

# Cisco

## Exam Questions 300-410

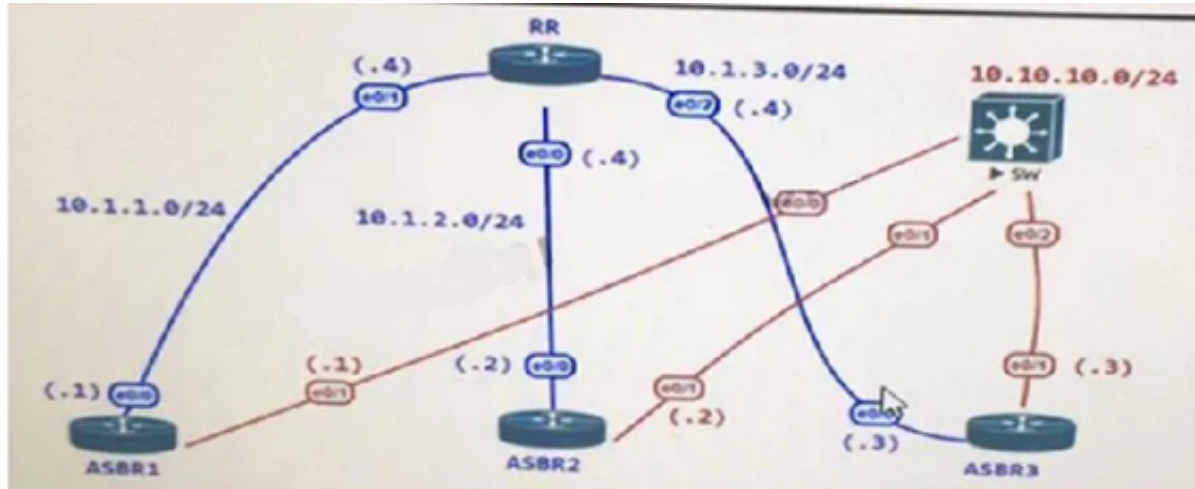
Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)



### NEW QUESTION 1

- (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 2

- (Exam Topic 3)

An engineer configures PBR on R5 and wants to create a policy that matches traffic destined toward 10.10.10.0/24 and forward 10.1.1.1. The traffic must also have its IP precedence set to 5. All other traffic should be forward toward 10.1.1.2 and have its IP precedence set to 0. Which configuration meets the requirements?

- A. access-list 1 permit 10.10.10.0 0.0.0.255 access-list 2 permit any route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 match ip address 2 set ip next-hop 10.1.1.2 set ip precedence 0 route-map CCNP permit 30
- B. access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 100 set ip next-hop 10.1.1.1 set ip precedence 0 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 5 ! route-map CCNP permit 30
- C. access-list 1 permit 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 1 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 0
- D. access-list 100 permit ip any 10.10.10.0 0.0.0.255 route-map CCNP permit 10 match ip address 100 set ip next-hop 10.1.1.1 set ip precedence 5 ! route-map CCNP permit 20 set ip next-hop 10.1.1.2 set ip precedence 0

**Answer: D**

### NEW QUESTION 3

- (Exam Topic 3)

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

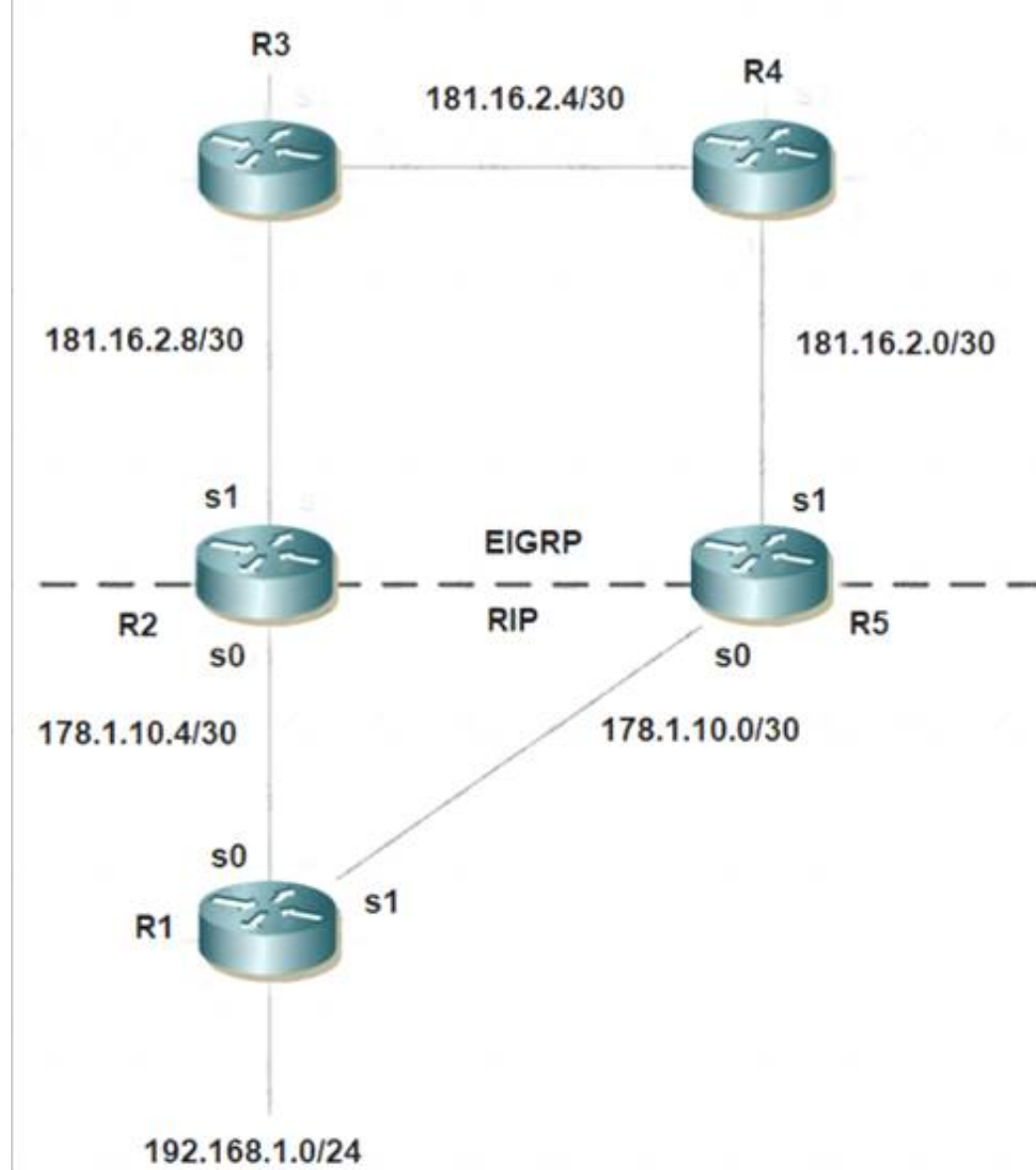
- A. Use pseudowire for Layer 2 routes
- B. Use MP-BGP for customer routes
- C. Use OSPF between PE and CE
- D. Use a unique RD per customer VRF
- E. Use LDP for customer routes

**Answer: CD**

#### NEW QUESTION 4

- (Exam Topic 3)

Refer to the exhibit.



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

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

**Answer: D**

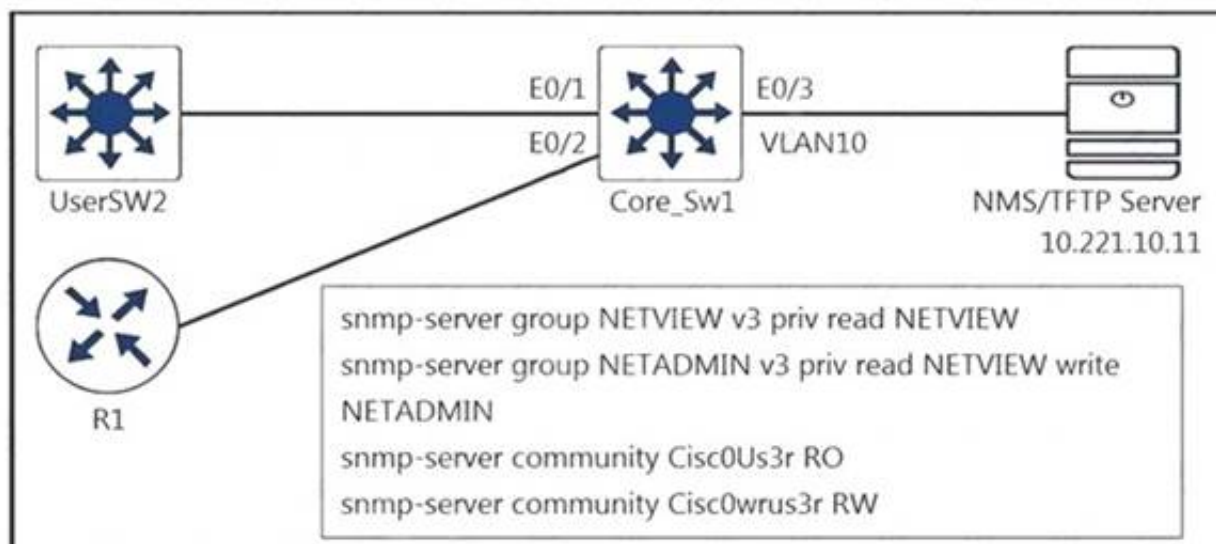
**Explanation:**

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

#### NEW QUESTION 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

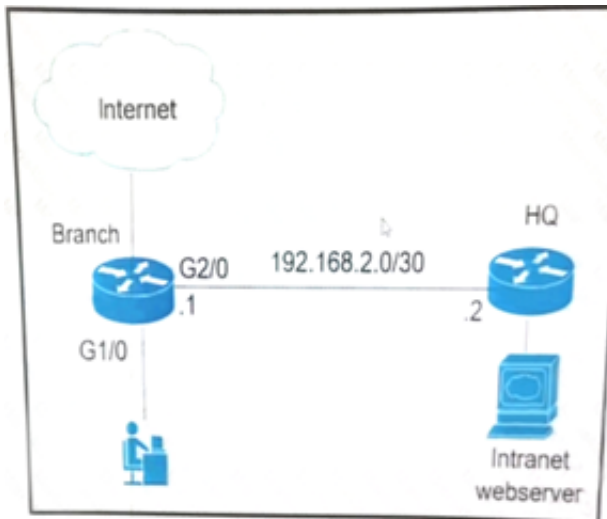
v3 priv read NETVIEW write NETADMIN access 20 snmp-server community Cisc0Us3r RO 20snmp-server community Cisc0wrus3r RW 20snmp-server tftp-server-list 20  
 B. access-list 20 permit 10.221.10.11 access-list 20 deny any log!snmp-server group NETVIEW v3 priv read NETVIEW access 20snmp-server group NETADMIN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

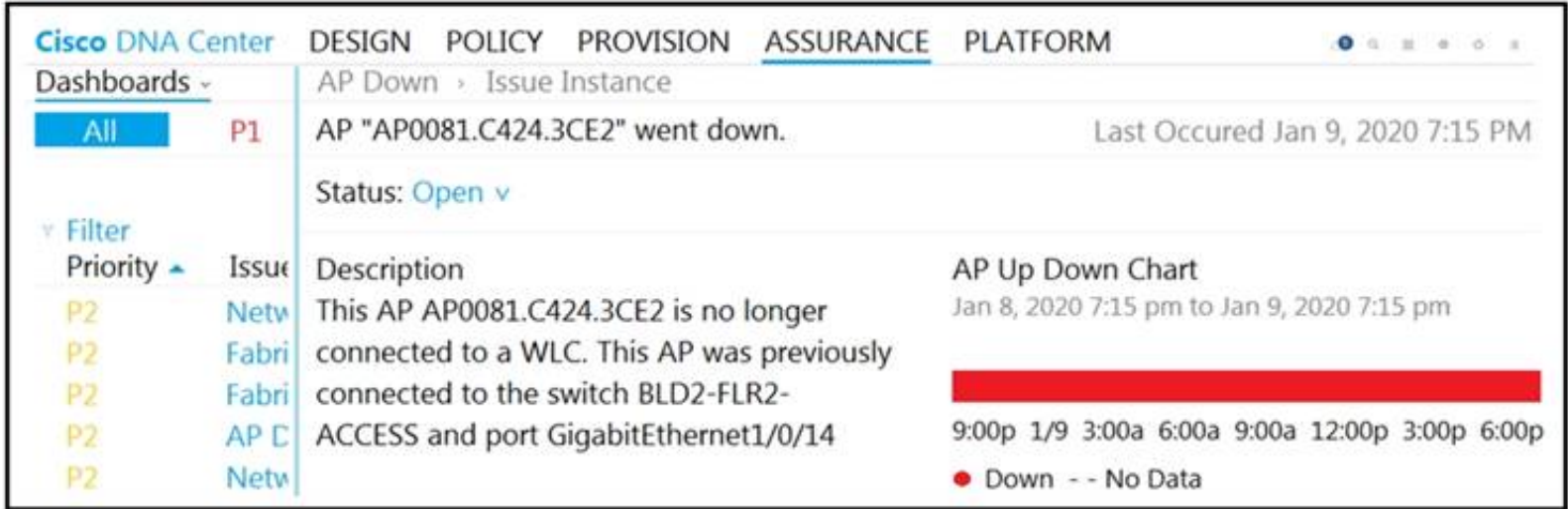
**Answer:** B

**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:

```

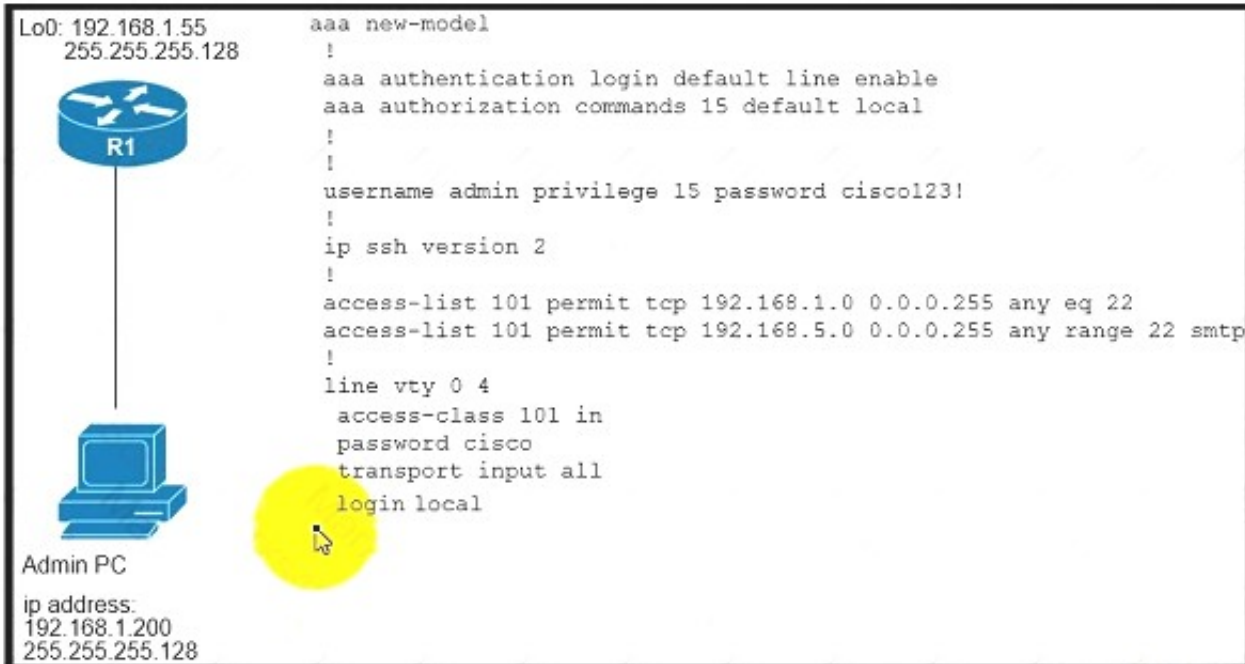
TDR test last run on: December 05 18:50:53
Interface Speed Local pair Pair length Remote pair Pair status
Gi1/0/14 1000M Pair A 19 +/- 10 meters Pair B Normal
          Pair B 19 +/- 10 meters Pair A Normal
          Pair C 19 +/- 10 meters Pair D Normal
          Pair D 19 +/- 10 meters Pair C Normal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

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)



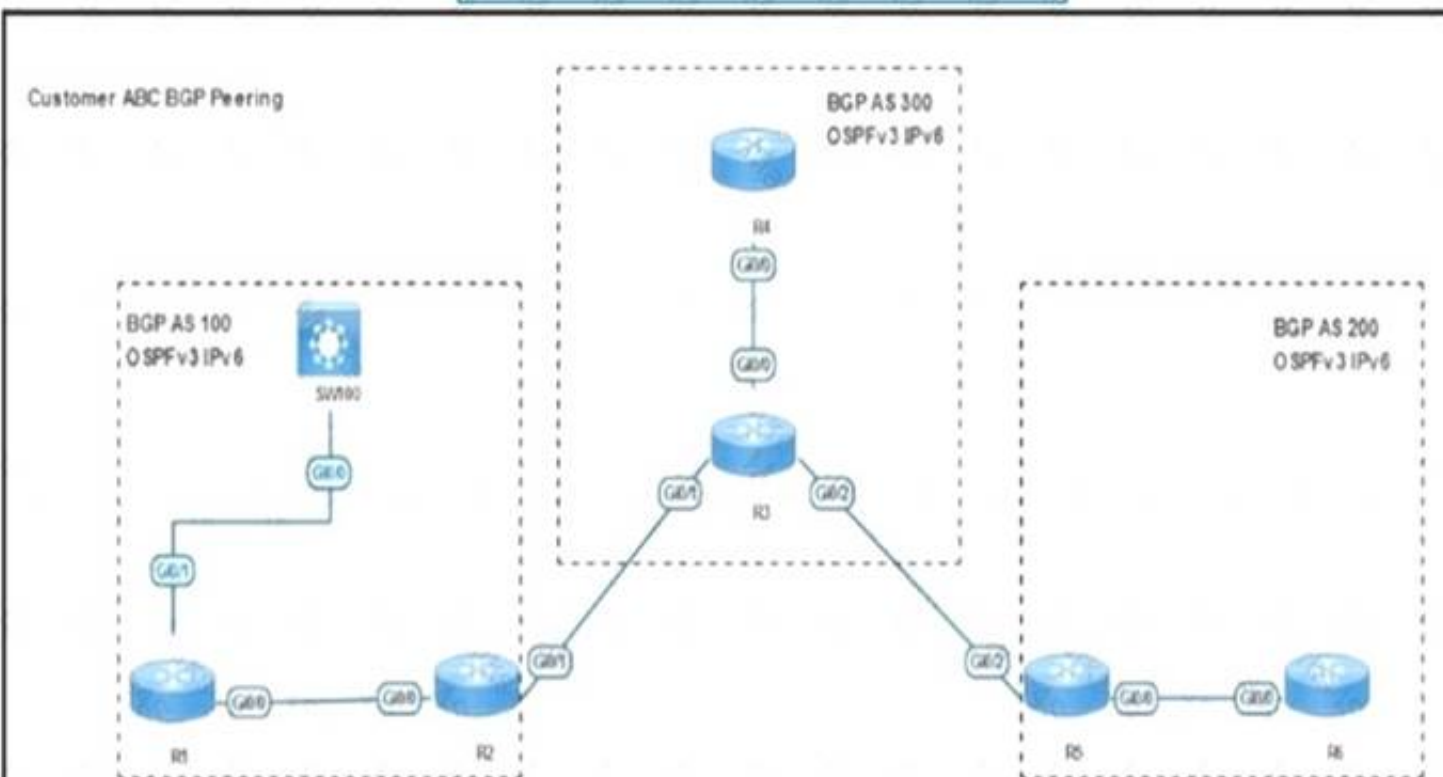
Refer to the exhibit. An engineer configured user login based on authentication database on the router, but no one can log into the router. Which configuration resolves the issue?

- 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)



```

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

```

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

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

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

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

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

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

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

**Answer: B**

#### NEW QUESTION 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.

