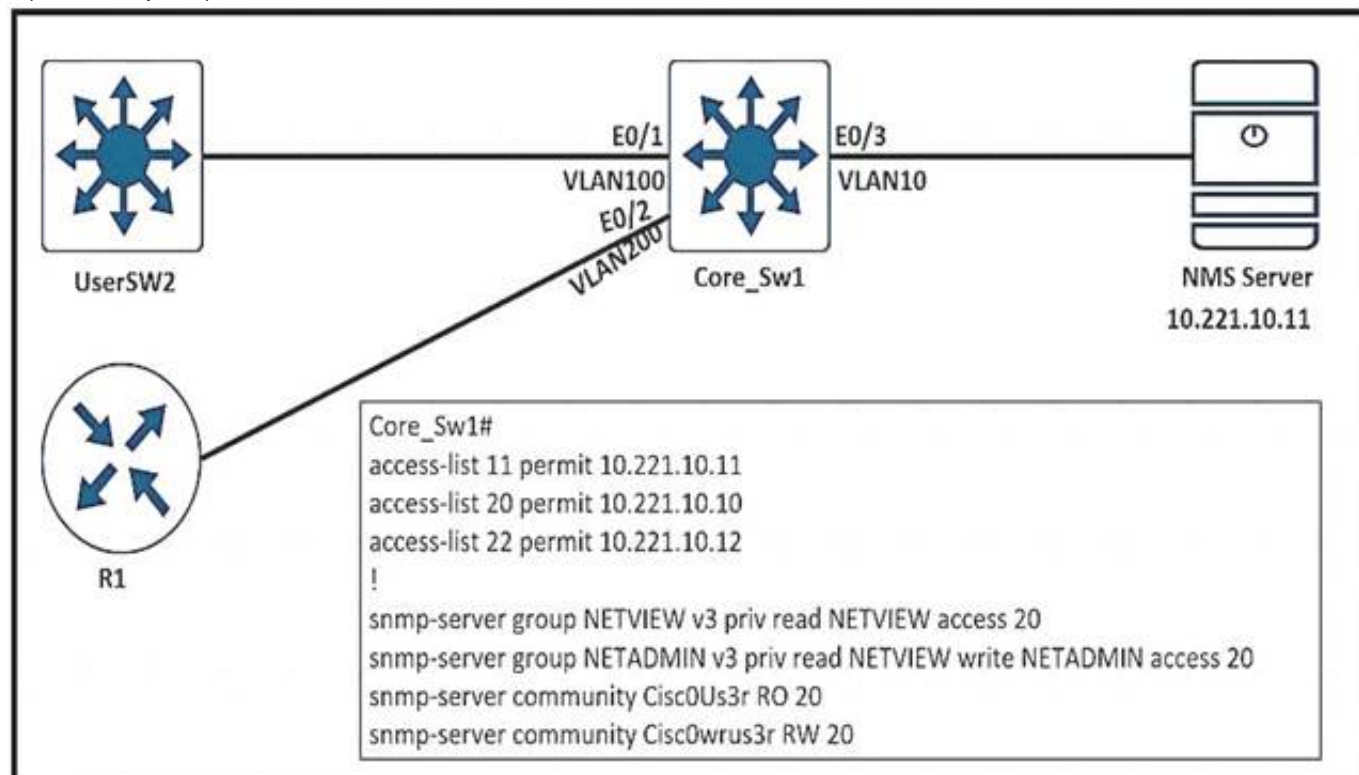
A network engineer receives a fault ticket about traffic drops from BANK SITE to BANK Users can reach BANK SITE Y from router RA as a source. Routers RB and RD are acting as route reflectors. Which configuration resolves the issue?

- 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 349

- (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 353

- (Exam Topic 3)

```

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

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

access-list 16 permit 10.1.1.2
  
```

Refer to the exhibit Which action resolves the issue?

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

Answer: D

#### NEW QUESTION 357

- (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 359

- (Exam Topic 3)

IPv6 is enabled in the infrastructure to support customers with an IPv6 network over WAN and to connect the head office to branch offices in the local network. One of the customers is already running IPv6 and wants to enable IPv6 over the DMVPN network infrastructure between the headend and branch sites. Which configuration command must be applied to establish an mGRE IPv6 tunnel neighborhood?

- A. tunnel protection mode ipv6
- B. ipv6 unicast-routing
- C. ipv6 nhrp holdtime 30
- D. tunnel mode gre multipoint ipv6

**Answer: D**

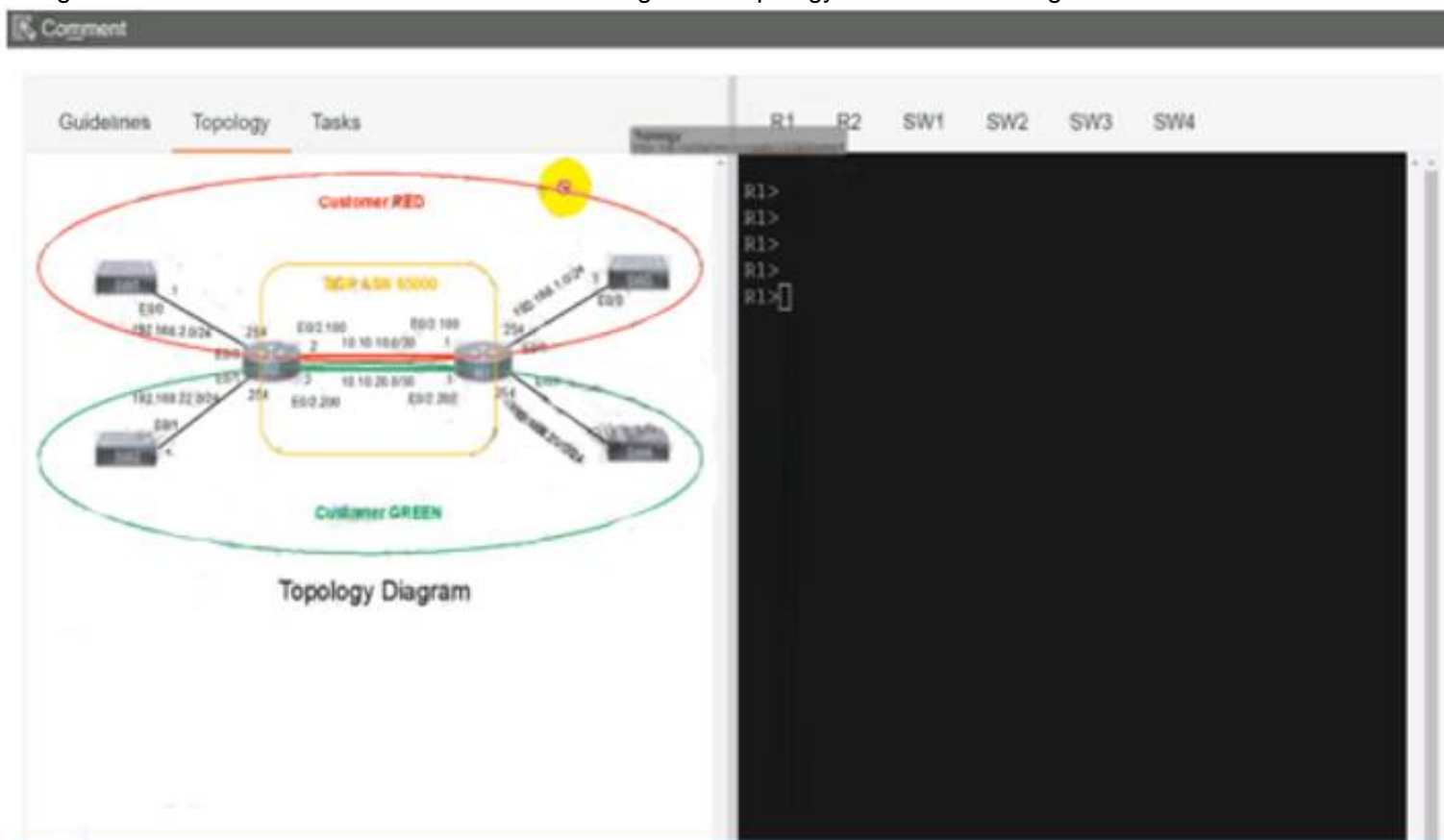
#### Explanation:

The command “tunnel mode gre multipoint ipv6 ” sets the encapsulation mode of the tunnel to mGRE IPv6.

#### NEW QUESTION 363

- (Exam Topic 3)

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



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
!
!