```

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

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

Which action resolves this issue?

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

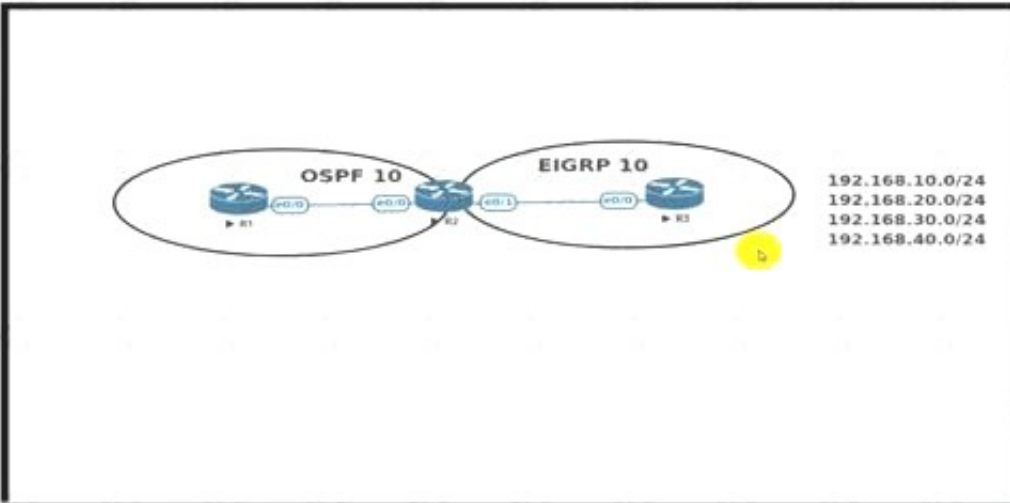
**Answer: D**

#### NEW QUESTION 12

- (Exam Topic 3)



Refer to the exhibit.



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

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

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

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

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

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

**Answer: B**

### NEW QUESTION 13

- (Exam Topic 3)

Refer to the exhibit.



```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                Interface      Hold Uptime    SRTT  RTO  Q  Seq
   (sec)                  (ms)          Cnt Num
1   192.168.10.1            Ser1/0        12 00:00:39    1  5000  2  0
*Jan  1 15:40:21.295: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is down: retry limit exceeded
*Jan  1 15:40:51.567: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is up: new adjacency
*Jan  1 15:42:11.107: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is down: retry limit exceeded
*Jan  1 15:42:14.879: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.10.1 (Serial1/0) is up: new adjacency
```

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
```

#### R1 Configuration:

```
key chain cisco
key 2
  key-string abc
!
interface Loopback0
ip address 10.10.1.1 255.255.255.0
!
interface Serial1/0
ip address 192.168.10.1 255.255.255.0
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 cisco
serial restart-delay 0
!
router eigrp 100
network 10.10.1.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

#### R2 configuration:

```
key chain cisco
key 1
  key-string 123
key 2
  key-string abc
!
interface Loopback0
ip address 10.10.2.2 255.255.255.0
!
interface Serial1/0
ip address 192.168.10.2 255.255.255.0
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 cisco
no fair-queue
!
!
router eigrp 100
network 10.10.2.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

R1 and R2 are configured for EIGRP peering using authentication and the neighbors failed to come up. Which action resolves the issue?

- A. Configure a matching key-id number on both routers
- B. Configure a matching lowest key-id on both routers
- C. Configure a matching key-chain name on both routers
- D. Configure a matching authentication type on both router

**Answer: A**

#### NEW QUESTION 16

- (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.)

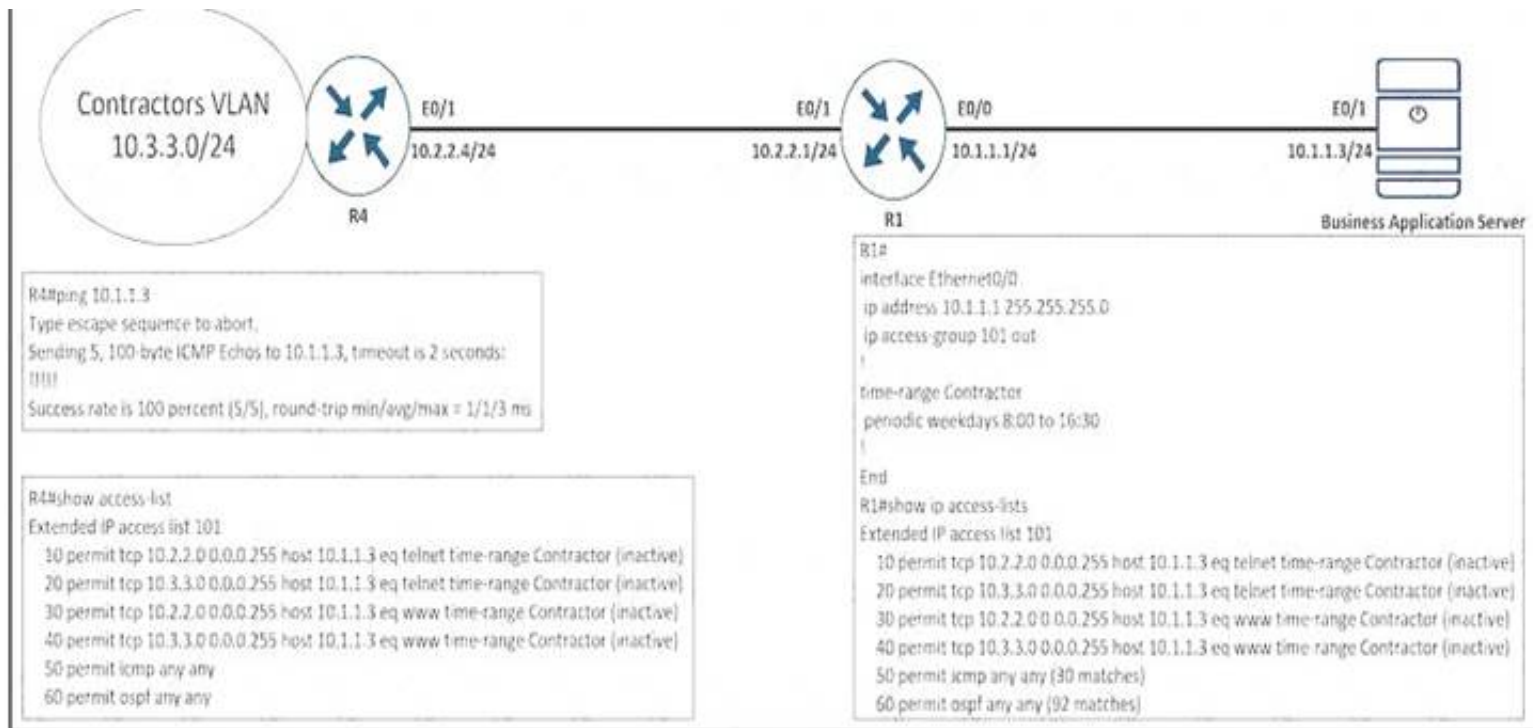
- A. interface E0/0no service-policy input PM-COPP!control-planeservice-policy input PM-COPP
- B. policy-map PM-COPP class CM-ADMINno police 500000 conform-action transmit police 500 conform-action transmit!control-planeservice-policy input PM-COPP
- C. no access-list 100access-list 100 permit tcp host 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 20

- (Exam Topic 3)

Refer to the exhibit.



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

- A)  
**R1**  
**time-range Contractor**  
**no periodic weekdays 8:00 to 16:30**  
**periodic daily 8:00 to 16:30**
- B)  
**R4**  
**time-range Contractor**  
**no periodic weekdays 17:00 to 23:59**  
**periodic daily 8:00 to 16:30**
- C)  
**R4**  
**no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor**
- D)  
**R1**  
**no access-list 101 permit tcp 10.3.3.0 0.0.0.255 host 10.1.1.3 eq telnet time-range Contractor**

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

**Answer: A**

#### NEW QUESTION 21

- (Exam Topic 3)

Refer to the exhibit.

```

R1(config)#ip access-list standard EIGRP-FILTER
R1(config-std-nacl)#permit 10.10.10.0 0.0.0.255
R1(config)#router eigrp 10
R1(config-router)#distribute-list route-map EIGRP in
!
R1(config)#route-map EIGRP permit 10
R1(config-route-map)#match ip address EIGRP-FILTER
!
R1#show ip route eigrp
D    10.10.10.0/24
  
```

An engineer must filter incoming EIGRP updates to allow only a set of specific prefixes. The distribute list is tested, and it filters out all routes except network 10.10.10.0/24. How should the engineer temporarily allow all prefixes to be learned by the routers again without adjusting the existing access list?

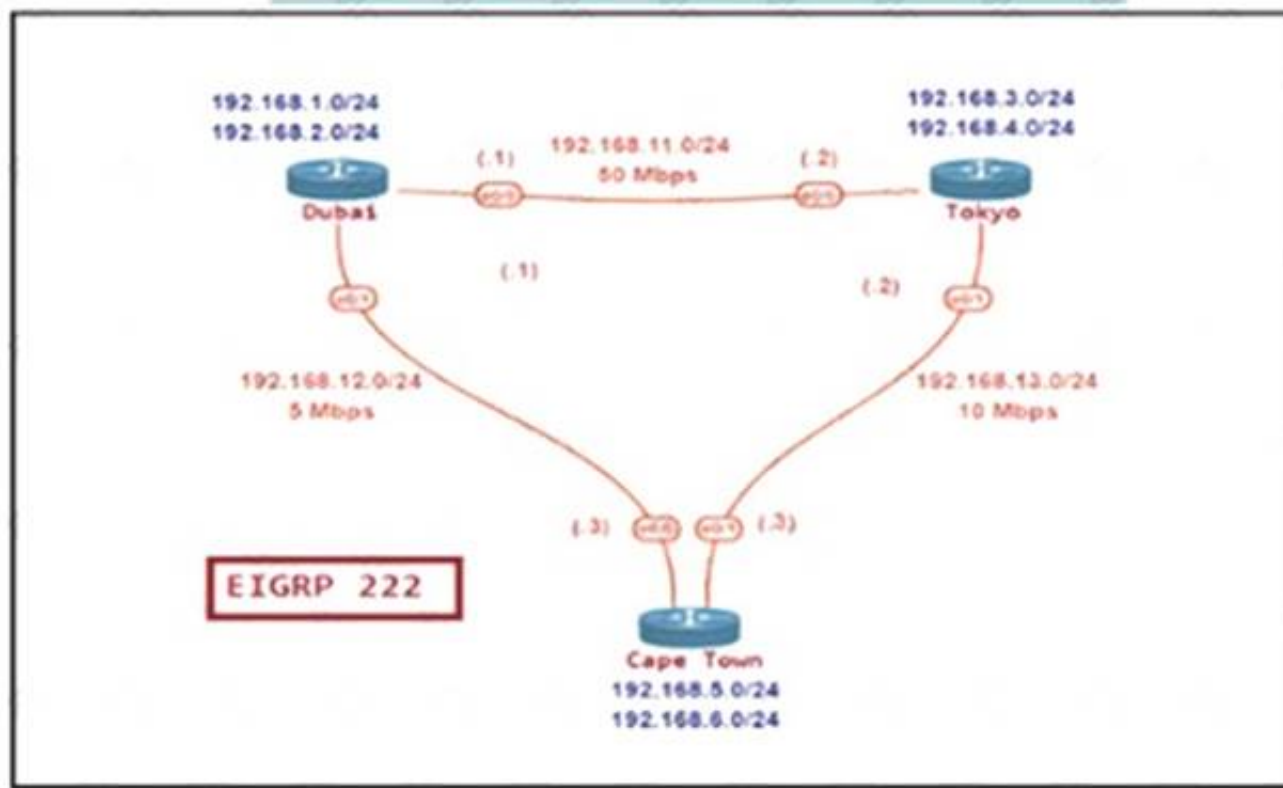
- A. A permit 20 statement should be added before completing the ACL with the required prefixes, and then the permit 20 statement can be removed.  
 B. A permit any statement should be added before completing the ACL with the required prefixes and then the permit any statement can be removed.  
 C. A continue statement should be added within the permit 10 statement before completing the ACL with the required prefixes, and then the continue statement can be removed.  
 D. An extended access list must be used instead of a standard access list to accomplish the task

**Answer: C**

#### NEW QUESTION 23

- (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 32

- (Exam Topic 3)

Refer to the exhibit.

```
R1#
router ospf 1
 redistribute rip subnets
 network 131.108.1.0 0.0.0.255 area 2
 network 131.108.2.0 0.0.0.255 area 2
 distribute-list 1 out
!
access-list 1 permit 132.108.4.0 0.0.0.255
```

The R1 OSPF neighbor is not receiving type 5 external LSAs for 132.108.2.0/24 and 132.108.3.0/24 networks. Which configuration command resolves the issue?

- A. access-list 1 permit 132.108.0.0 0.0.1.255
- B. access-list 1 permit 132.108.0.0 0.0.3.255
- C. access-list 1 permit 132.108.2.0 0.0.0.255
- D. access-list 1 permit 132.108.4.0 0.0.3.255

**Answer:** B

# NEW QUESTION 34

- (Exam Topic 3)

```
RF#traceroute 192.168.1.1
 1 10.0.0.9 40 msec 28 msec 24 msec
 2 * * *
 3 * * *

RE#show ip prefix-list detail
Prefix-list with the last deletion/insertion: Customer
ip prefix-list Customer:
  count: 2, range entries: 1, sequences: 5 - 10, refcount: 3
  seq 5 deny 192.168.1.1/32 (hit count: 5, refcount: 1)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 26, refcount: 1)