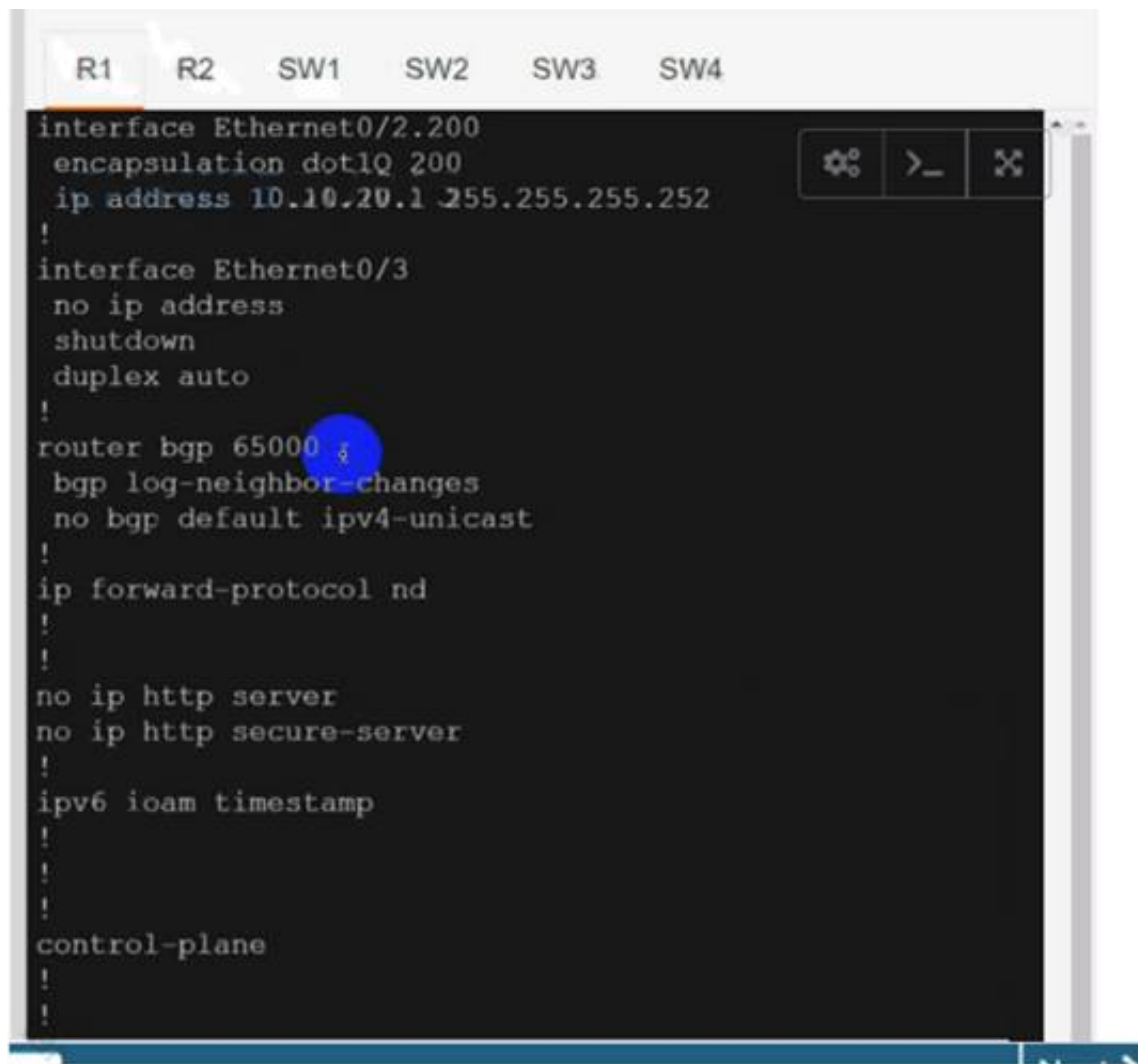
```



```

R1      R2      SW1      SW2      SW3      SW4
!
!
!
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.1.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.20.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/2.100
 encapsulation dot1Q 100
 ip address 10.10.10.1 255.255.255.252
!
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.1 255.255.255.252

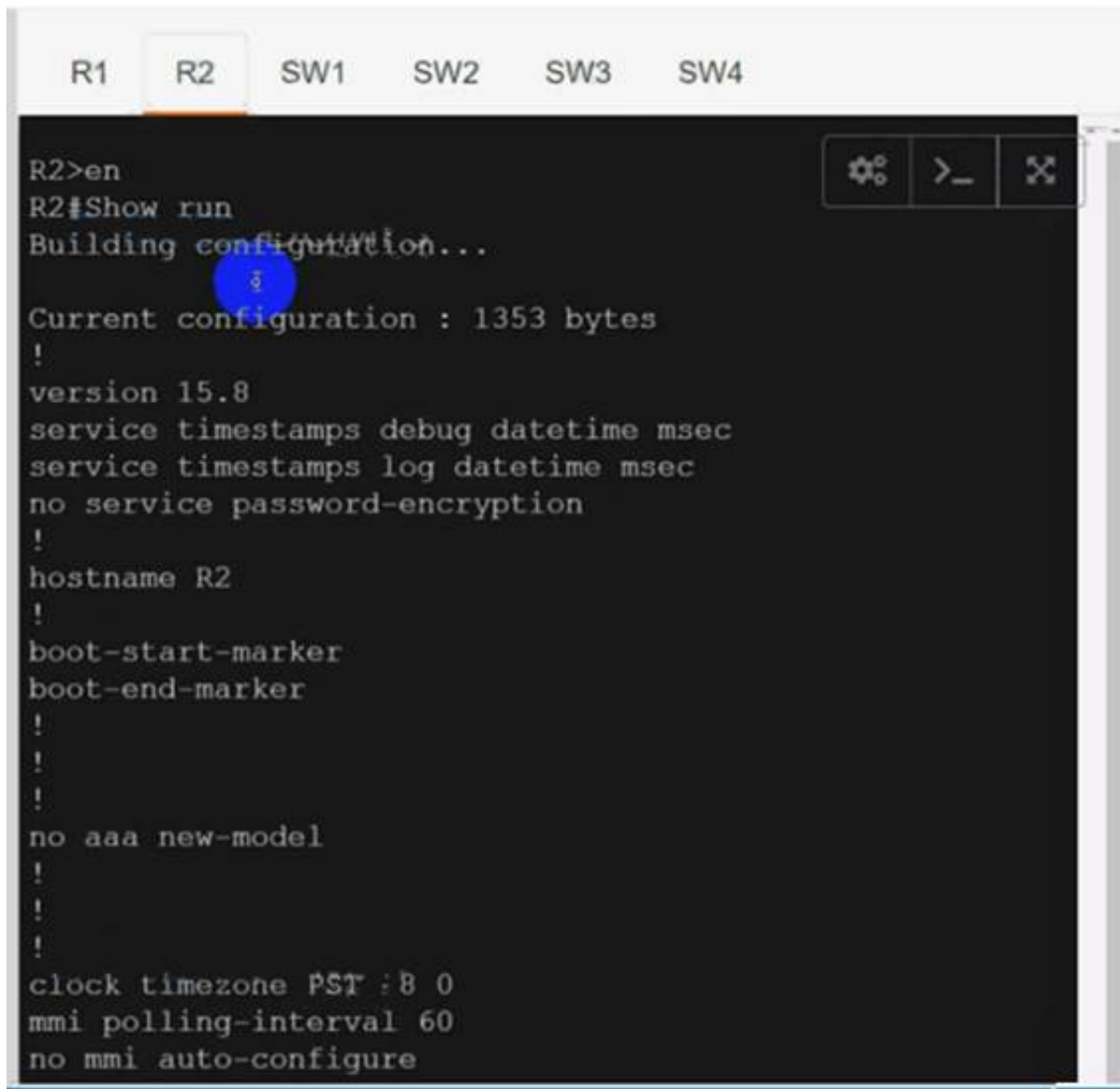
```



A screenshot of a Cisco IOS configuration window for router R1. The window has tabs for R1, R2, SW1, SW2, SW3, and SW4. The R1 tab is selected. The configuration text is as follows:

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

R2



A screenshot of a Cisco IOS configuration window for router R2. The window has tabs for R1, R2, SW1, SW2, SW3, and SW4. The R2 tab is selected. The configuration text is as follows:

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

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

```

R1  R2  SW1  SW2  SW3  SW4
!
!
!
!
interface Loopback0
 ip address 10.10.2.2 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.2.254 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.22.254 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 no ip address
 duplex auto
!
interface Ethernet0/2.100
 encapsulation dot1Q 100
 ip address 10.10.10.2 255.255.255.252
!
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252

```



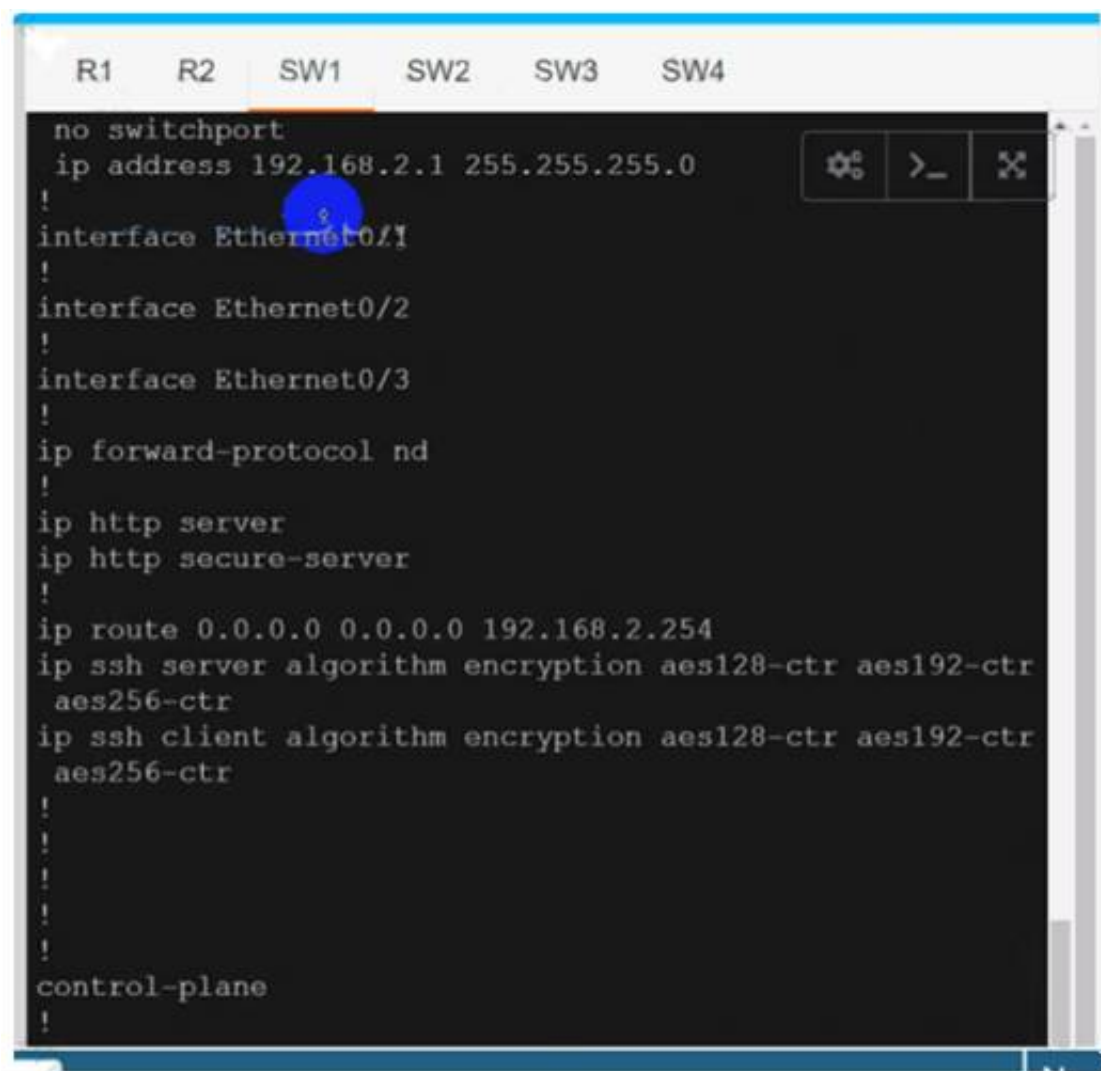
```
R1  R2  SW1  SW2  SW3  SW4
interface Ethernet0/2.200
 encapsulation dot1Q 200
 ip address 10.10.20.2 255.255.255.252
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
router bgp 65000
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
!
ip forward-protocol nd
!
!
no ip http server
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

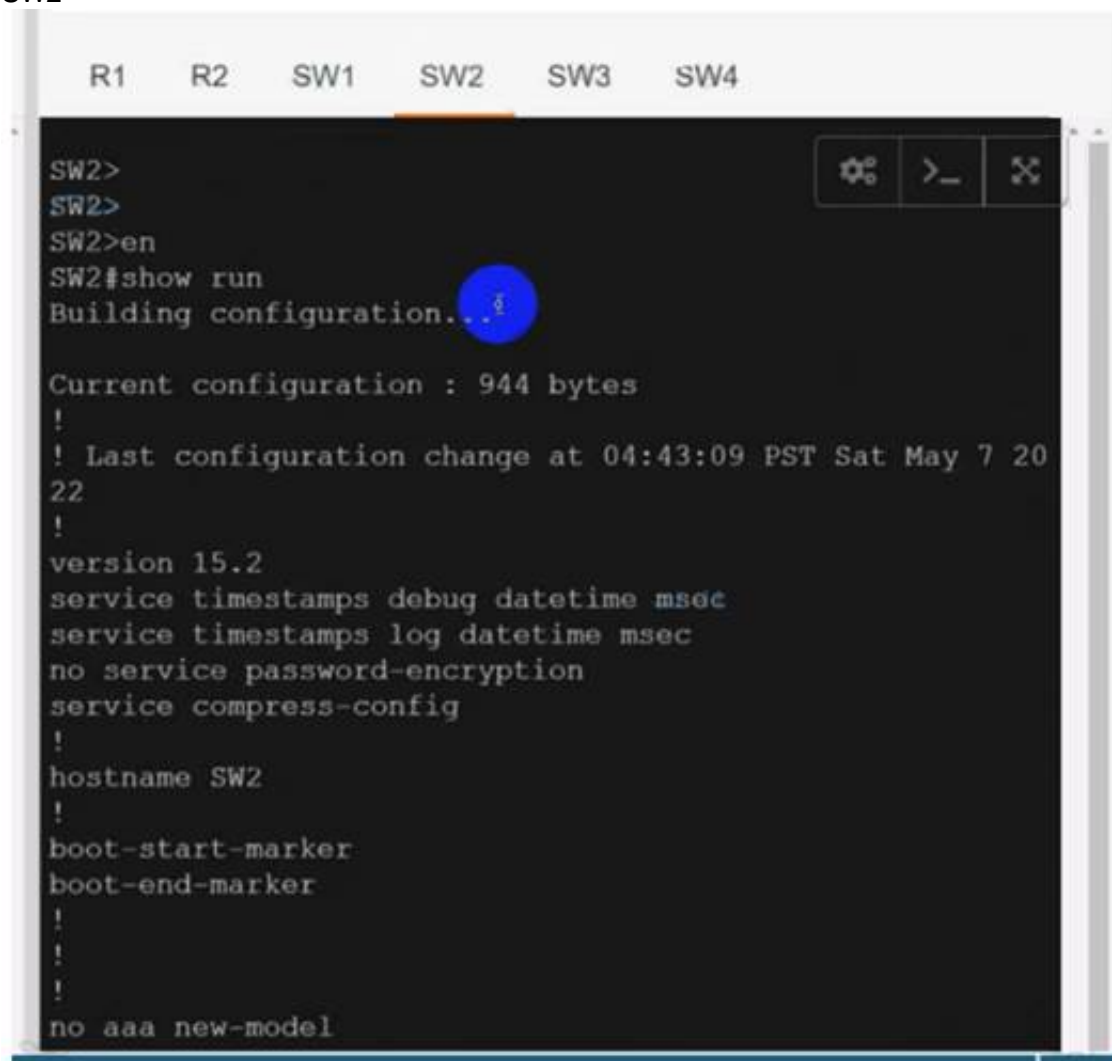
The screenshot shows a network configuration interface with tabs for R1, R2, SW1, SW2, SW3, and SW4. The SW1 tab is active. A terminal window displays the following commands:

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

A screenshot of a Cisco IOS configuration window for switch SW1. The window has tabs for R1, R2, SW1 (selected), SW2, SW3, and SW4. The configuration text is as follows:

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

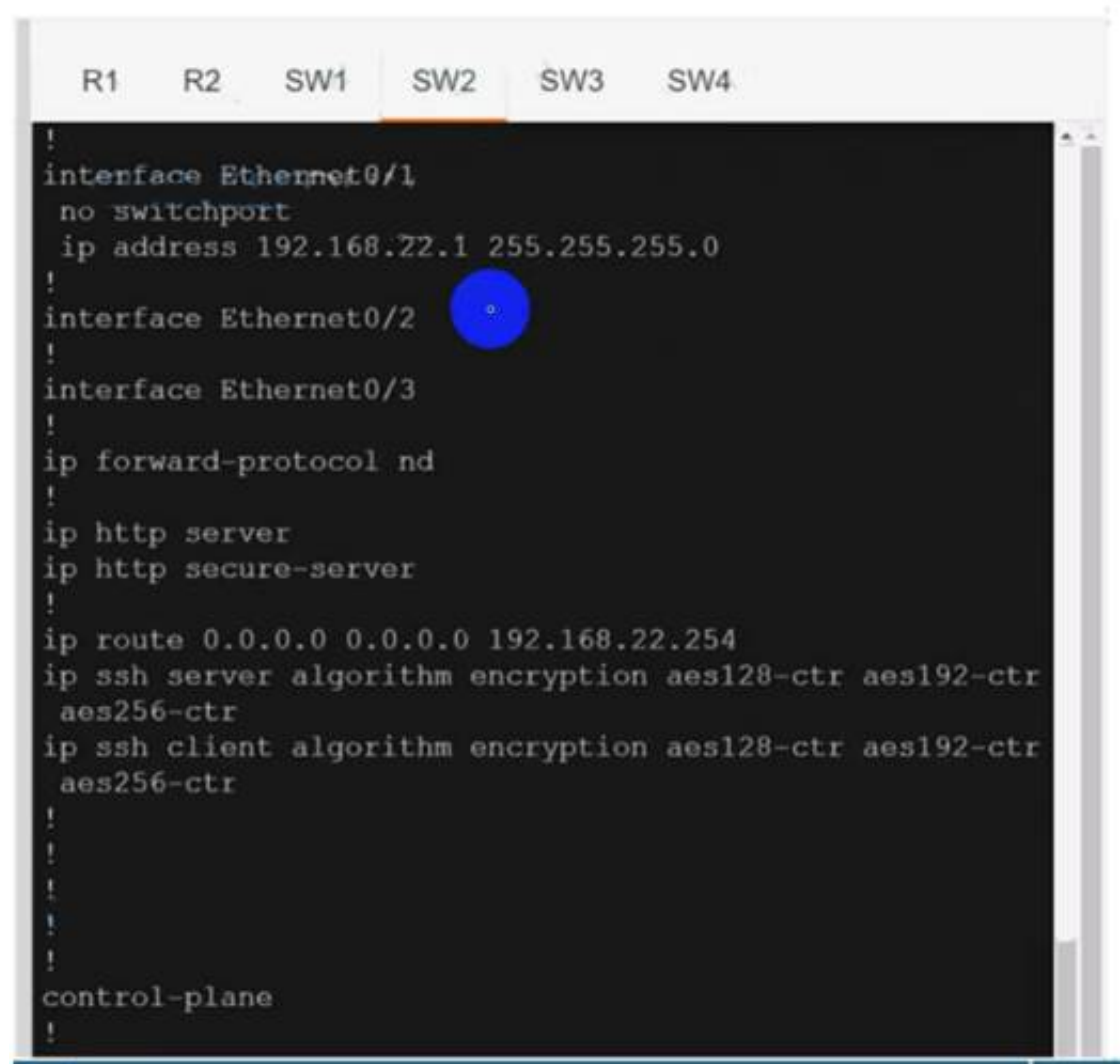
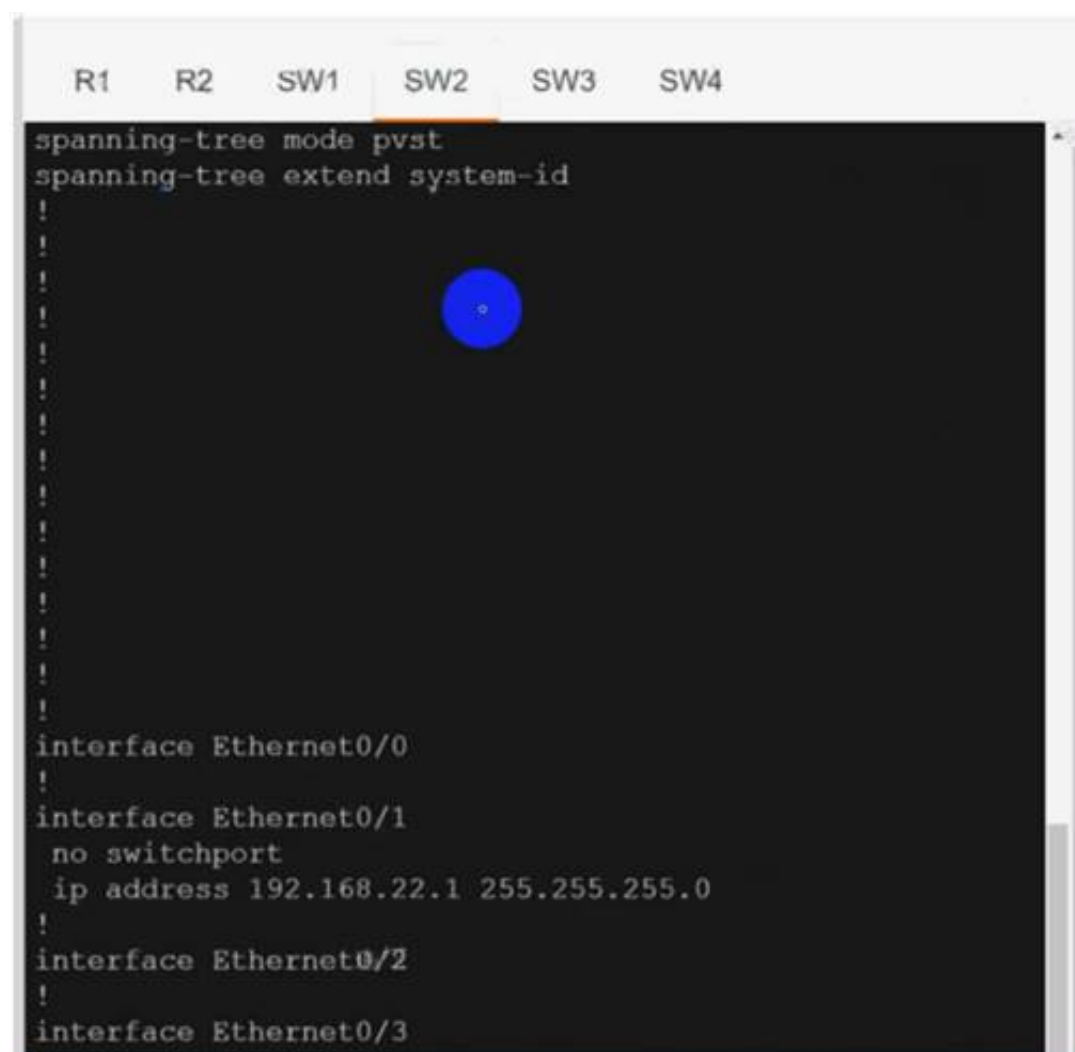
SW2

A screenshot of a Cisco IOS configuration window for switch SW2. The window has tabs for R1, R2, SW1, SW2 (selected), SW3, and SW4. The configuration text is as follows:

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

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





SW3

```
R1      R2      SW1      SW2      SW3      SW4  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
no switchport  
ip address 192.168.1.1 255.255.255.0  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
!  
interface Ethernet0/3
```

```
R1  R2  SW1  SW2  SW3  SW4
no switchport
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip ssh server algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr
aes256-ctr
!
!
!
!
!
control-plane
!
```

```
R1  R2  SW1  SW2  SW3  SW4
SW4>en
SW4#show run
Building configuration...

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




```
R1    R2    SW1    SW2    SW3    SW4
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
 no switchport
 ip address 192.168.20.1 255.255.255.0
!
interface Ethernet0/2
!
interface Ethernet0/3
```

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

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.

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Solution:

➤ Use cu-red under interfaces facing SW1 & SW3:

On R1:

```
interface Ethernet0/0
```

```
ip vrf forwarding cu-red
```

```
ip address 192.168.1.254 255.255.255.0
```

Check reachability to SW1: R1#ping vrf cu-red 192.168.1.1 Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On R2:

```
interface Ethernet0/0
```

```
ip vrf forwarding cu-red
```

```
ip address 192.168.2.254 255.255.255.0
```

Check reachability to SW3: R2#ping vrf cu-red 192.168.2.1 Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!

➤ Use vrf cu-green for SW2 & SW4:

On R1:

```
interface Ethernet0/1
```

```
ip vrf forwarding cu-green
```

```
ip address 192.168.20.254 255.255.255.0
```

Test reachability to SW2: R1#ping vrf cu-green 192.168.20.1 Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

On R2:

```
interface Ethernet0/1
```

```
ip vrf forwarding cu-green
```

```
ip address 192.168.22.254 255.255.255.0
```

Test reachability to SW4: R2#ping vrf cu-green 192.168.22.1 Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

➤ On R1:

```
interface Ethernet0/2.100 mpls ip
```

```
!
```

```
interface Ethernet0/2.200 mpls ip
```

```
!
```

Configure BGP:

```
router bgp 65000
```

```
neighbor 10.10.10.2 remote-as 65000
```

```
neighbor 10.10.20.2 remote-as 65000
```

```
!
```

```
address-family vpnv4 neighbor 10.10.10.2 activate
```

```
neighbor 10.10.20.2 activate exit-address-family
```

```
!
```

```
address-family ipv4 vrf cu-green redistribute connected
```

```
exit-address-family
```

```
!
```

```
address-family ipv4 vrf cu-red redistribute connected
```

```
exit-address-family
```

```
!
```

```
R1(config)#ip vrf cu-red
```

```
R1(config-vrf)#route-target both 65000:100
```

```
!
```

```
R1(config)#ip vrf cu-green
```

```
R1(config-vrf)#route-target both 65000:200
```

➤ On R2:

```
interface Ethernet0/2.100
```

```
mpls ip
```

```
!
```

```
interface Ethernet0/2.200 mpls ip
```

```
!
```

```
router bgp 65000
```

```
neighbor 10.10.10.1 remote-as 65000
```

```
neighbor 10.10.20.1 remote-as 65000
```

```
!
```

```
address-family vpnv4 neighbor 10.10.10.1 activate
```

```
neighbor 10.10.20.1 activate exit-address-family
```

```
!
```

```
address-family ipv4 vrf cu-green redistribute connected
```

```
exit-address-family
```

```
!
```

```
address-family ipv4 vrf cu-red redistribute connected
```

```
exit-address-family R2(config)#ip vrf cu-red
R2(config-vrf)#route-target both 65000:100
!
R2(config)#ip vrf cu-green
R2(config-vrf)#route-target both 65000:200
> Verification:
From SW1 to SW3: SW1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW2 or SW4 in VRF cu-green: SW1#ping 192.168.22.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
SW1#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
Same Test for SW2: From SW2 to SW4: SW2#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
But can't Reach SW3 or SW1 in VRF cu-red: SW2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
SW2#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds: U.U.U
Success rate is 0 percent (0/5)
Both R1 & R2 has separate tables for VRFs cu-red and cu-green.
```

**NEW QUESTION 366**

- (Exam Topic 3)

Refer to the exhibit.