RC#show ip prefix-list detail
Prefix-list with the last deletion/insertion: Customer
ip prefix-list Customer:
  count: 1, range entries: 1, sequences: 10 - 10, refcount: 4
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 7, refcount: 1)
```



Refer to the exhibit The enterprise users fail to authenticate with the TACACS server when a direct fiber link fails between RB and RD The NOC team observes

- > Users connected on AS65201 fail to authenticate with TACACS server 192 168 1 1
- > Users connected on AS65101 successfully authenticate with TACACS server 192 168 1 1
- > All AS65101 and AS65201 users are configured to authenticate with the TACACS server

Which configuration resolves the issue?

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

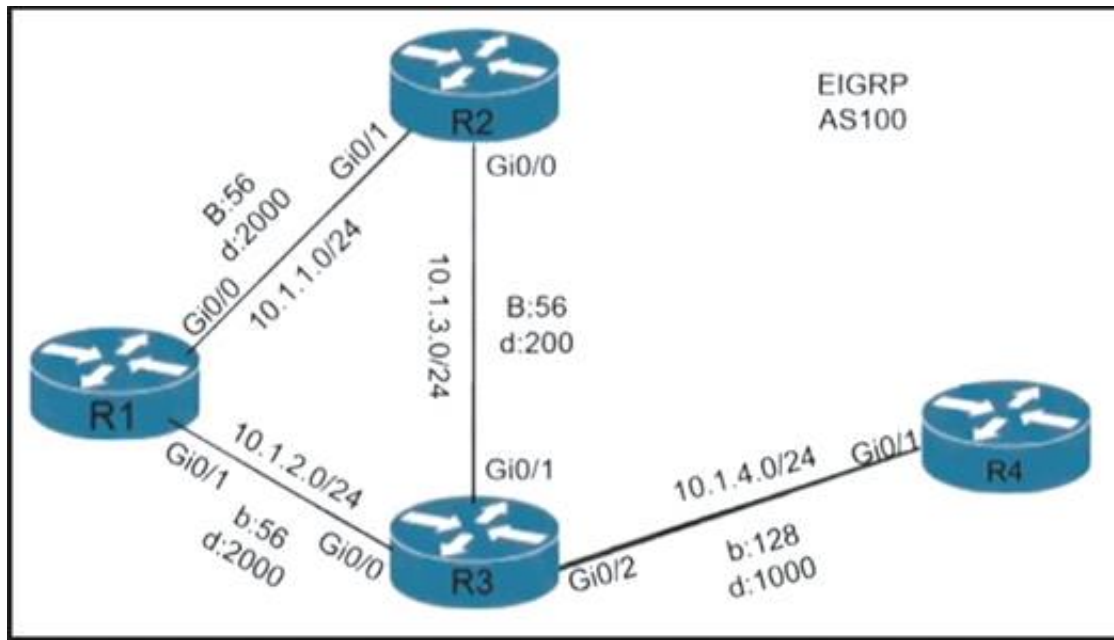
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

# NEW QUESTION 38

- (Exam Topic 3)

Refer to the exhibit.



A loop occurs between R1, R2, and R3 while EIGRP is run with poison reverse enabled. Which action prevents the loop between R1, R2, and R3?

- A. Configure route tagging
- B. Enable split horizon
- C. Configure R2 as stub receive-only
- D. Configure route filtering

**Answer: B**

### NEW QUESTION 39

- (Exam Topic 3)



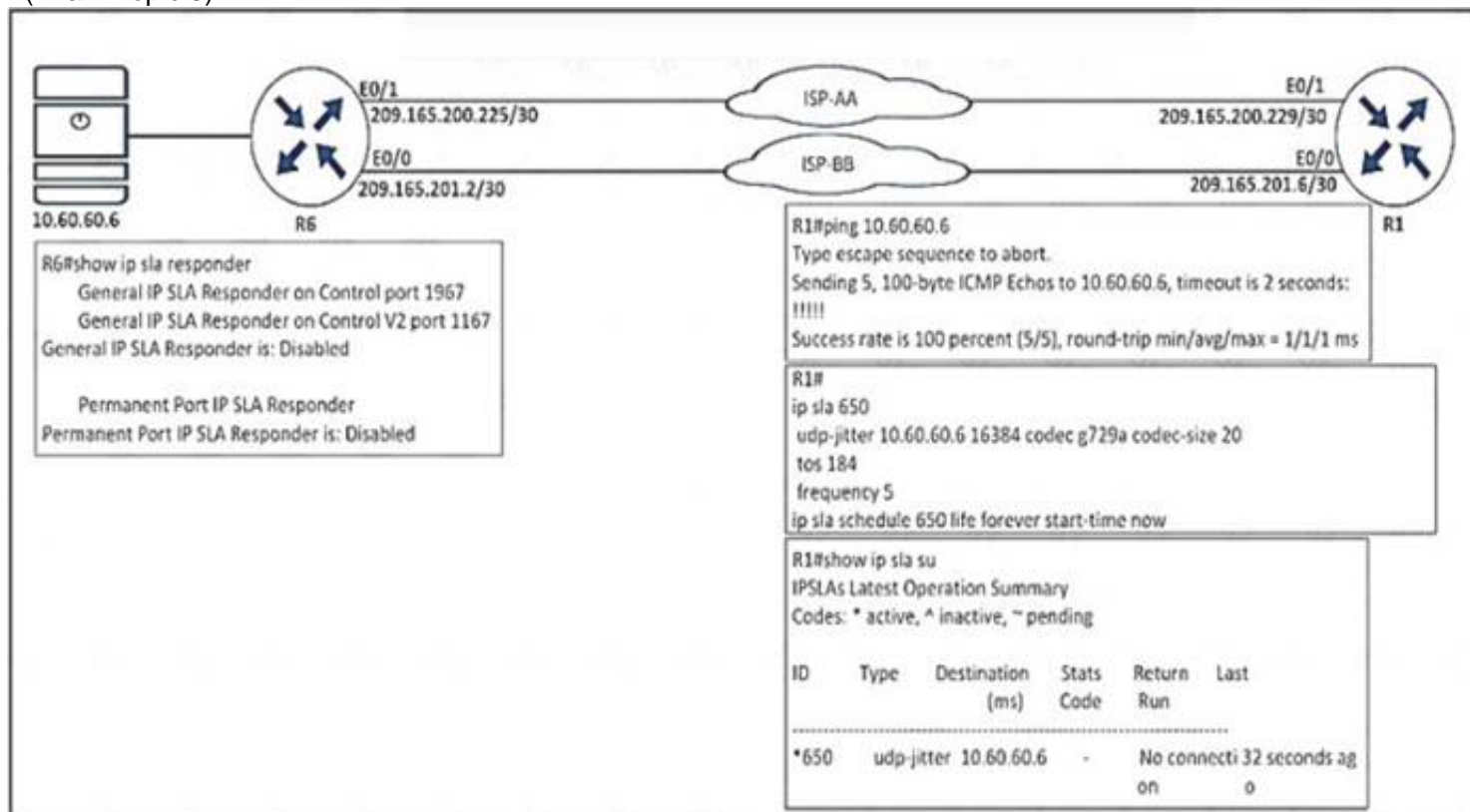
Refer to the exhibit. An engineer is investigating an OSPF issue reported by the Cisco DNA Assurance Center. Which action resolves the issue?

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

**Answer: B**

### NEW QUESTION 43

- (Exam Topic 3)





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

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

**Answer:** A

#### NEW QUESTION 44

- (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 Tunnel0 Interface netmask.
- C. Advertise the Loopback0 interface from R2 across the tunnel.
- D. Readdress the IP network on the Tunnel0 on both routers using the /31 netmask.

**Answer:** A

#### NEW QUESTION 49

- (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 52

- (Exam Topic 3)

Refer to the exhibit.

```
R1# show ip ospf database self-originate

OSPF Router with ID (10.255.255.1) (Process ID 1)

Router Link States (Area 0)

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

Summary Net Link States (Area 0)

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

Type-5 AS External Link States

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

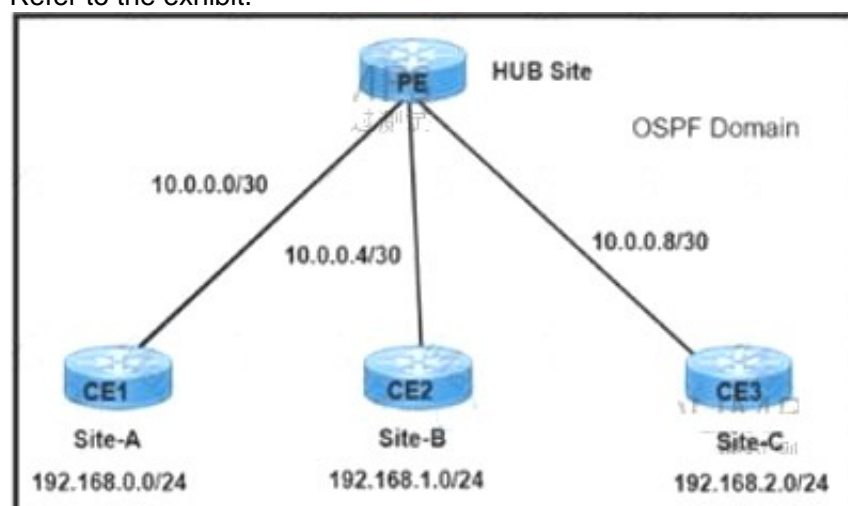
- A. Clear the OSPF process on R1 to flush stale LSAs sent by other routers.
- B. Change the R1 router ID from 10.255.255.1 to a unique value and clear the process.
- C. Increase the SPF delay interval on R1 to synchronize routes.
- D. Disconnect the router with the OSPF router ID 0.0.0.0 from the network.

**Answer: B**

#### NEW QUESTION 54

- (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 57

- (Exam Topic 3)

Refer to the exhibit.

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

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

**Answer: AD**

#### NEW QUESTION 59

- (Exam Topic 3)

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

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

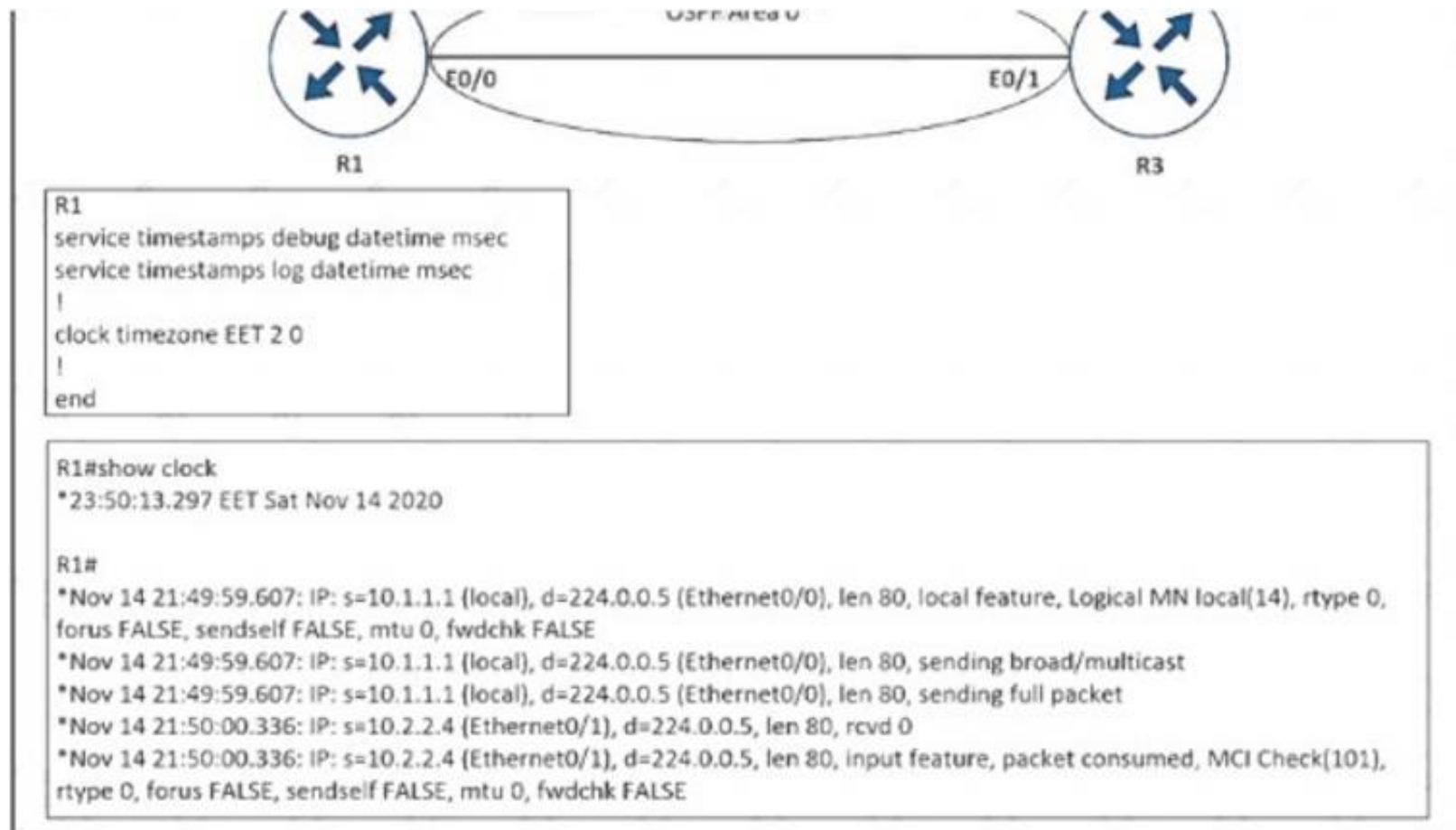
- A. Use the ftp username and ip ftp password configuration commands to specify valid FTP server credentials.  
 B. Use the copy flash:packages.conf scp: command instead and enter the FTP server credentials when prompted.  
 C. Enter the FTP server credentials directly in the FTP URL using the ftp://username:password@192.0.2.40/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

**Answer: AC**

#### NEW QUESTION 63

- (Exam Topic 3)





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

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

**Answer: B**

#### NEW QUESTION 66

- (Exam Topic 3)

What is considered the primary advantage of running BFD?

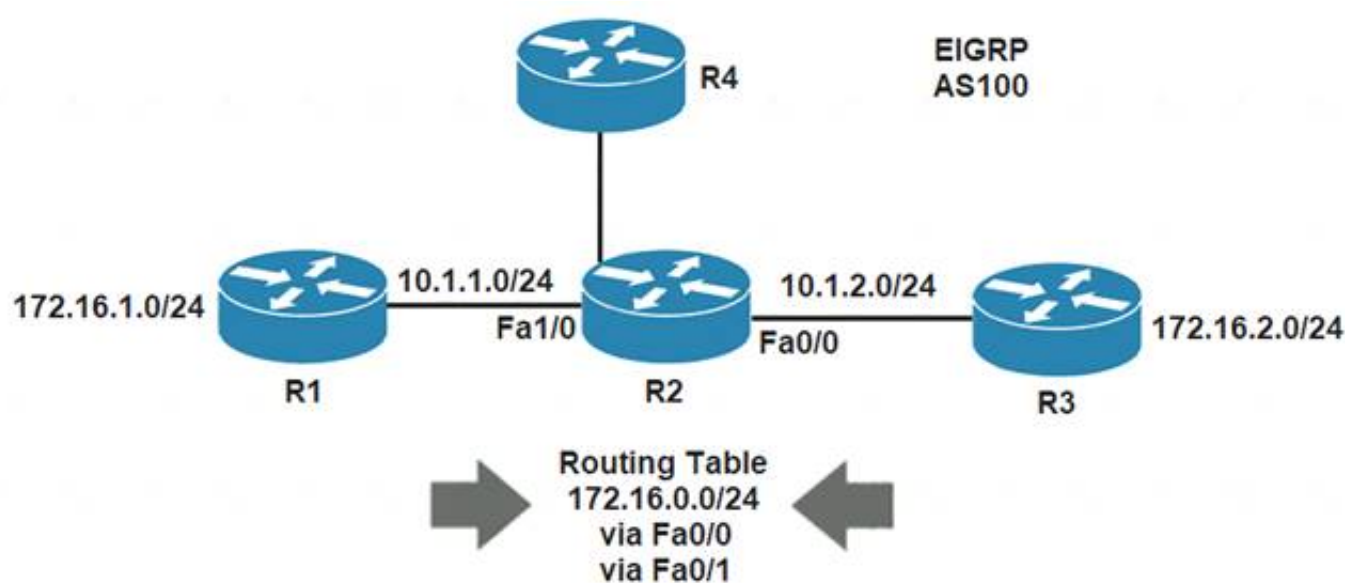
- A. reduction in time needed to detect Layer 2 switched neighbor failures
- B. reduction in time needed to detect Layer 3 routing neighbor failures
- C. reduction in CPU needed to detect Layer 2 switch neighbor failures
- D. reduction in CPU needed to detect Layer 3 routing neighbor failures

**Answer: B**

#### NEW QUESTION 67

- (Exam Topic 3)

Refer to the exhibit.



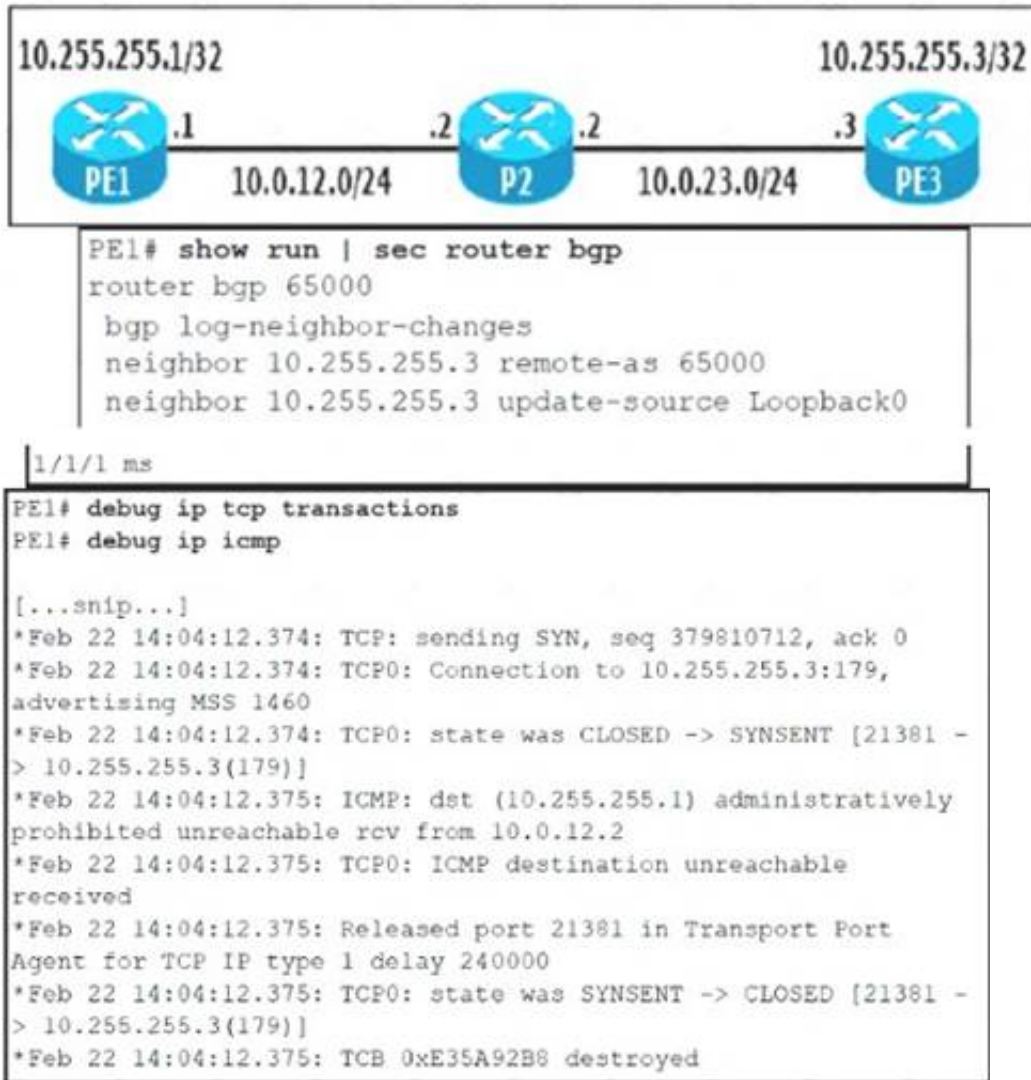
R4 is experiencing packet drop when trying to reach 172.16.2.7 behind R2. Which action resolves the issue?