```
*17:40:07.826: AAA/BIND(00000055): Bind i/f
*17:40:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*17:40:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*17:40:07.826: TPLUS: TPLUS(00000055) login timer started 1020 sec timeout
*17:40:07.826: TPLUS: processing authentication start request id 85
*17:40:07.826: TPLUS: Authentication start packet created for 850
*17:40:07.826: Using server 10.106.60.182
*17:40:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*17:40:07.830: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.830: TPLUS(00000055)/0/READ: Would block while reading
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*17:40:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*17:40:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*17:40:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

An engineer is troubleshooting a TACACS problem. Which action resolves the issue?

- A. Configure a matching TACACS server IP.
- B. Configure a matching preshared key.
- C. Generate authentication from a relative source interface.
- D. Apply a configured AAA profile to the VTY.

**Answer: B**

**Explanation:**

Reference:

<https://community.cisco.com/t5/network-access-control/issues-with-tacacs-authentication/td-p/3412001> The last line shows us the reason, which is "Invalid AUTHEN packet (check keys)" so the most likely cause of this problem is key mismatch.

**NEW QUESTION 369**

- (Exam Topic 3)



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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated with medium confidence

**NEW QUESTION 372**

- (Exam Topic 3)

```
CPE# show ip route static
<output omitted>
S* 0.0.0.0/0 is directly connected, Dialer0
S 198.51.100.0/24 [1/0] via 192.168.1.1
S 203.0.113.0/24 [1/0] via 192.168.2.1

CPE# show run | section router ospf
router ospf 1
 redistribute static subnets

CPE# show ip ospf database | begin Type-5
Type-5 AS External Link States

Link ID      ADV Router   Age         Seq#         Checksum Tag
198.51.100.0 192.168.0.1  14          0x80000001  0x0007D0 0
203.0.113.0  192.168.0.1  14          0x80000001  0x009C5C 0
```

Refer to the exhibit. The default route is not advertised to the neighboring router. Which action resolves the issue?

- A. Configure the redistribute static metric 200 subnets command under OSPF.
- B. Configure OSPF on the Dialer0 interface.
- C. Configure the network 0.0.0.0 255.255.255.255 area 0 command under OSPF.
- D. Configure the default-information originate command under OSPF.

**Answer:** D

**NEW QUESTION 376**

- (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 379**

- (Exam Topic 3)

Refer to the exhibit.

```
R2#sh ip route
Codes: 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

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, Serial1/0
C    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C    172.16.160.0/19 is directly connected, Loopback1
C    172.16.128.0/19 is directly connected, Loopback0
C    172.16.224.0/19 is directly connected, Loopback3
C    172.16.192.0/19 is directly connected, Loopback2
D    172.16.0.0/16 is a summary, 00:01:27, Null0
```

An engineer must configure EIGRP between R1 and R2 with no summary route. Which configuration resolves the issue?

A)

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
```

B)

```
R2 (config)#router eigrp 1
R2 (config-router)#no auto-summary
```

C)

```
R2 (config)#router eigrp 1
R2 (config-router)#auto-summary
```

D)

```
R1(config)#router eigrp 1
R1(config-router)#auto-summary
```

A. Option A

B. Option B

C. Option C

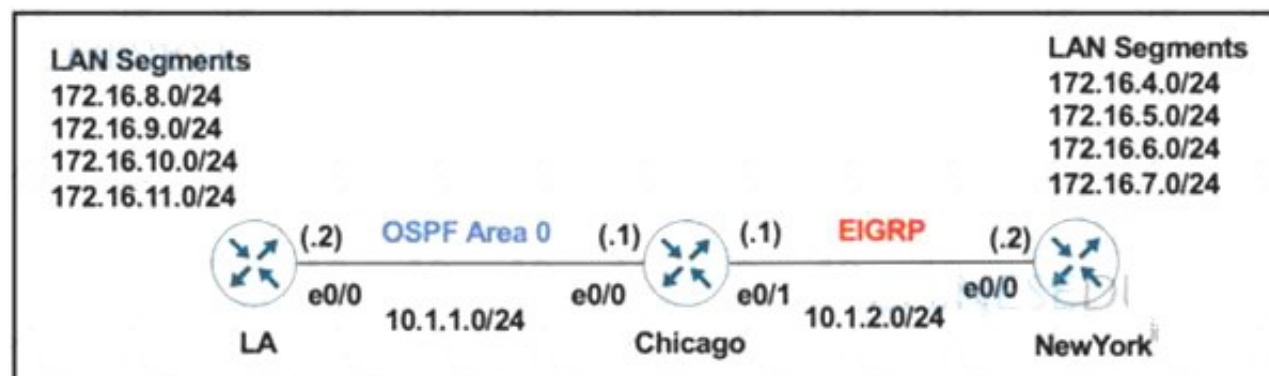
D. Option D

**Answer: B**

**NEW QUESTION 382**

- (Exam Topic 3)

Refer to the exhibit.



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

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

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

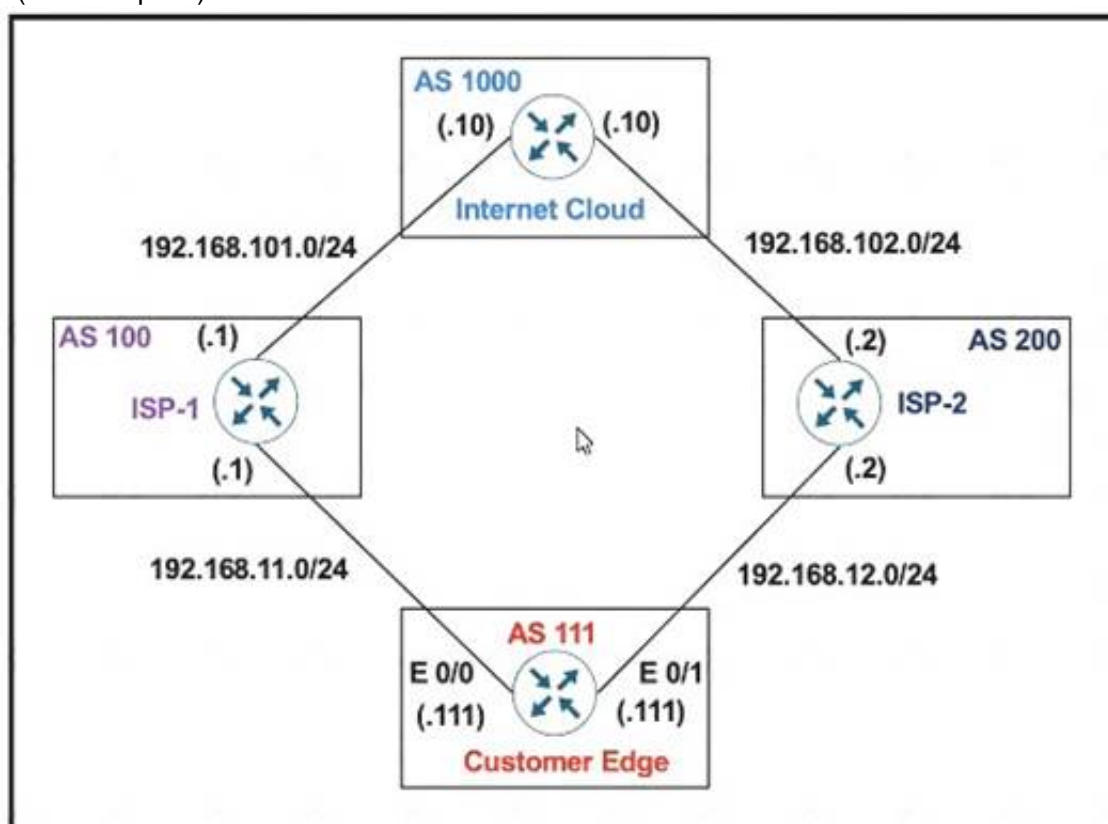
- ☒ interface E 0/1  
ip summary-address eigrp 100 172.16.0.0 255.255.0.0
- ☐ interface E 0/1  
ip summary-address eigrp 100 172.16.8.0 255.255.252.0
- ☐ router eigrp 100  
summary-address 172.16.8.0 255.255.252.0
- ☐ router eigrp 100  
summary-address 172.16.0.0 255.255.0.0

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

Answer: B

### NEW QUESTION 386

- (Exam Topic 3)



```
ISP-1
ip as-path access-list 1 permit ^111
!
router bgp 100
 neighbor 192.168.101.10 remote-as 1000
 neighbor 192.168.11.111 remote-as 111
 neighbor 192.168.11.111 filter-list 1 in
```

Refer to the exhibit. AS 111 must not be used as a transit AS, but ISP-1 is getting ISP-2 routes from AS 111. Which configuration stops Customer AS from being used as a transit path on ISP-1?

- A. ip as-path access-list 1 permit ^\$
- B. ip as-path access-list 1 permit \_111\_
- C. ip as-path access-list 1 permit."
- D. ip as-path access-list 1 permit ^111\$

Answer: A

### NEW QUESTION 390

- (Exam Topic 2)

How are MPLS Layer 3 VPN services deployed?

- A. The RD and RT values must match under the VRR
- B. The RD and RT values under a VRF must match on the remote PE router
- C. The import and export RT values under a VRF must always be the same.
- D. The label switch path must be available between the local and remote PE routers.

Answer: D

#### Explanation:

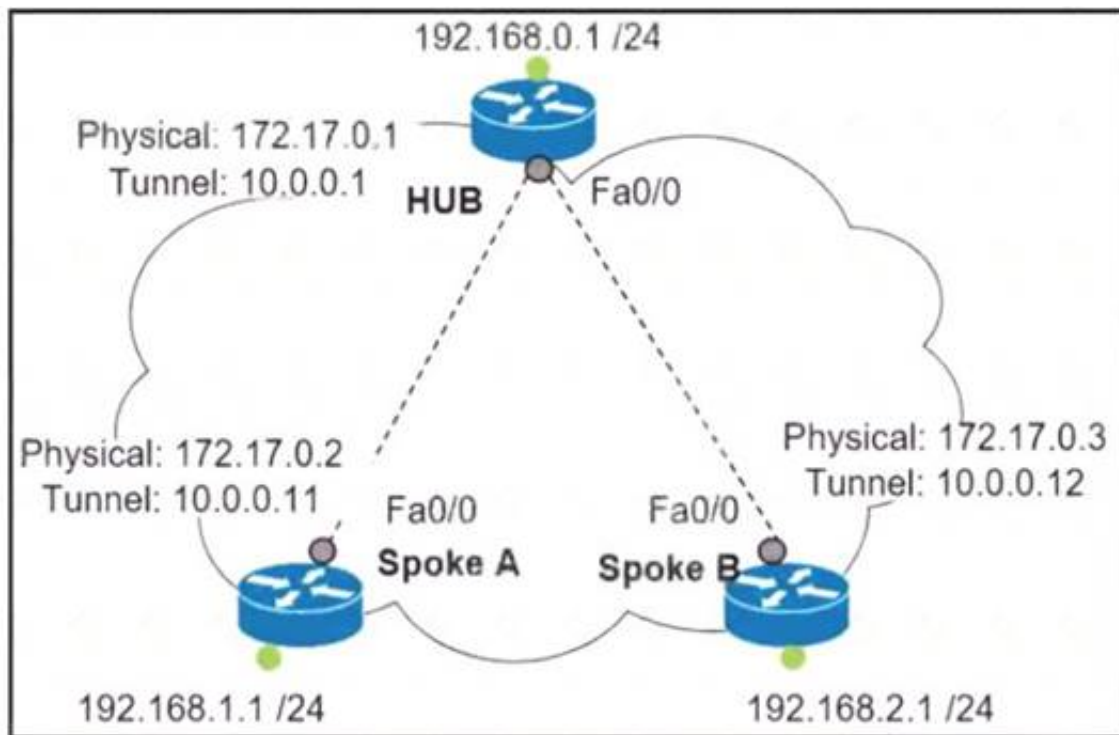
<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/vpn/65x/b-l3vpn-cg-ncs5500-65x/b-l3vpn-cg-ncs5500-65> The ingress PE router must be able to reach the egress PE router for a packet to be relayed to its destination.



**NEW QUESTION 394**

- (Exam Topic 2)

Refer to the exhibit.



Which interface configuration must be configured on the HUB router to enable MVPN with mGRE mode?

- ☒ interface Tunnel0  
description mGRE - DMVPN Tunnel  
ip address 10.1.0.1 255.255.255.0  
ip nhrp map multicast dynamic  
ip nhrp network-id 1  
tunnel source 172.17.0.1  
ip nhrp map 10.0.0.11 172.17.0.2  
ip nhrp map 10.0.0.12 172.17.0.3  
tunnel mode gre
- ☐ interface Tunnel0  
description mGRE - DMVPN Tunnel  
ip address 10.0.0.1 255.255.255.0  
ip nhrp map multicast dynamic  
ip nhrp network-id 1  
tunnel source 10.0.0.1  
tunnel mode gre multipoint
- ☐ interface Tunnel0  
description mGRE - DMVPN Tunnel  
ip address 10.0.0.1 255.255.255.0  
ip nhrp network-id 1  
tunnel source 172.17.0.1  
tunnel mode gre multipoint
- ☐ interface Tunnel0  
description mGRE - DMVPN Tunnel  
ip address 10.0.0.1 255.255.255.0  
ip nhrp map multicast dynamic  
ip nhrp network-id 1  
tunnel source 10.0.0.1  
tunnel destination 172.17.0.2  
tunnel mode gre multipoint

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

**Answer: C**

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-m](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-m)

**NEW QUESTION 399**

- (Exam Topic 3)

```
R1#show ip rip database
10.0.0.0/8   auto-summary
10.1.1.0/24  directly connected, GigabitEthernet0/0
10.1.3.0/24
   [2] via 10.1.12.2, 00:00:03, GigabitEthernet1/0
10.1.12.0/24 directly connected, GigabitEthernet1/0
10.1.23.0/24
   [1] via 10.1.12.2, 00:00:03, GigabitEthernet1/0
```

Refer to the exhibit. A customer reports that networks in the 10.0.1.0/24 space do not appear in the RIP database. What action resolves the issue?

- A. Remove summarization of 10.0.0.0/8.
- B. Permit 10.0.1.0/24 address in the ACL.
- C. Remove ACL on R1 blocking 10.0.1.0/24 network.
- D. Configure 10.0.1.0/24 network under RIP.

**Answer:** A

#### NEW QUESTION 401

- (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 404

- (Exam Topic 2)

Refer to the exhibit.

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
time-range Office-hour
periodic weekdays 08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh time-range Office-hour
```

An IT staff member comes into the office during normal office hours and cannot access devices through SSH. Which action should be taken to resolve this issue?

- A. Modify the access list to use the correct IP address.
- B. Configure the correct time range.
- C. Modify the access list to correct the subnet mask.
- D. Configure the access list in the outbound direction.

**Answer:** A

#### Explanation:

To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

#### NEW QUESTION 407

- (Exam Topic 2)

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

label edge router	allows an LSR to remove the label before forwarding the packet
label switch router	accepts unlabeled packets and imposes labels
forwarding equivalence class	group of packets that are forwarded in the same manner
penultimate hop popping	receives labeled packets and swaps labels

A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs push an MPLS label onto an incoming packet and pop it off an outgoing packet.  
A forwarding equivalence class (FEC) is a term

**NEW QUESTION 411**

- (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.

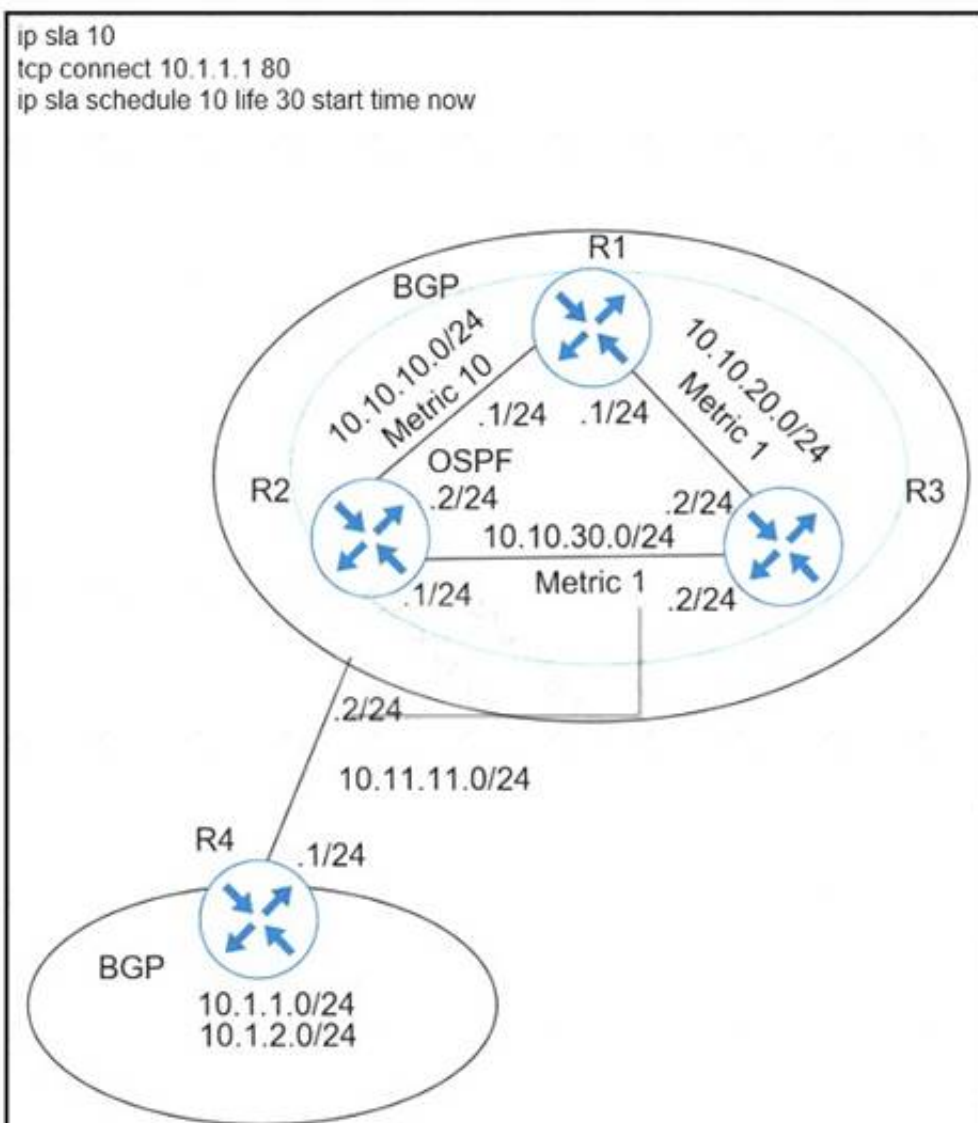
Reference:

[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 412**

- (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 414

- (Exam Topic 2)

Refer to the exhibit.

```
MASS-RTR#show running-config
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 0236244818115F3348
username cisco privilege 15 password 7 0607072C494A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!
```

```
MASS-RTR#show archive log config all
idx    sess    user@line  Logged command
  1      1      console@console |interface GigabitEthernet0/0
  2      1      console@console | no shutdown
  3      1      console@console | ip address dhcp
  4      2      admin@vty0    |username cisco privilege 15 password cisco
  5      2      admin@vty0    |!config: USER TABLE MODIFIED
```

A client is concerned that passwords are visible when running this show archive log config all. Which router configuration is needed to resolve this issue?

- A. MASS-RTR(config-archive-log-cfg)#password encryption aes
- B. MASS-RTR(config)#aaa authentication arap
- C. MASS-RTR(config)#service password-encryption
- D. MASS-RTR(config-archive-log-cfg)#hidekeys

**Answer: D**

#### Explanation:

Step 7 hidekeys

Example:

```
Device(config-archive-log-config)# hidekeys
```

(Optional) Suppresses the display of password information in configuration log files.

Note

Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.

#### NEW QUESTION 417

- (Exam Topic 2)

A DMVPN single hub topology is using IPsec + mGRE with OSPF. What should be configured on the hub to ensure it will be the designated router?

- A. tunnel interface of the hub with ip nhrp ospf dr
- B. OSPF priority to 0
- C. route map to set the metrics of learned routes to 110
- D. OSPF priority greater than 1

**Answer: D**

#### Explanation:

By default, the priority is 1 on all routers so we can set the OSPF priority of the hub to a value which is greater than 1 to make sure it would become the DR.

#### NEW QUESTION 422

- (Exam Topic 2)

Refer to the exhibit.

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

When monitoring an IPv6 access list, an engineer notices that the ACL does not have any hits and is causing unnecessary traffic to pass through the interface. Which command must be configured to resolve the issue?

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

**Answer: C**

#### NEW QUESTION 427

- (Exam Topic 2)

Refer to the exhibit.

```
router ospf 1
 redistribute eigrp 1 subnets route-map EIGRP->OSPF
!
router eigrp 1
 network 10.0.106.0 0.0.0.255
!
route-map EIGRP->OSPF permit 10
 match ip address WAN_PREFIXES
route-map EIGRP->OSPF permit 20
 match ip address LOCAL_PREFIXES
route-map EIGRP->OSPF permit 30
 match ip address VPN_PREFIXES
!
ip prefix-list LOCAL_PREFIXES seq 5 permit 172.16.0.0/12 le 24
ip prefix-list VPN_PREFIXES seq 5 permit 192.168.0.0/16 le 24
ip prefix-list WAN_PREFIXES seq 5 permit 10.0.0.0/8 le 24
!
```

The network administrator configured redistribution on an ASBR to reach to all WAN networks but failed. Which action resolves the issue?

- A. The route map must have the keyword prefix-list to evaluate the prefix list entries.
- B. The OSPF process must have a metric when redistributing prefixes from EIGRP.
- C. The route map EIGRP->OSPF must have the 10.0.106.0/24 entry to exist in one of the three prefix lists to pass.
- D. EIGRP must redistribute the 10.0.106.0/24 route instead of using the network statement.

**Answer: A**

#### Explanation:

In order to use a prefix-list in a route-map, we must use the keyword "prefix-list" in the "match" statement. . For example:

```
match ip address prefix-list WAN_PREFIXES
```

Without this keyword, the router will try to find an access-list with the same name instead.

#### NEW QUESTION 429

- (Exam Topic 2)

Refer to the exhibit.

```
L 172.1.12.3/32 is directly connected, Ethernet0/0
C 172.1.13.0/24 is directly connected, Ethernet0/1
L 172.1.13.3/32 is directly connected, Ethernet0/1
O 192.168.1.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O 192.168.2.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O 192.168.3.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
O 192.168.4.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
 192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.5.0/24 is directly connected, Loopback0
L 192.168.5.1/32 is directly connected, Loopback0
 192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.6.0/24 is directly connected, Loopback1
L 192.168.6.1/32 is directly connected, Loopback1
```

San Francisco and Boston routers are choosing slower links to reach each other despite the direct links being up. Which configuration fixes the issue?

☐ Boston Router

```
router ospf 1
auto-cost reference-bandwidth 1000
```

☐ SanFrancisco Router

```
router ospf 1
auto-cost reference-bandwidth 1000
```

☐ All Routers

```
router ospf 1
auto-cost reference-bandwidth 100
```

☐ All Routers

```
router ospf 1
auto-cost reference-bandwidth 1000
```

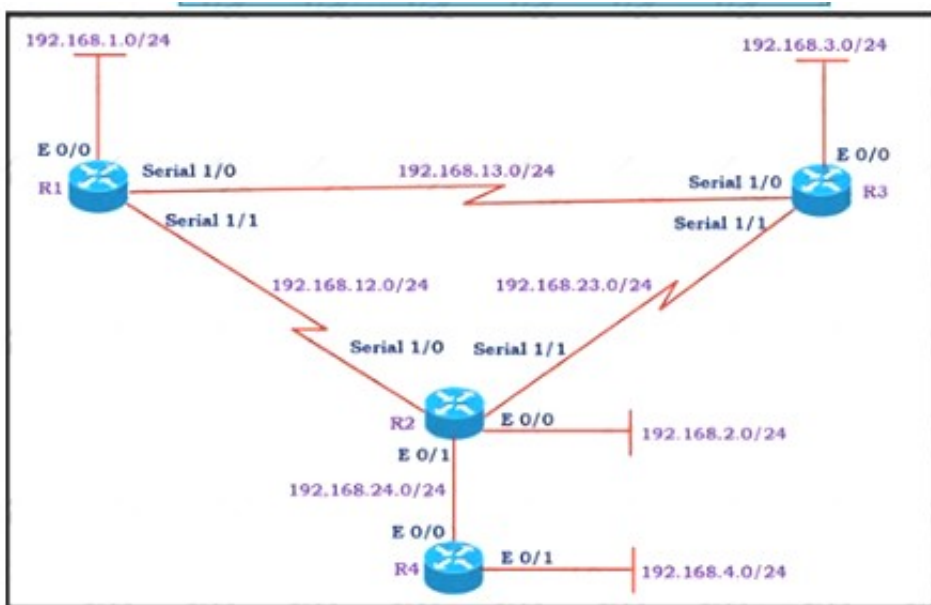
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

### NEW QUESTION 432

- (Exam Topic 2)

Refer to the exhibit.



#### # Show IP route on R1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

- C 192.168.1.0/24 is directly connected, Ethernet0/0
  - L 192.168.1.1/32 is directly connected, Ethernet0/0
  - D 192.168.2.0/24 [90/2297856] via 192.168.12.2, 00:02:14, Serial1/1
  - S 192.168.3.0/24 [1/0] via 192.168.12.2
- 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.12.0/24 is directly connected, Serial1/1
  - L 192.168.12.1/32 is directly connected, Serial1/1
- 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.13.0/24 is directly connected, Serial1/0
  - L 192.168.13.1/32 is directly connected, Serial1/0
  - D 192.168.23.0/24 [90/2681856] via 192.168.13.3, 00:06:38, Serial1/0
- [90/2681856] via 192.168.12.2, 00:06:38, Serial1/1

All the serial between R1, R2, and R3 have the Same bandwidth. User on the 192.168.1.0/24 network report slow response times while they access resource on network 192.168.3.0/24. When a traceroute is run on the path. It shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up. What must the network administrator to fix the slowness?