- A. Insert a /16 floating static route on R2 toward R3 with metric 254
- B. Insert a /24 floating static route on R2 toward R3 with metric 254
- C. Enable auto summarization on all three routers R1, R2, and R3
- D. Disable auto summarization on R2

**Answer: D**

#### NEW QUESTION 72

- (Exam Topic 3)



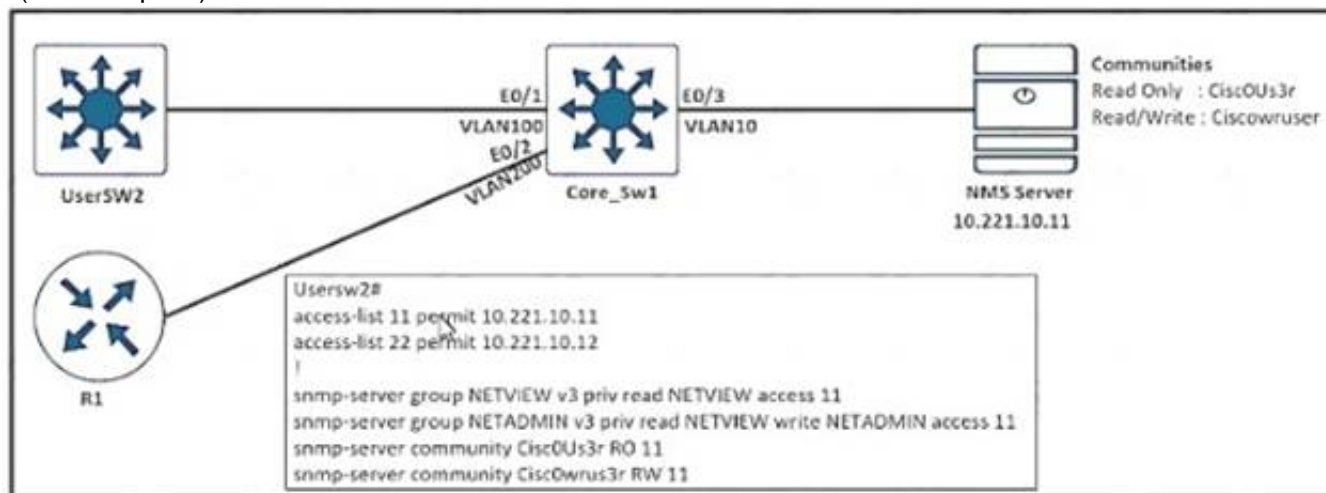
Refer to the exhibit. The administrator is troubleshooting a BGP peering between PE1 and PE3 that is unable to establish Which action resolves the issue?

- 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 73

- (Exam Topic 3)



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

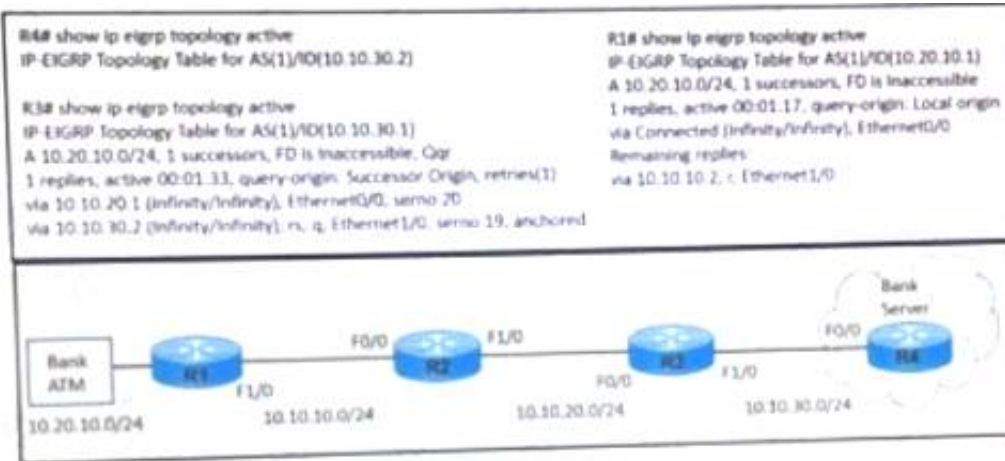
- A. snmp-server community Ciscowruser RW 11
- B. snmp-server group NETADMIN v3 priv read NETVIEW write NETADMIN access 22
- C. snmp-server community CiscoUs3r RW 11
- D. snmp-server group NETVIEW v2c priv read NETVIEW access 11

**Answer: A**

### NEW QUESTION 77

- (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 81

- (Exam Topic 3)



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

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



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

**Answer:** C

#### NEW QUESTION 83

- (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 88

- (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 93

- (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 95

- (Exam Topic 3)

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

A)

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

B)

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

C)

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

D)

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

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

**Answer: C**

**Explanation:**

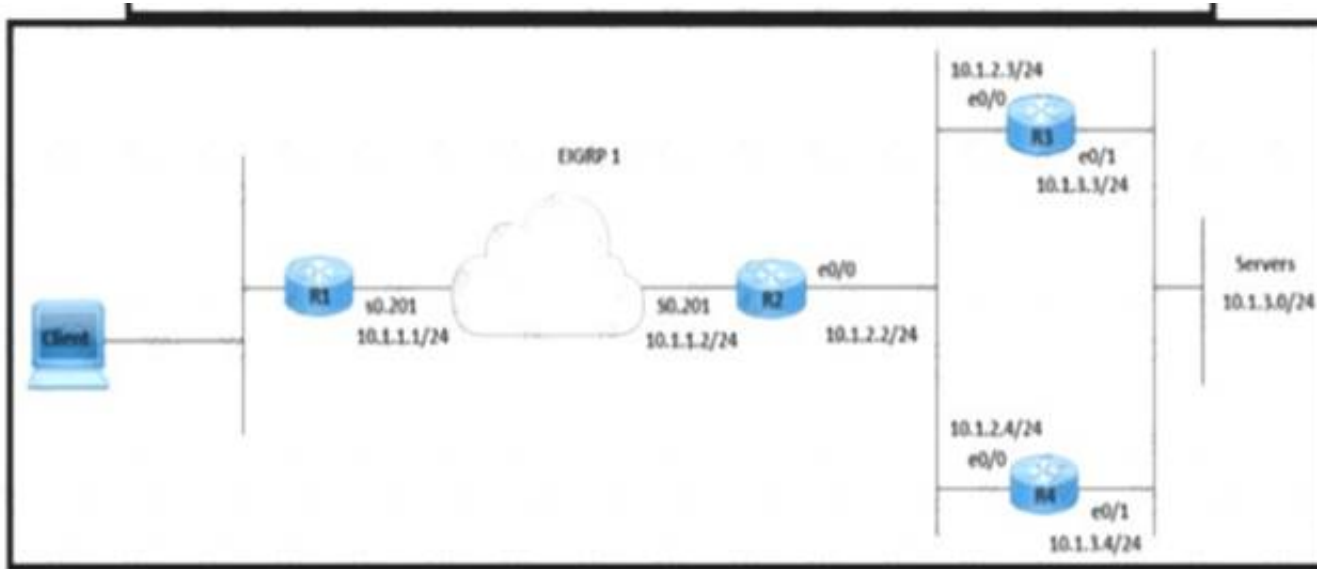
The command “ip nhrp map multicast dynamic” allows NHRP to automatically add spoke routers to the multicast NHRP mappings.

**NEW QUESTION 100**

- (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 103

- (Exam Topic 3)

Refer to the exhibit.

```

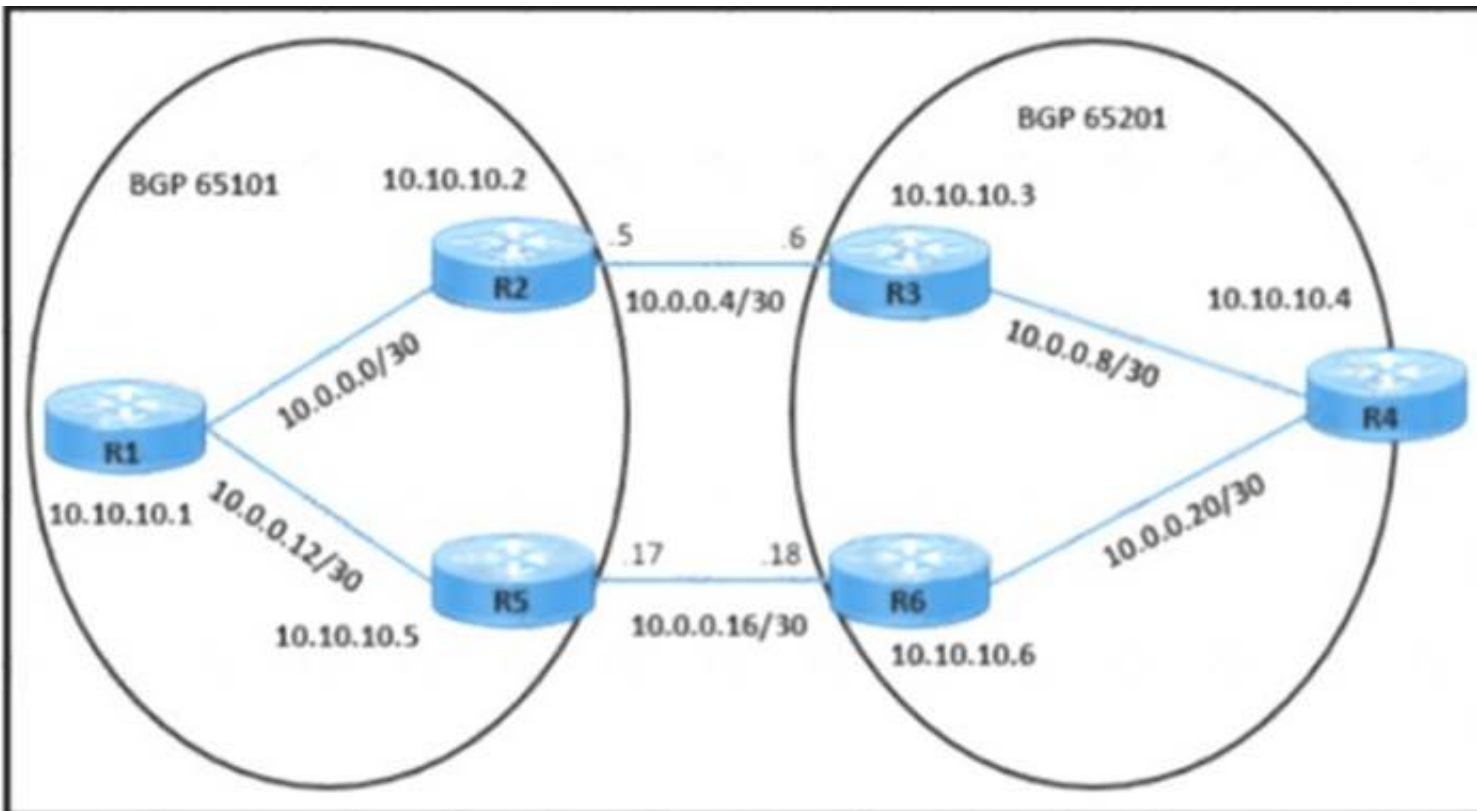
R3#
*Sep  5 07:29:34.031: %TCP-6-BADAUTH: No MD5 digest from 10.10.10.2(179) to
10.10.10.3(60942) (RST)
R2# show ip bgp neighbors 10.10.10.3
BGP neighbor is 10.10.10.3, remote AS 65201, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 00:02:19, last write 00:02:19, 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 105

- (Exam Topic 3)

Refer to the exhibit.

```

RD#
*Sep 19 00:53:43.004: BGPNSF state: 10.10.10.3 went from nsf_not_active to
nsf_not_active
*Sep 19 00:53:43.006: BGP: 10.10.10.3 went from Established to Idle
*Sep 19 00:53:43.006: BGP-5-ADJCHANGE: neighbor 10.10.10.3 Down User reset
*Sep 19 00:53:43.006: BGP: 10.10.10.3 closing
*Sep 19 00:53:43.106: BGP_Router: unhandled major event code 128, minor 0

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

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

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

**Answer: B**

#### NEW QUESTION 108

- (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 113

- (Exam Topic 3)

Which router takes an active role between two LDP neighbors when initiating LDP session negotiation and LDP TCP connection establishment?

- A. with the higher IP address
- B. with the larger number of LDP TCP neighbors
- C. with the lowest IP address
- D. with one interface in the MPLS backbone

**Answer:** A

#### NEW QUESTION 115

- (Exam Topic 3)

```
R4#
interface FastEthernet1/0
ip address 10.1.1.14 255.255.255.252
ip access-group VENDOR in
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 EIGRPKEY
speed 100
full-duplex
!
interface loopback 100
ip address 10.199.100.1 255.255.255.255
!
router eigrp 100
network 10.1.1.8 0.0.0.3
network 10.1.1.12 0.0.0.3
no auto-summary
eigrp router-id 100.4.4.4
neighbor 10.1.1.13 FastEthernet1/0
redistribute connected
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 100.4.4.4 mask 255.255.255.255
neighbor 10.1.1.13 remote-as 65001
no auto-summary
!
ip access-list extended VENDOR
permit tcp 192.168.32.0 0.0.7.255 host 10.199.100.1 eq 22 time-range VENDOR_ACCESS
!
time-range VENDOR_ACCESS
periodic weekend 22:00 to 23:00
```

Refer to the exhibit A network engineer received a call from the vendor for a failed attempt to remotely log in to their managed router loopback interface from 192.168.40.15. Which action must the network engineer take to resolve the issue?

- A. The IP access list VENDOR must be applied to interface loopback 100
- B. The time-range configuration must be changed to use absolute instead of periodic
- C. The EIGRP configuration must be updated to include a network statement for loopback 100
- D. The source IP summarization must be updated to include the vendor source IP address

**Answer:** C

#### NEW QUESTION 117

- (Exam Topic 3)



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

A)

```

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

B)

```

router eigrp 100
network 209.165.200.224 0.0.0.7
  
```

C)