- A. Change the Administrative Distance of EIGRP to 5.
- B. Add a static route on R1 using the next hop of R3.
- C. Remove the static route on R1.
- D. Redistribute the R1 route to EIGRP



**Answer:** C

**NEW QUESTION 436**

- (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 441**

- (Exam Topic 2)

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

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

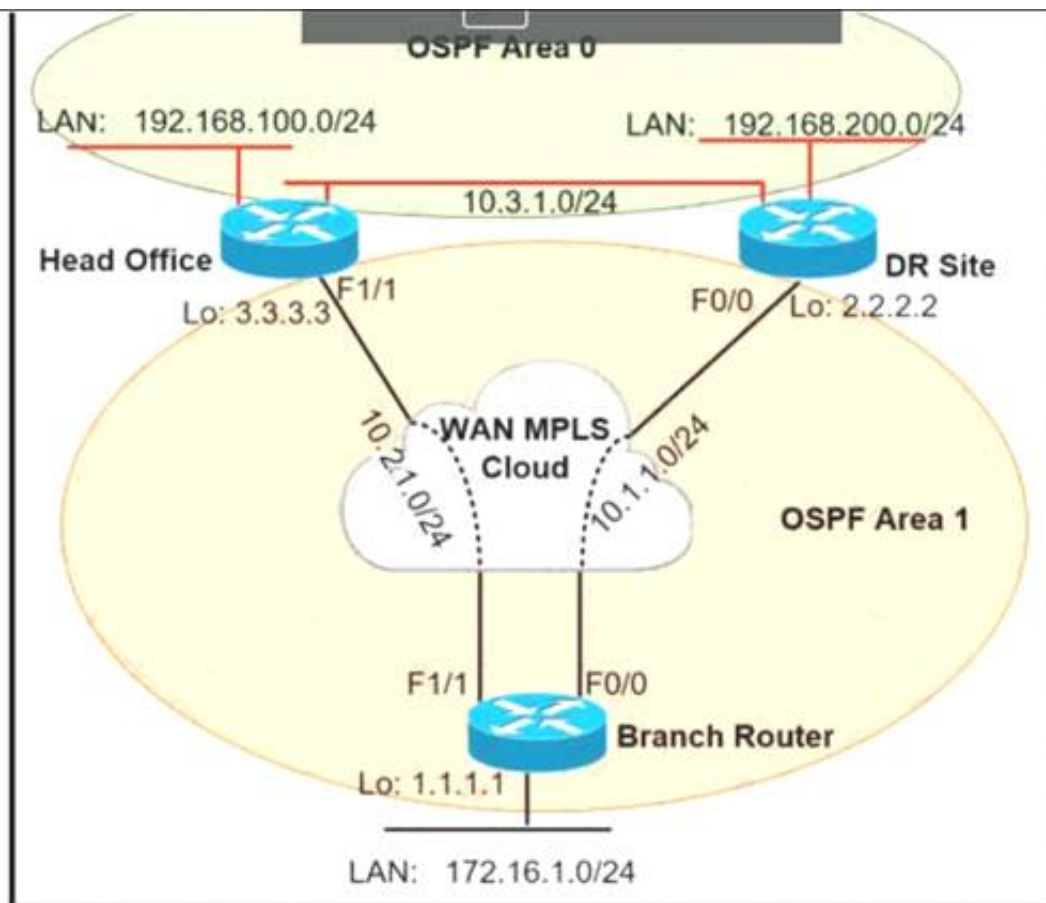
- A. ipv6 access-list inbound permit tcp any any syn deny ipv6 any any log!interface gi0/0ipv6 traffic-filter inbound out
- B. ipv6 access-list inbound permit tcp any any syn deny ipv6 any any log!interface gi0/0ipv6 traffic-filter inbound in
- C. ipv6 access-list inbound permit tcp any any establisheddeny ipv6 any any log!interface gi0/0ipv6 traffic-filter inbound in
- D. ipv6 access-list inbound permit tcp any any established deny ipv6 any any log!interface gi0/0ipv6 traffic-filter inbound out

**Answer:** C

**NEW QUESTION 443**

- (Exam Topic 2)

Refer to the exhibit.



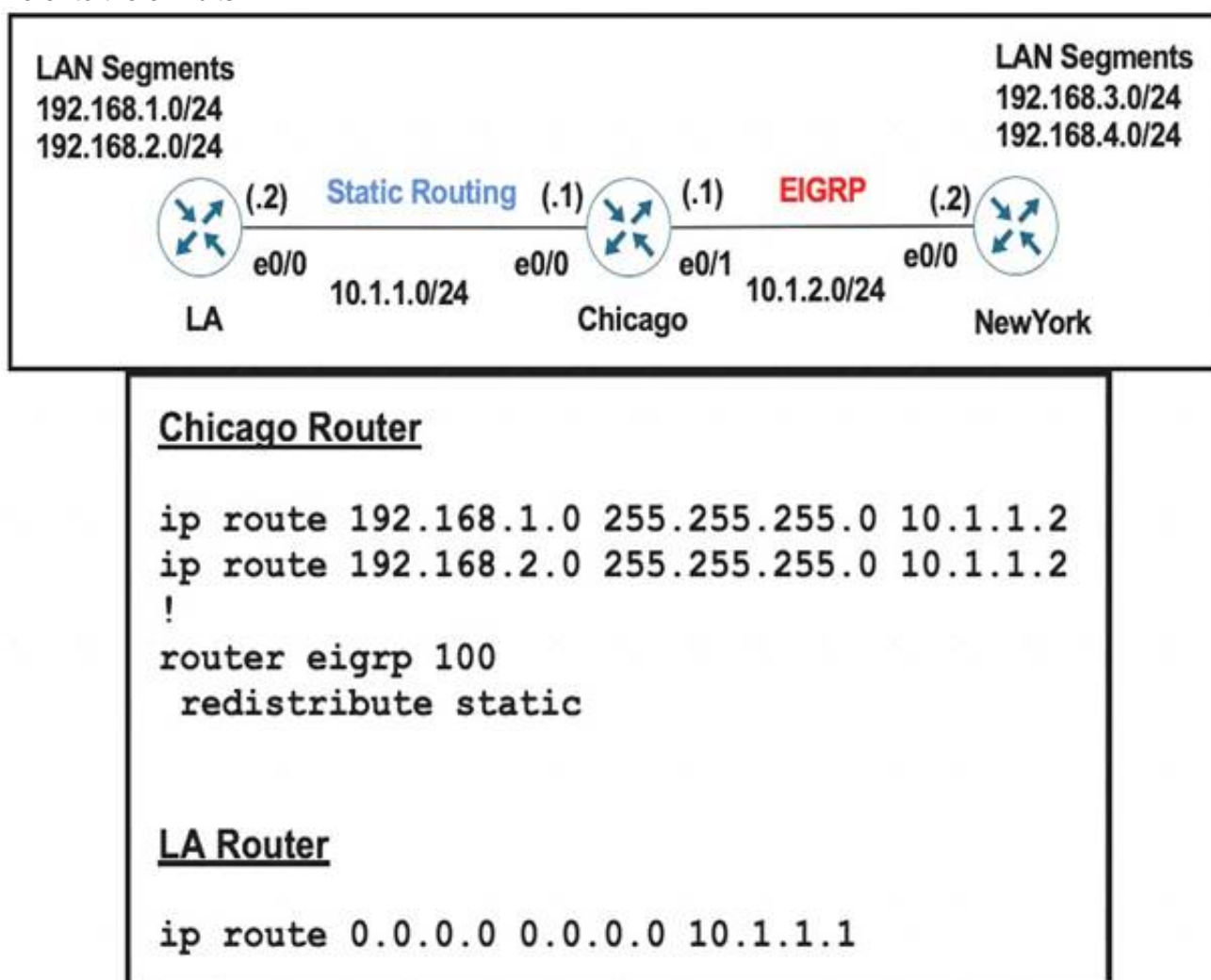
A network administrator reviews the branch router console log to troubleshoot the OSPF adjacency issue with the DR router. Which action resolves this issue?

- 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 445

- (Exam Topic 2)  
Refer to the exhibits.



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

- A)  
**Chicago Router**  
  
router eigrp 100  
redistribute static metric 10 10 10 10 10
- B)  
**Chicago Router**  
  
router eigrp 100  
redistribute connected

C)

Chicago Router

```
ip route 192.168.3.0 255.255.255.0 10.1.2.2
```

```
ip route 192.168.4.0 255.255.255.0 10.1.2.2
```

D)

LA Router

```
ip route 192.168.3.0 255.255.255.0 10.1.1.1
```

```
ip route 192.168.4.0 255.255.255.0 10.1.1.1
```

A. Option A

B. Option B

C. Option C

D. Option D

**Answer:** B

**NEW QUESTION 446**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 300-410 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/300-410-dumps.html>