```

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

D)

```

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

A. Option A

B. Option B

C. Option C

D. Option D

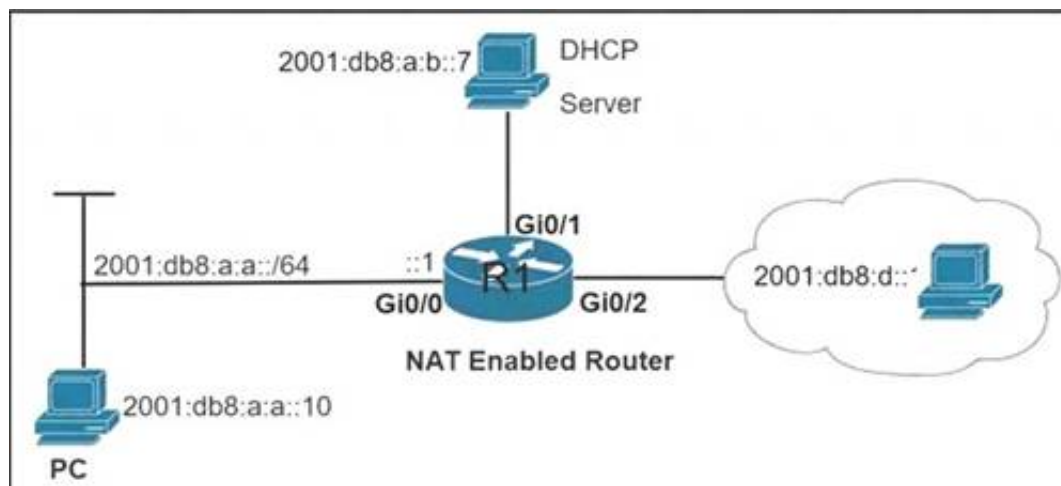
**Answer: D**

#### NEW QUESTION 120

- (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 122

- (Exam Topic 3)

How does an MPLS Layer 3 VPN differentiate the IP address space used between each VPN?

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

**Answer: A**

#### NEW QUESTION 123

- (Exam Topic 3)

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

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

The transfer fails. Which action resolves the issue?

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

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

**Answer:** B

**NEW QUESTION 127**

- (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 131**

- (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 133**

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

Reference:

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

**NEW QUESTION 137**

- (Exam Topic 3)



Refer to the exhibit. The traffic from spoke to hub is dropping. The operations team observes:

- R2-R3 link is down due to the fiber cut.
- R2 and R5 receive traffic from R1 in AS 65101.
- R3 and R5 receive traffic from R4 in AS 65201.

Which configuration resolves the issue?

- A)  
R6(config)#router bgp 65101  
R6(config-router)#no neighbor 10.0.0.17 update-source Loopback0
- B)  
R5(config)#router bgp 65101  
R5(config-router)#no neighbor 10.0.0.18 update-source Loopback0
- C)  
R6(config)#router bgp 65201  
R6(config-router)#neighbor 10.10.10.5 remote-as 65101  
R6(config-router)#neighbor 10.10.10.5 update-source Loopback0  
R6(config-router)#neighbor 10.10.10.5 ebgp-multihop 3
- D)  
R5(config)#router bgp 65101  
R5(config-router)#neighbor 10.10.10.6 remote-as 65201  
R5(config-router)#neighbor 10.10.10.6 update-source Loopback0  
R5(config-router)#neighbor 10.10.10.6 ebgp-multihop 3

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

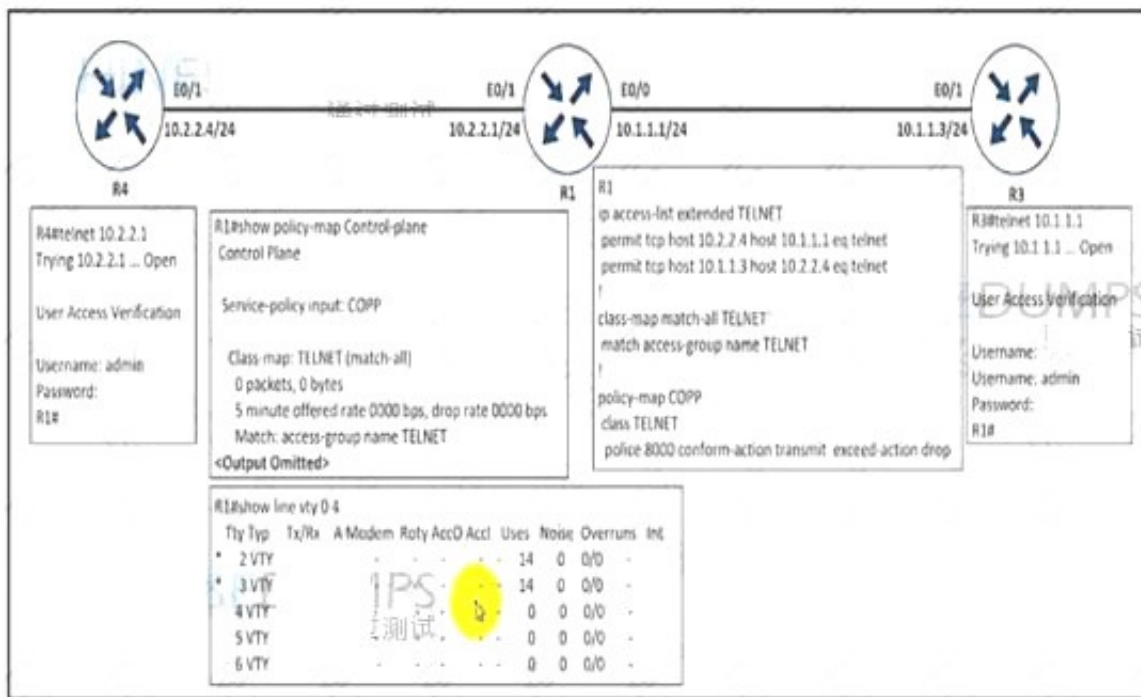
**Answer: C**

#### NEW QUESTION 141

- (Exam Topic 3)

Refer to the exhibit.





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

- ☐ policy-map COPP  
 class TELNET  
 police 8000 conform-action transmit exceed-action transmit
- ☒ policy-map COPP  
 class TELNET  
 police 8000 conform-action transmit exceed-action transmit violate-action drop
- ☐ ip access-list extended TELNET  
 permit tcp host 10.2.2.1 host 10.2.2.4 eq telnet  
 permit tcp host 10.1.1.1 host 10.1.1.3 eq telnet
- ☐ ip access-list extended TELNET  
 permit tcp host 10.2.2.4 host 10.2.2.1 eq telnet  
 permit tcp host 10.1.1.3 host 10.1.1.1 eq telnet

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

**Answer: D**

#### NEW QUESTION 145

- (Exam Topic 3)

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

**Answer: B**

#### NEW QUESTION 147

- (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?

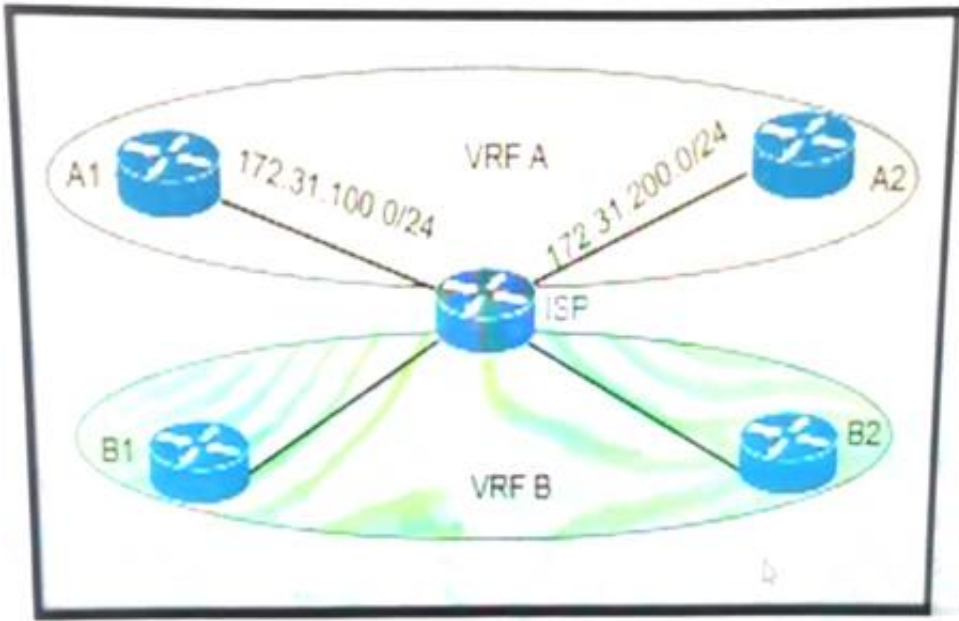
- A. Use allows in and as-override at all Pes.
- B. Use allows in and as-override at the PE-Hub.
- C. Use Allowas-in the PE\_Hub
- D. Use as-override at the PE\_Hub

**Answer: D**

#### NEW QUESTION 152

- (Exam Topic 3)

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



- A. A1interface fa0/0 description To->ISPip add 172.31.100.1 255.255.255.0no shut!router ospf 100net 172.31.100.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISPip add 172.31.200.1 255.255.255.0no shut!router ospf 100net 172.31.200.1 0.0.0.255 area 0
- B. A1interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.100.1 255.255.255.0no shut!router ospf 100net 172.31.100.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.200.1 255.255.255.0no shut!router ospf 100net 172.31.200.1 0.0.0.255 area 0
- C. A1interface fa0/0 description To->ISPip add 172.31.200.1 255.255.255.0no shut!router ospf 100net 172.31.200.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISPip add 172.31.100.1 255.255.255.0no shut!router ospf 100net 172.31.100.1 0.0.0.255 area 0
- D. A1interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.100.1 255.255.255.0no shut!router ospf 100 vrf Anet 172.31.200.1 0.0.0.255 area 0 A2interface fa0/0 description To->ISP ip vrf forwarding Aip add 172.31.100.1 255.255.255.0no shut!router ospf 100 vrf Anet 172.31.200.1 0.0.0.255 area 0

**Answer: C**

**Explanation:**

A1 and A2 routers do not know they belong to VRF A. The two interfaces of ISP (which are connected to A1 & A2) should be configured like this (we only show the configure of one interface):

ISP router:

interface g0/0

description ISP->To\_CustomerA ip vrf forwarding A

ip address 172.31.100.2 255.255.255.0

router ospf 100 vrf A

network 172.31.200.2 0.0.0.255 area 0

**NEW QUESTION 157**

- (Exam Topic 3)

Refer to the exhibit.

```
access-list 1 permit 209.165.200.215
access-list 2 permit 209.165.200.216
!
interface ethernet 1
ip policy route-map Texas
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next-hop 209.165.200.217
!
route-map Texas permit 20
match ip address 2
set ip next-hop 209.165.200.218
```

Packets arriving from source 209.165.200.215 must be sent with the precedence bit set to 1, and packets arriving from source 209.165.200.216 must be sent with the precedence bit set to 5. Which action resolves the issue?

- A. set ip precedence critical in route-map Texas permit 10
- B. set ip precedence critical in route-map Texas permit 20
- C. set ip precedence immediate in route-map Texas permit 10
- D. set ip precedence priority in route-map Texas permit 20

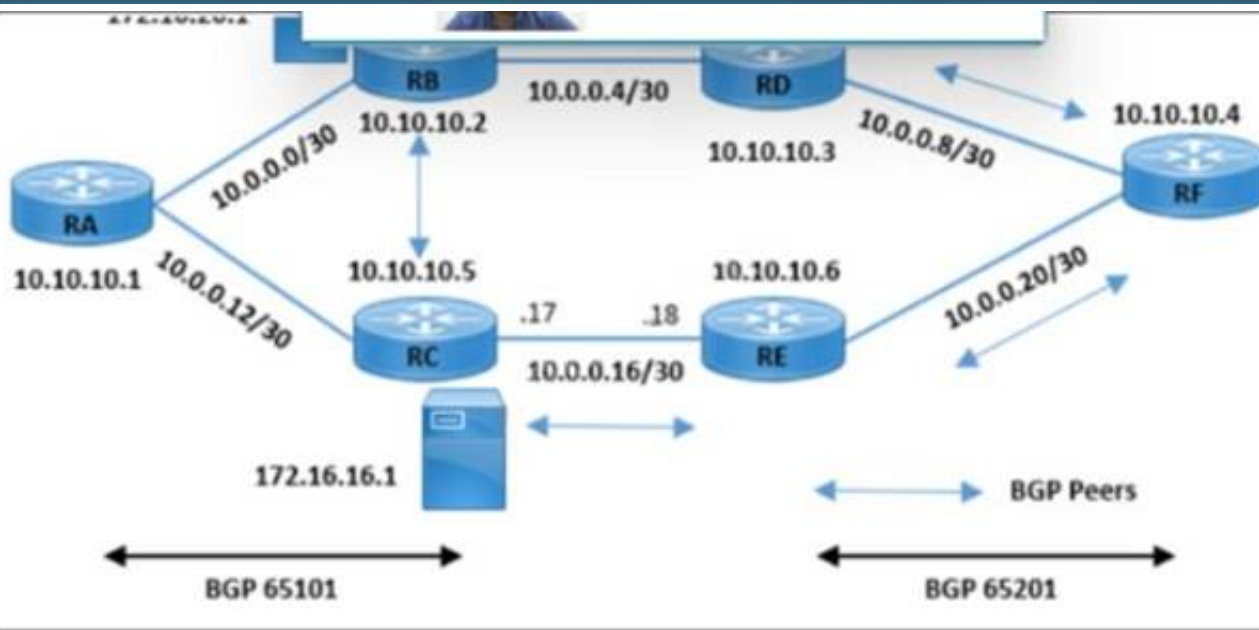
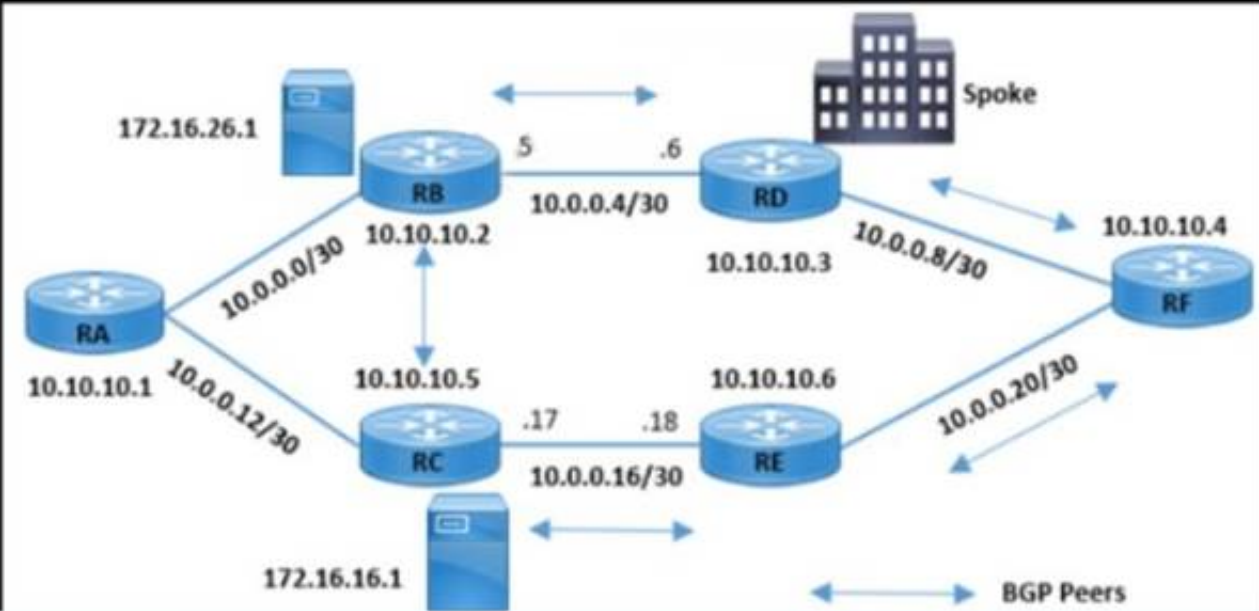
**Answer: B**

**NEW QUESTION 158**

- (Exam Topic 3)

```
RB#show ip bgp 172.16.16.1
BGP routing table entry for 172.16.16.1/32, version 11
Paths: (1 available, no best path)
Not advertised to any peer
Local
 10.10.10.5 (metric 3) from 10.10.10.5 (172.16.16.1)
  Origin IGP, metric 0, localpref 100, valid, internal, not synchronized

RD#traceroute 172.16.16.1
Tracing the route to 172.16.16.1
 1 10.0.0.10 [MPLS: Label 29 Exp 0] 64 msec 56 msec 60 msec
 2 10.0.0.21 60 msec 56 msec 72 msec
 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 163

- (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 168**

- (Exam Topic 3)

Which mechanism provides traffic segmentation within a DMVPN network?

- A. RSVP
- B. BGP
- C. MPLS
- D. iPsec

**Answer: C**

**Explanation:**

To use the DMVPN – Traffic Segmentation Within DMVPN feature you must configure Multiprotocol Label Switching (MPLS) by using the mpls ip command.  
Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_conn\\_dmvpn/configuration/xr-16/sec-conn-dmvpn-xr-16-book/sec-conn-dmvpn-dmvpn.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xr-16/sec-conn-dmvpn-xr-16-book/sec-conn-dmvpn-dmvpn.html)

**NEW QUESTION 173**

- (Exam Topic 3)

```
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 Ethernet0/0 203.0.113.1 name ISP1 track 1
ip route 0.0.0.0 0.0.0.0 Ethernet0/1 198.51.100.1 2 name ISP2
```

Refer to the exhibit. After recovering from a power failure, Ethernet0/1 stayed down while Ethernet0/0 returned to the up/up state. The default route through ISP1 was not reinstated in the routing table until Ethernet0/1 also came up. Which action resolves the issue?

- A. Reference the track object 1 in both static default routes
- B. Remove the references to the interface names from both static default routes
- C. Configure the default route through ISP1 with a higher administrative distance than 2.
- D. Add a static route to the 8.8.8.8/32 destination through the next hop 203.0.113.1

**Answer: D**

**NEW QUESTION 176**

- (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 of 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 177**

- (Exam Topic 3)

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

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

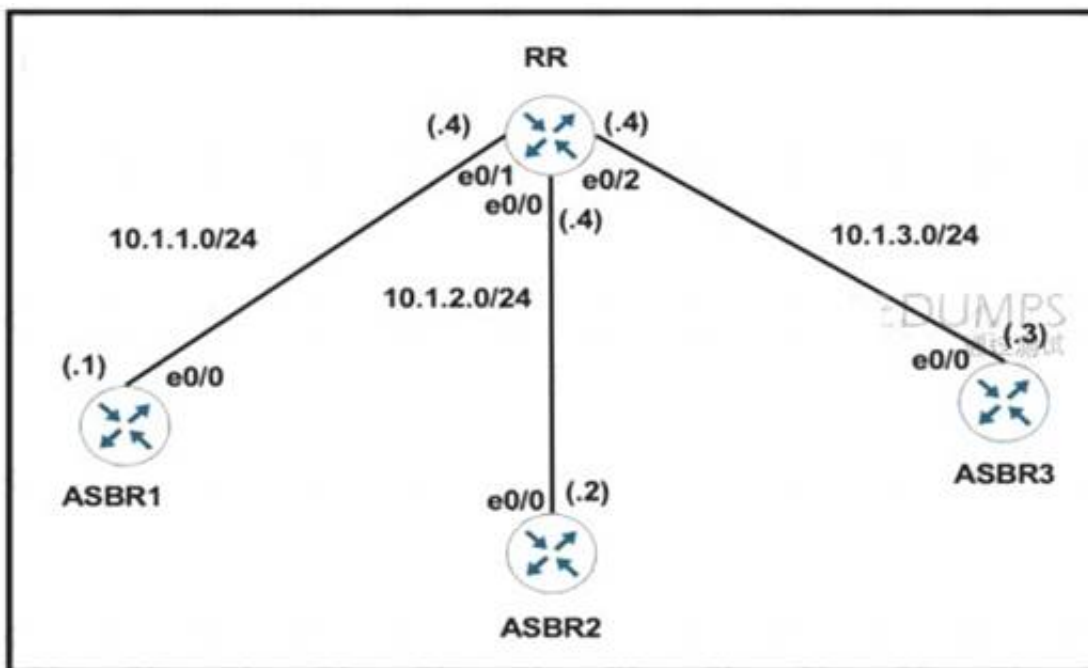
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

#### NEW QUESTION 179

- (Exam Topic 3)

Refer to the exhibit.



RR Configuration:

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

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

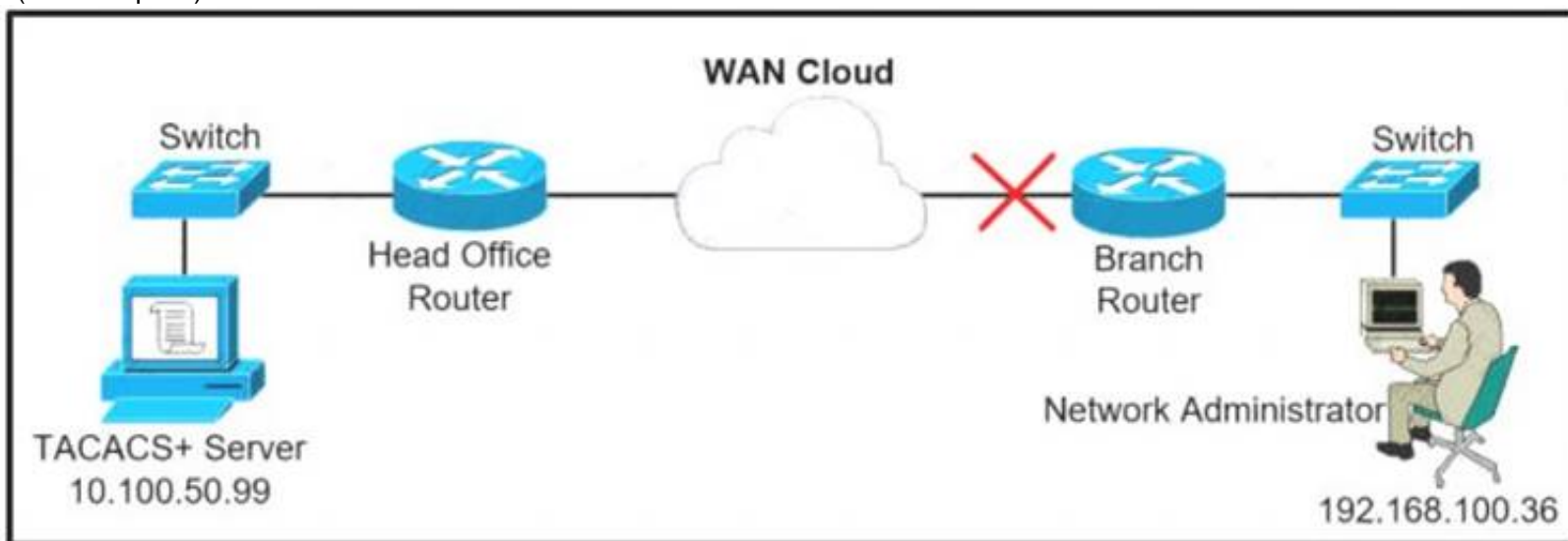
- ☒ router bgp 100  
neighbor 10.1.1.1 next-hop-self  
neighbor 10.1.2.2 next-hop-self  
neighbor 10.1.3.3 next-hop-self
- ☐ router bgp 100  
neighbor IBGP update-source Loopback0
- ☐ router bgp 100  
neighbor IBGP next-hop-self
- ☒ router bgp 100  
neighbor 10.1.1.1 peer-group IBGP  
neighbor 10.1.2.2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

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

**Answer: D**

#### NEW QUESTION 184

- (Exam Topic 3)



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

```
aaa new-model
aaa authorization commands 15 default group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
tacacs-server host 10.100.50.99
tacacs-server key Ci$co123
```

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

- A. aaa authentication login default group tacacs+ local
- B. aaa authentication login default group tacacs+ enable
- C. aaa authentication login default group tacacs+ console
- D. aaa authentication login console group tacacs+ enable

**Answer: A**

#### Explanation:

With the “aaa authentication login default group tacacs+ local ” command configured, when logging in, the password supplied will be attempted to be verified by the TACACS+ server before access is granted. If the server is unavailable/unreachable, then the switch will fall back to using the local authentication database.

#### NEW QUESTION 189

- (Exam Topic 3)

An engineer must establish a connection between two CE routers for two customers with overlapping IP addresses Customer\_a is connected to interfaces Gig0/0, and Customer\_b is connected to interfaces Gig0/1. Routers CE1 and CE2 are configured as follows:

```
ip vrf customer_a
rd 1:1
route-target both 1:1
!
ip vrf customer_b
rd 2:2
route-target both 2:2
```

Drag and drop the code snippets from the right onto the boxes in the configuration to establish the needed connection. Snippets may be used more than once.



CE1

interface Gig0/0

ip vrf forwarding

ip address

!

interface Gig0/1

ip vrf forwarding

ip address

customer\_a

customer\_b

192.168.1.1 255.255.255.0

192.168.1.2 255.255.255.0

CE2

interface Gig0/0

ip vrf forwarding

ip address

!

interface Gig0/1

ip vrf forwarding

ip address

customer\_a

customer\_b

192.168.1.1 255.255.255.0

192.168.1.2 255.255.255.0

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

CE1

interface Gig0/0

ip vrf forwarding

ip address

!

interface Gig0/1

ip vrf forwarding

ip address

customer\_a

customer\_b

192.168.1.1 255.255.255.0

192.168.1.2 255.255.255.0

CE2

interface Gig0/0

ip vrf forwarding

ip address

!

interface Gig0/1

ip vrf forwarding

ip address

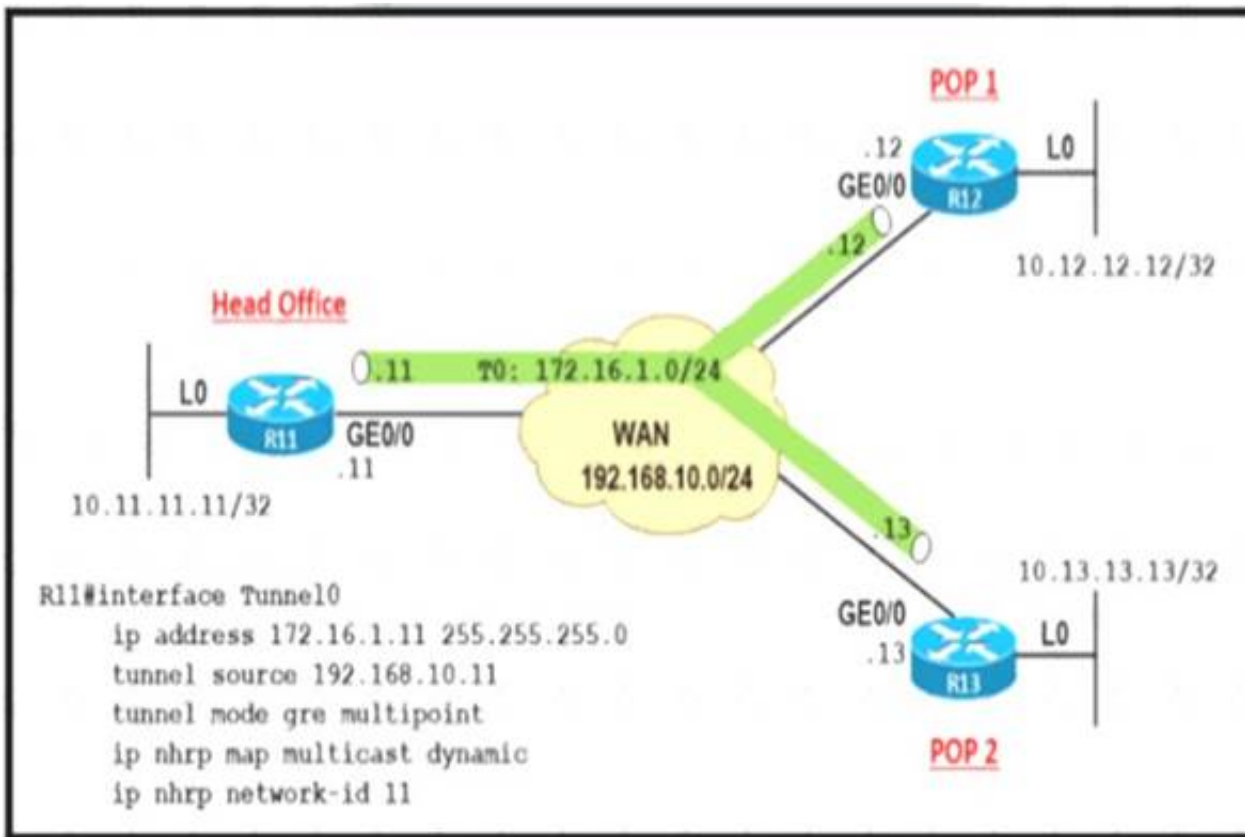
customer\_a

customer\_b

192.168.1.1 255.255.255.0

192.168.1.2 255.255.255.0

NEW QUESTION 194  
- (Exam Topic 3)



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

☐ R12#  
**interface Tunnel0**  
**ip nhrp map multicast 192.168.10.11**  
**ip nhrp map 172.16.1.11 192.168.10.11**  
**ip nhrp network-id 12**  
**ip nhrp nhs 172.16.1.11**

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

☐ R12#  
**interface Tunnel0**  
**ip nhrp map multicast 172.16.1.11**  
**ip nhrp map 172.16.1.11 192.168.10.11**  
**ip nhrp network-id 12**  
**ip nhrp nhs 192.168.10.11**

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

☐ Configure routers R12 and R13 as:

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

☐ Configure routers R12 and R13 as:

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

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

Answer: D

#### NEW QUESTION 195

- (Exam Topic 3)

Refer to the exhibit.

```
R2#show running-config | section ospf
ip ospf 1 area 1
ip ospf 1 area 1
router ospf 1
log-adjacency-changes
area 1 stub no-summary
R2#show ip ospf interface brief
```

Interface	PtID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Lo0	1	1	10.0.0.2/32	1	Loop	0/0	
Fa0/0	1	1	10.10.10.1/30	1	DR	0/1	

```
R2#show running-config interface fastEthernet 0/0
Building configuration...

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

R2#show ip ospf neighbor
```

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

```
R1#show running-config | section ospf
ip ospf 1 area 0
ip ospf 1 area 1
router ospf 1
log-adjacency-changes
area 1 stub no-summary
R1#show ip ospf interface brief
```

Interface	PtID	Area	IP Address/Mask	Cost	State	Nbrs	F/C
Lo0	1	0	10.0.0.1/32	1	LOOP	0/0	
Lo0	1	1	10.10.10.2/30	1	BDR	0/1	

```
R1#show running-config interface fastEthernet 1/0
Building configuration...

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

R1#show ip ospf neighbor
```

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

Which action restores OSPF adjacency between R1 and R2?

- A. Change the IP MTU of R1 Fa1/0 to 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 198

- (Exam Topic 3)

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



```

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

```

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

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

**Answer: C**

**Explanation:**

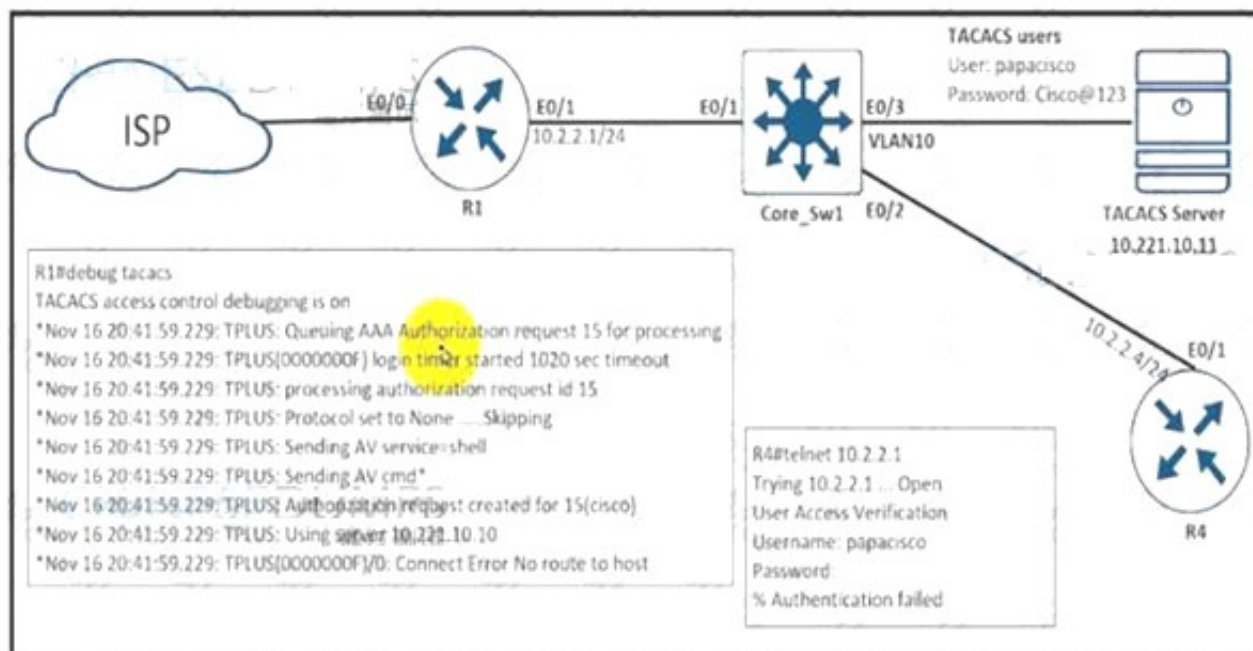
The last command “aaa authentication login telnet group TAC-SERV” created the method list name telnet so we need to assign it to line vty.

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

**NEW QUESTION 203**

- (Exam Topic 3)

Refer to the exhibit.



An engineer is trying to connect to R1 via Telnet with no success. Which configuration resolves the issue?

- ☐ tacacs server prod  
 address ipv4 10.221.10.10  
 exit
- ☒ ip route 10.221.10.10 255.255.255.255 ethernet 0/1
- ☐ tacacs server prod  
 address ipv4 10.221.10.11  
 exit
- ☐ ip route 10.221.0.11 255.255.255.255 ethernet 0/1

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

**Answer: B**

**NEW QUESTION 207**

- (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

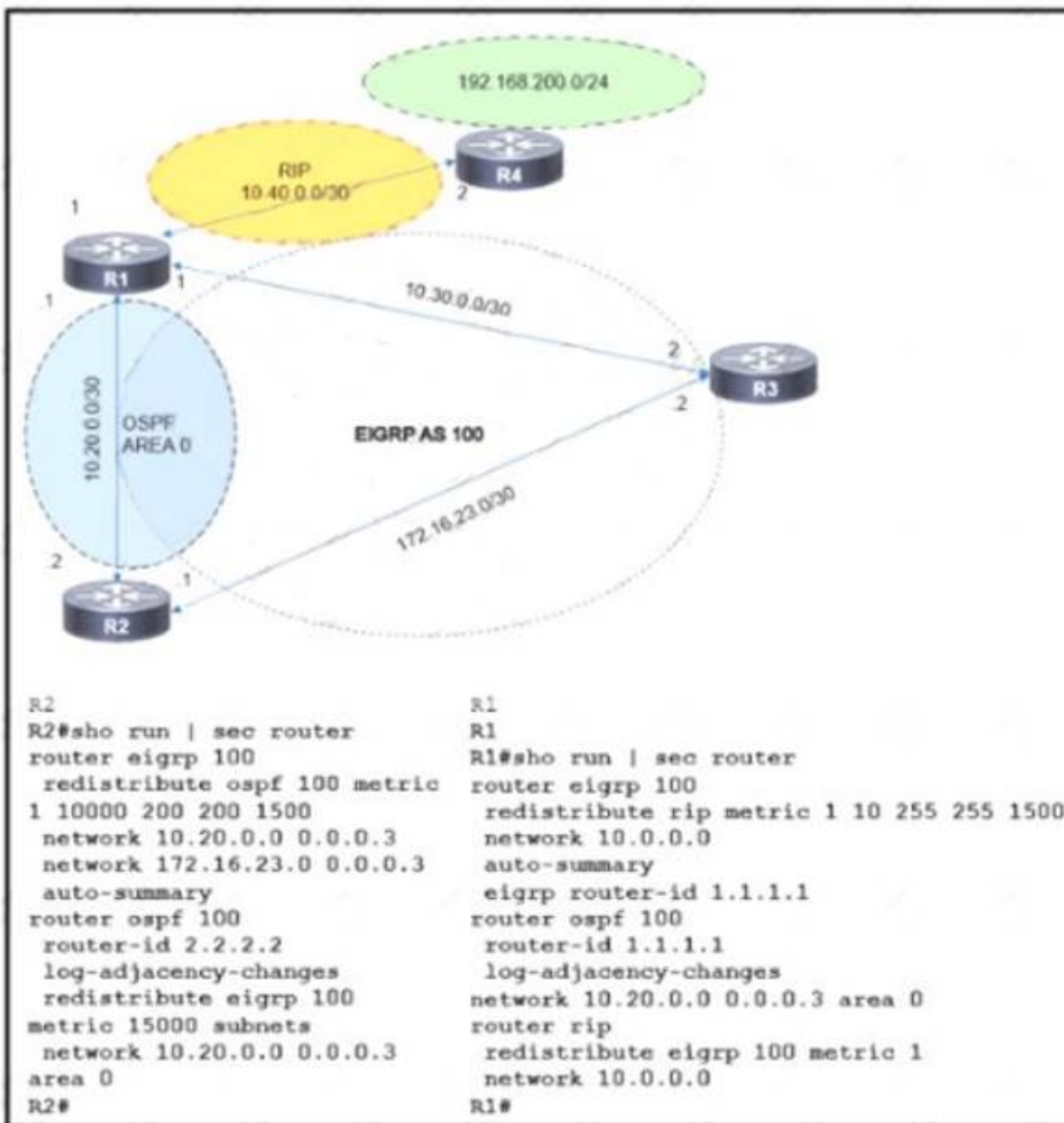
Refer to the exhibit. After reloading the router an administrator discovered that the interface utilization graphs displayed inconsistencies with their previous history in the NMS. Which action prevents this issue from occurring after another router reload in the future?

- 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 210

- (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?

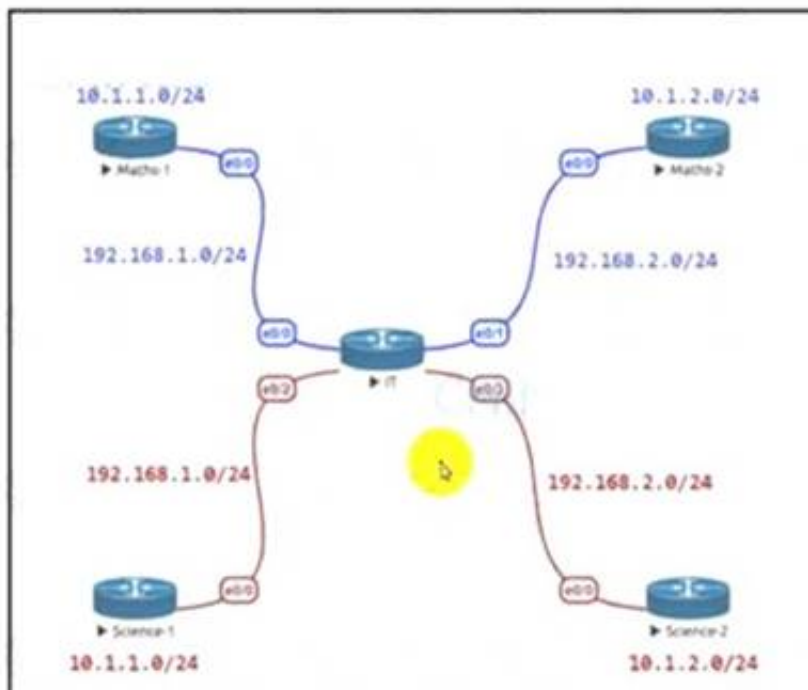
- ☒ R2(config)#router ospf 100  
R2(config-router)#no redistribute eigrp 100  
R2(config-router)#redistribute eigrp 100 metric 1 subnets
- ☐ R1(config)#no router rip  
R1(config)#ip route 192.168.200.0 255.255.255.0 10.40.0.2
- ☐ R2(config)#router eigrp 100  
R2(config-router)#no redistribute ospf 100  
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 211**

- (Exam Topic 3)



IT Router

```
vrf definition Science
 address-family ipv4
```

```

!
Interface E 0/2
  Vrf forwarding Science
  Ip address 192.168.1.1 255.255.255.0
  No shut
!
Interface E 0/3
  Vrf forwarding Science

```

```
!
Interface E 0/3
Vrf forwarding Science
Ip address 192.168.2.1 255.255.255.0
No shut
```

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

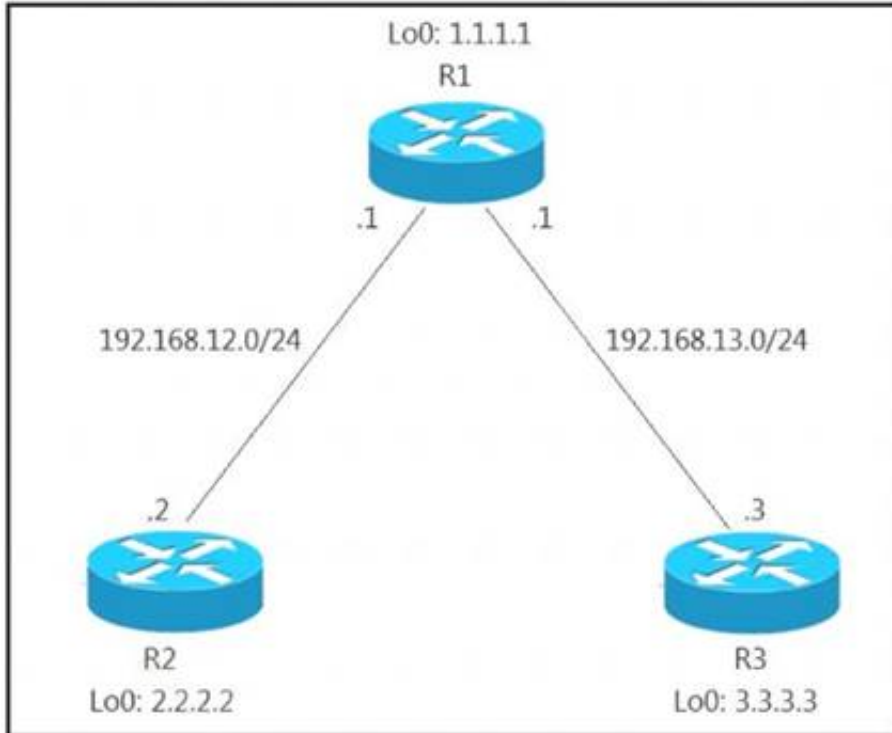
**Answer: D**

**NEW QUESTION 216**

- (Exam Topic 3)



Refer to the exhibit.



An engineer has configured R1 as EIGRP stub router. After the configuration, router R3 failed to reach to R2 loopback address. Which action advertises R2 loopback back into the R3 routing table?

- A. Add a static route for R2 loopback address in R1 and redistribute it to advertise to R3.
- B. Use a leak map on R1 that matches the required prefix and apply it with the distribute list command toward R3.
- C. Use a leak map on R3 that matches the required prefix and apply it with the EIGRP stub feature.
- D. Add a static null route for R2 loopback address in R1 and redistribute it to advertise to R3.

**Answer: B**

**Explanation:**

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

```
R1(config)#ip access-list standard R2_L0
R1(config-std-nacl)#permit host 2.2.2.2
R1(config)#route-map R2_L0_LEAK
R2(config-route-map)#match ip address R2_L0
R1(config)#router eigrp 1
R1(config-router)#eigrp stub leak-map R2_L0_LEAK
```

**NEW QUESTION 219**

- (Exam Topic 3)

Which MPLS value is combined with the IP prefix to convert to a VPNv4 prefix?

- A. 16-byte Route Distinguisher
- B. 8-byte Route Target
- C. 16-byte Route Target
- D. 8-byte Route Distinguisher

**Answer: D**

**NEW QUESTION 221**

- (Exam Topic 3)

How do devices operate in MPLS L3VPN topology?

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

**Answer: C**

**NEW QUESTION 224**

- (Exam Topic 3)

Refer to the exhibit.

```
Dallas_Router:

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

ip access-list extended GUEST-ACCESS
remark Internet Access Only
permit udp any any eq bootpc
permit udp any any eq bootps
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip any 224.0.0.0 31.255.255.255
deny ip any 169.254.0.0 0.0.255.255
deny ip any 127.0.0.0 0.255.255.255
deny ip any 192.0.2.0 0.0.0.255
deny ip any host 0.0.0.0
permit ip 10.66.42.0 0.0.0.255 any
permit ip 10.66.46.0 0.0.0.255 any
!

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

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

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

Answer: C

#### NEW QUESTION 228

- (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?

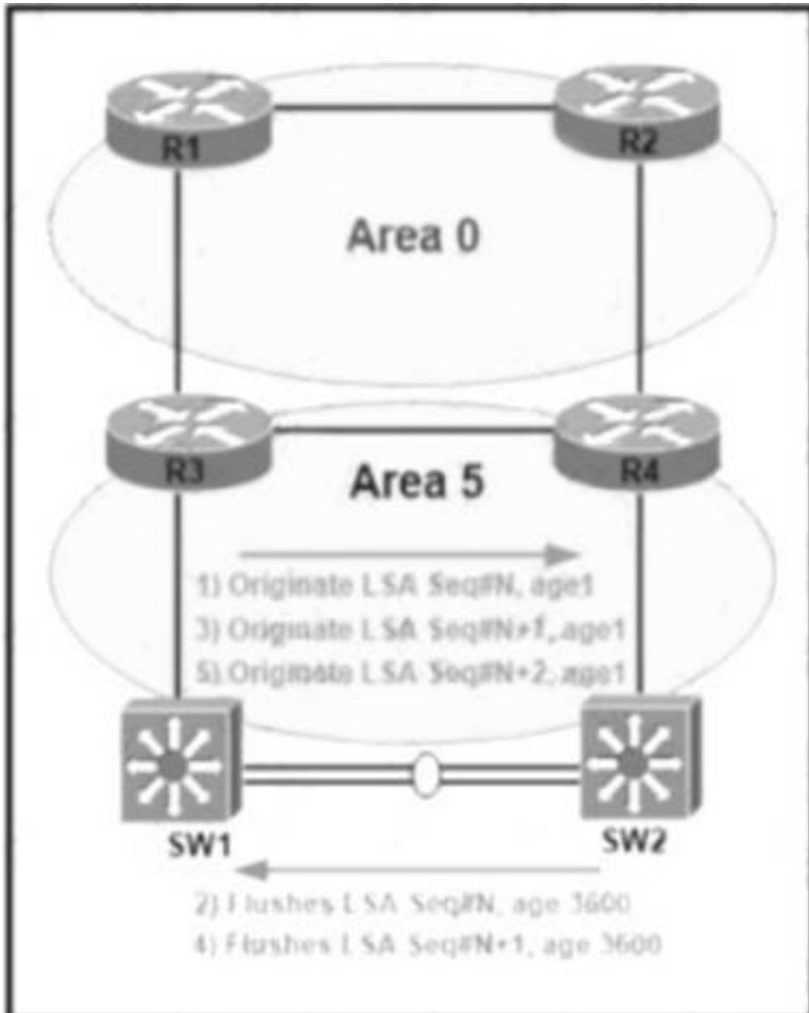
- A. Change the R1 dead timer to 20.
- B. Change the R2 dead timer to 20.
- C. Change the R2 hello timer to 20.
- D. Change the R1 hello timer to 20.

Answer: A

#### NEW QUESTION 230

- (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 232

- (Exam Topic 3)

Refer to the exhibit.

```
R1#sh run | s bgp
router bgp 65001
no synchronization
bgp router-id 10.100.1.50
bgp log-neighbor-changes
network 10.1.1.0 mask 255.255.255.252
network 10.1.1.12 mask 255.255.255.252
network 10.100.1.50 mask 255.255.255.255
timers bgp 20 60
neighbor R2 peer-group
neighbor R4 peer-group
neighbor 10.1.1.2 remote-as 65001
neighbor 10.1.1.2 peer-group R2
neighbor 10.1.1.14 remote-as 65001
neighbor 10.1.1.14 peer-group R4
no auto-summary
```

While troubleshooting a BGP route reflector configuration, an engineer notices that reflected routes are missing from neighboring routers. Which two BGP configurations are needed to resolve the issue? (Choose two)

- A. neighbor 10.1.1.14 route-reflector-client
- B. neighbor R2 route-reflector-client
- C. neighbor 10.1.1.2 allowas-in
- D. neighbor R4 route-reflector-client
- E. neighbor 10.1.1.2 route-reflector-client

**Answer: AE**

#### NEW QUESTION 234

- (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 GigabitEthernet2 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 239**

- (Exam Topic 3)

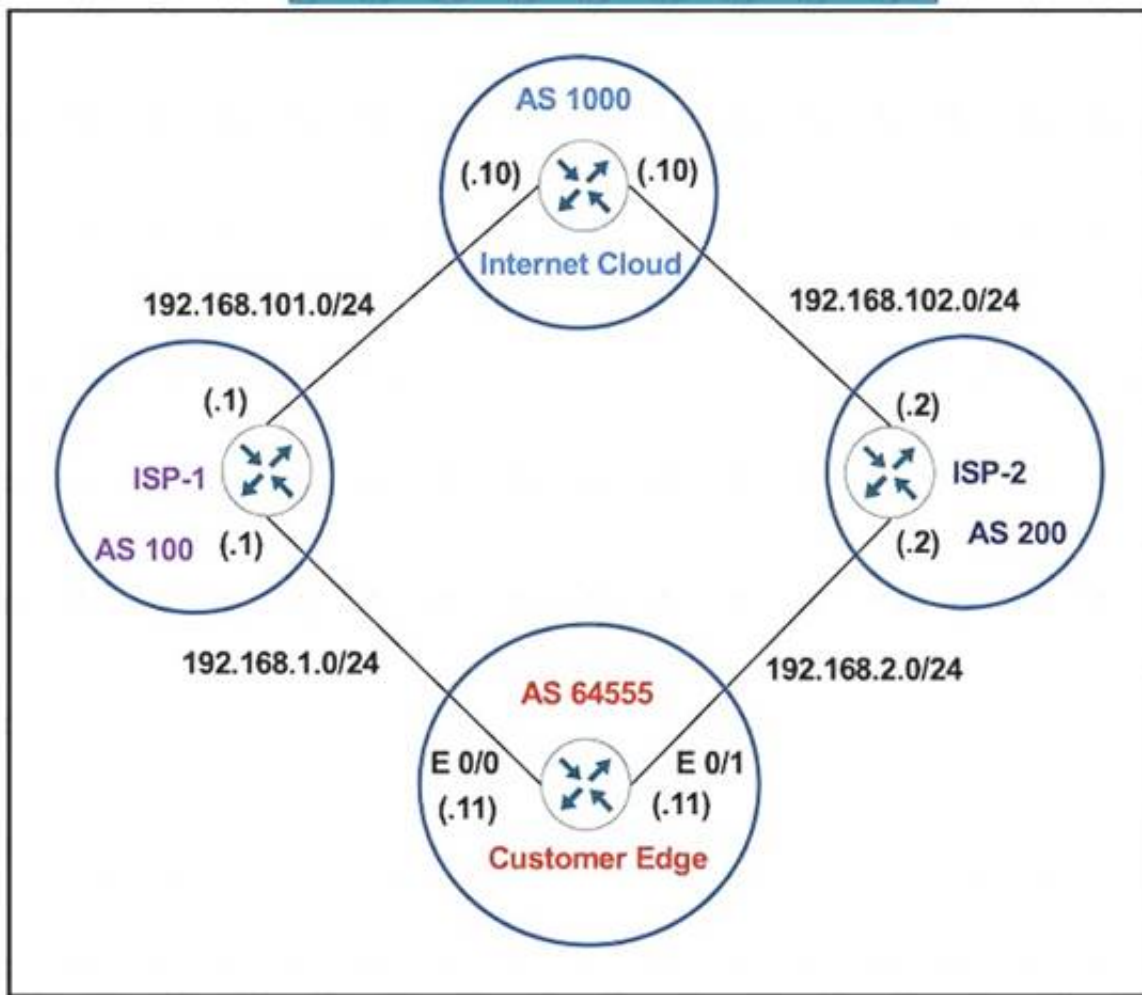
What action is performed for untagged outgoing labels in an MPLS router?

- 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 243**

- (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)

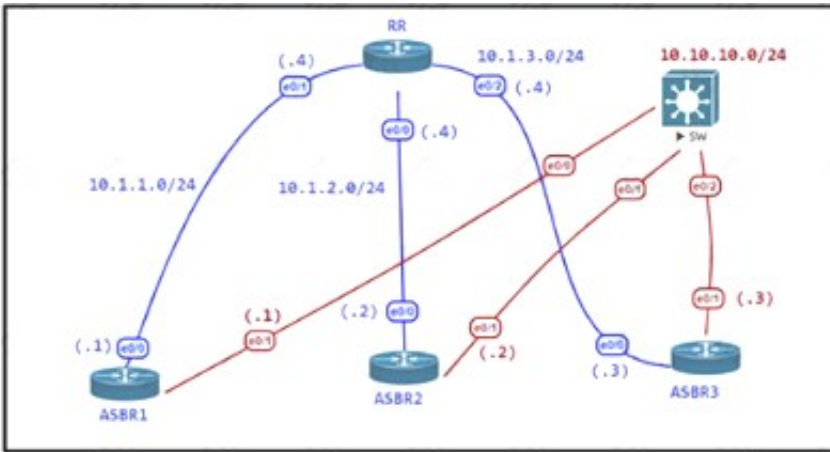
```
route-map SETAS
set as-path prepend 111
!
router bgp 64555
neighbor 192.168.1.1 remote-as 100
neighbor 192.168.2.2 remote-as 200
neighbor 192.168.2.2 route-map SETAS out
```

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

**Answer:** C**NEW QUESTION 247**

- (Exam Topic 3)

Exhibits:



#### 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
```

#### 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
```

Refer to the exhibit The administrator configured the network devices for end-to-end reachability, but the ASBRs are not propagating routes to each other Which set of configurations resolves this issue?

- ☐ 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
- ☐ 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
- ☐ router bgp 100  
 neighbor 10.1.1.1 next-hop-self  
 neighbor 10.1.2.2 next-hop-self  
 neighbor 10.1.3.3 next-hop-self
- ☐ router bgp 100  
 neighbor 10.1.1.1 ebgp-multihop  
 neighbor 10.1.2.2 ebgp-multihop  
 neighbor 10.1.3.3 ebgp-multihop

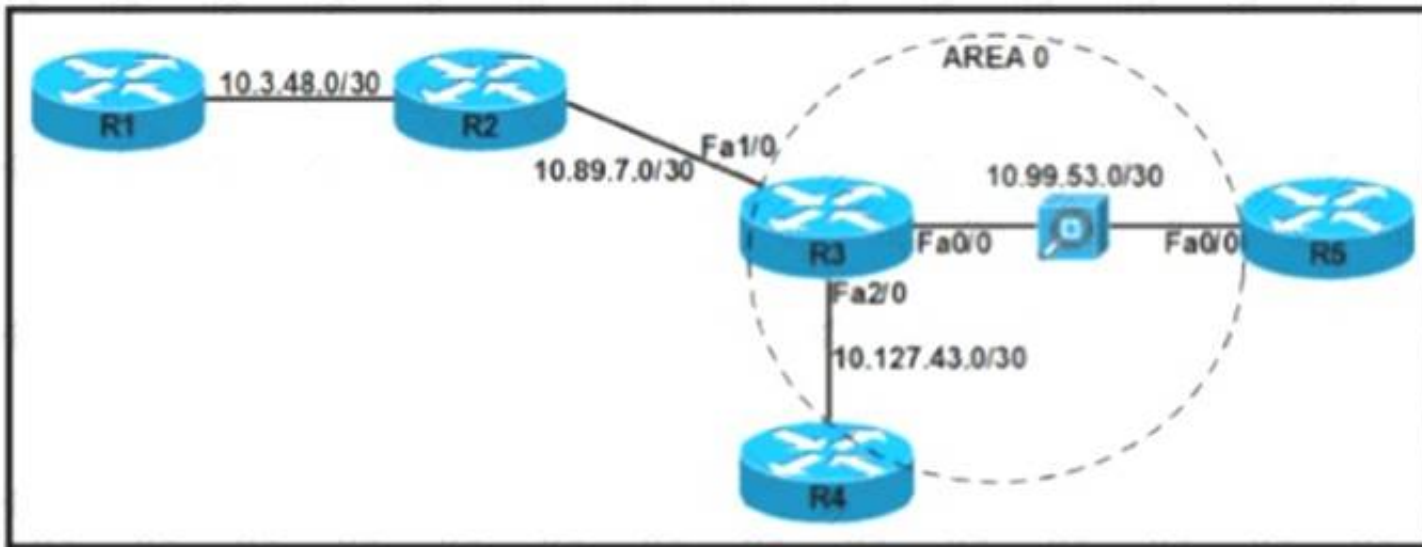
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

#### **NEW QUESTION 249**

- (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)

```

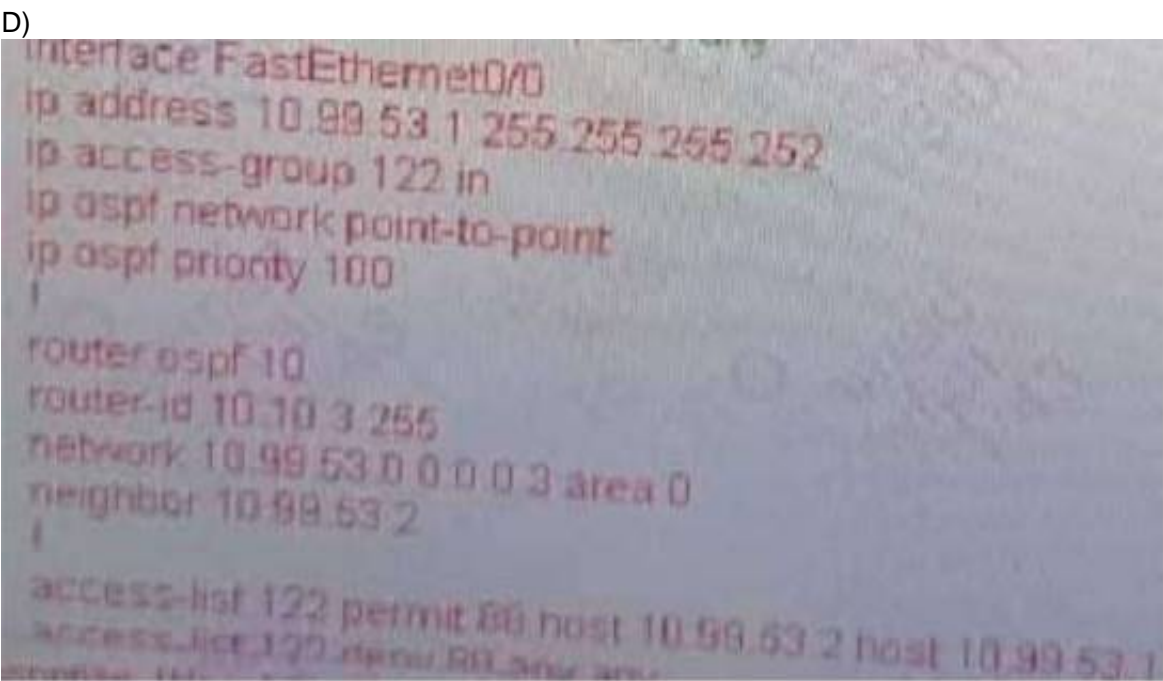
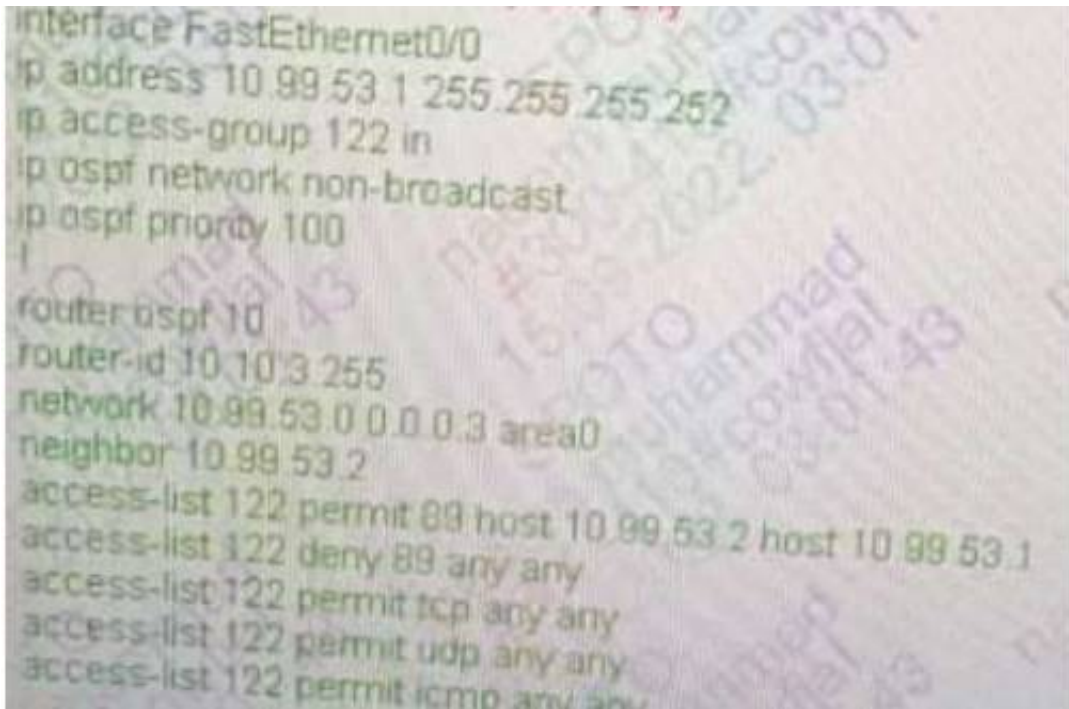
interface FastEthernet0/0
ip address 10.99.53.1 255.255.255.252
ip access-group 122 in
ip ospf network non-broadcast
ip ospf priority 0
!

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)



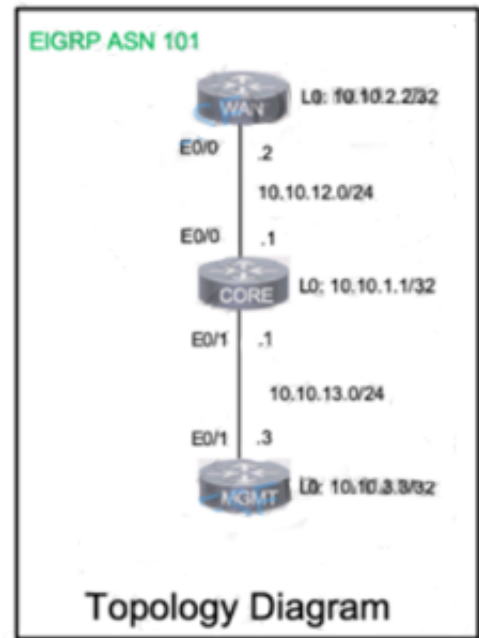
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 253

- (Exam Topic 3)

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



Guidelines Topology **Tasks**

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

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

WAN

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

WAN CORE MGMT

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

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

CORE



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

```
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.10.12.1 255.255.255.0
 duplex auto
!
interface Ethernet0/1
 ip address 10.10.13.1 255.255.255.0
 duplex auto
!
```

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

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

MGMT

```

WAN  CORE  MGMT
interface Loopback0
ip address 10.10.3.3 255.255.255.255
!
interface Loopback1
ip address 172.16.3.3 255.255.255.0
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface Ethernet0/1
ip address 10.10.13.3 255.255.255.0
duplex auto
!
interface Ethernet0/2
no ip address
shutdown
duplex auto
!
interface Ethernet0/3
no ip address
shutdown
duplex auto
!
!
router eigrp 101
network 10.10.0.0 0.0.255.255
network 172.16.3.0 0.0.0.255
eigrp router-id 10.10.3.3

```

```

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

```

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

```

access-list 120 remark *** ACL for CoPP-Critical ***
access-list 120 permit ip 10.10.0.0 0.0.255.255 any
access-list 120 permit ip any any
access-list 120 permit ip any 10.10.0.0 0.0.255.255
access-list 121 permit icmp 10.10.0.0 0.0.255.255 any
access-list 121 permit tcp 10.10.0.0 0.0.255.255 any eq 22
access-list 121 permit tcp 10.10.0.0 0.0.255.255 any eq telnet
access-list 122 remark *** ACL for CoPP-NORMAL ***
access-list 122 permit udp 10.10.0.0 0.0.255.255 any
access-list 122 permit udp any 10.10.0.0 0.0.255.255
access-list 122 permit udp any 10.10.0.0 0.0.255.255 range 33434 33464
access-list 122 permit udp 10.10.0.0 0.0.255.255 any range 33434 33464
!
control-plane
service-policy input CoPP
!
!
!

```

CORE# Copy run start TESTING: CORE

Graphical user interface Description automatically generated with medium confidence

```

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

```

MGMT

Graphical user interface, text Description automatically generated

```

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

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open

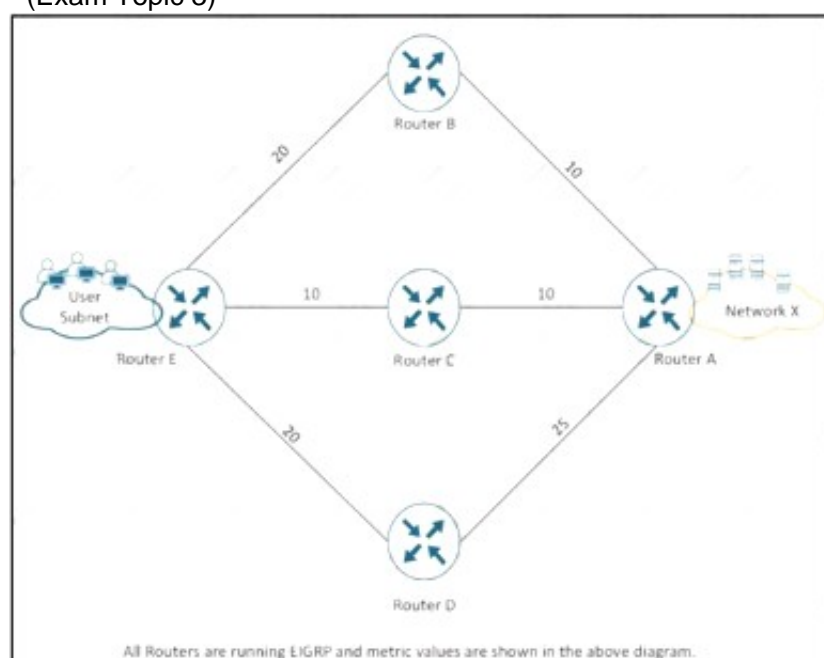
Password required, but none set

[Connection to 10.10.13.1 closed by foreign host]
MGMT#

```

## NEW QUESTION 254

- (Exam Topic 3)



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

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

**Answer: A**

## NEW QUESTION 255



- (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 260**

- (Exam Topic 3)

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

A)

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

B)

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

C)

```
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

D)

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

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

**Answer: A**

**NEW QUESTION 265**

- (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 269

- (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 274

- (Exam Topic 3)

Refer to the exhibit.

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

Which command must be configured to make VRF CCNP work?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 276

- (Exam Topic 3)

Which protocol must be secured with MD-5 authentication across the MPLS cloud to prevent hackers from introducing bogus routers?

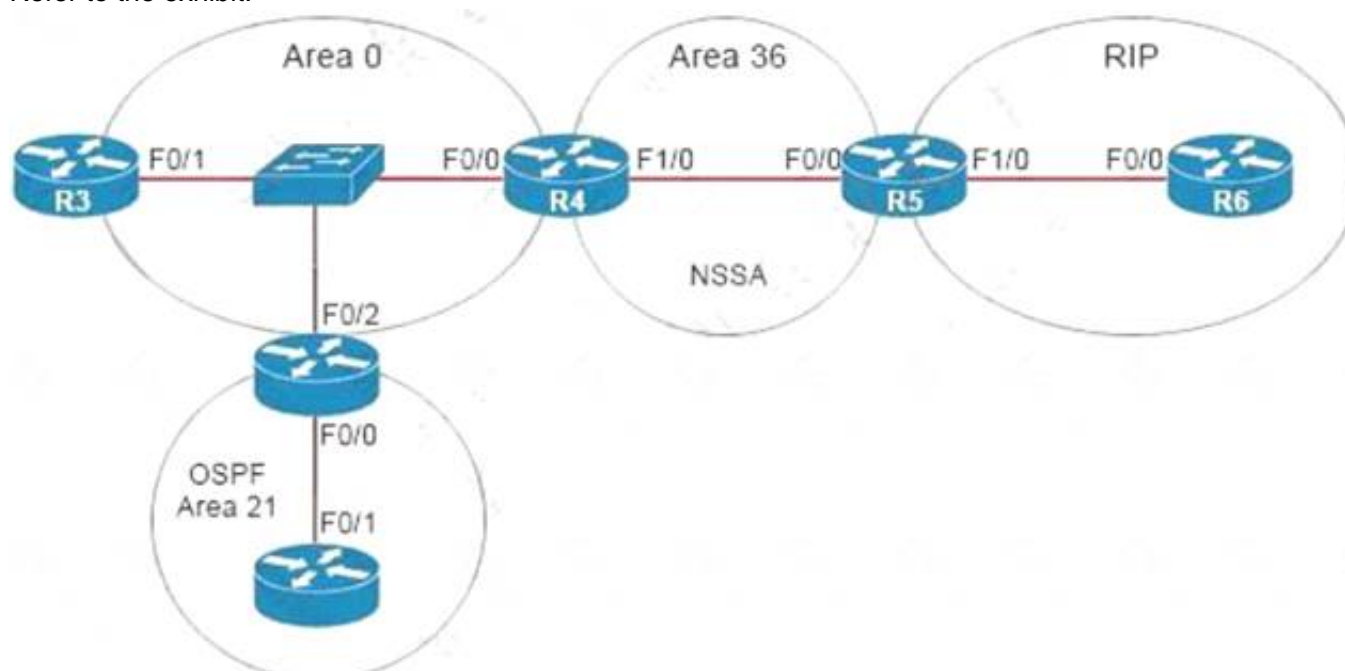
- A. MP-BGP
- B. LSP
- C. RSVP
- D. LDP

**Answer: A**

#### NEW QUESTION 279

- (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 282**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 286**

- (Exam Topic 3)

How is VPN routing information distributed in an MPLS network?

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

**Answer:** C

**Explanation:**

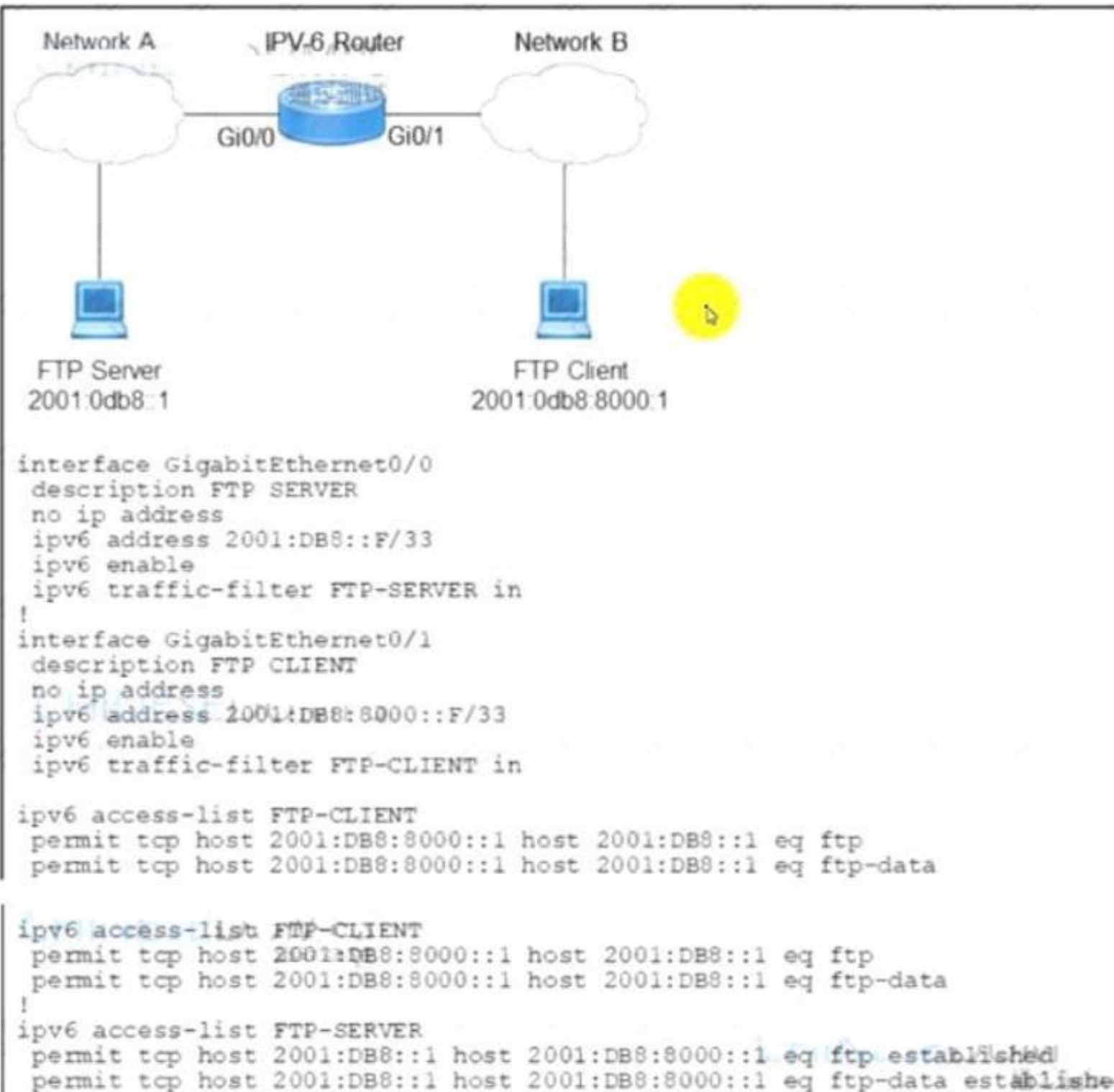
The distribution of virtual private network (VPN) routing information is controlled through the use of VPN route target communities, implemented by Border Gateway Protocol (BGP) extended communities.

Reference:

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

**NEW QUESTION 289**

- (Exam Topic 3)



Refer to the exhibit. When an FTP client attempts to use passive FTP to connect to the FTP server, the file transfers fail Which action resolves the issue?

- A. Configure active FTP traffic.
- B. Modify FTP-SERVER access list to remove established at the end.
- C. Modify traffic filter FTP-SERVER in to the outbound direction.
- D. Configure to permit TCP ports higher than 1023.

**Answer: D**

#### NEW QUESTION 292

- (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
  
```

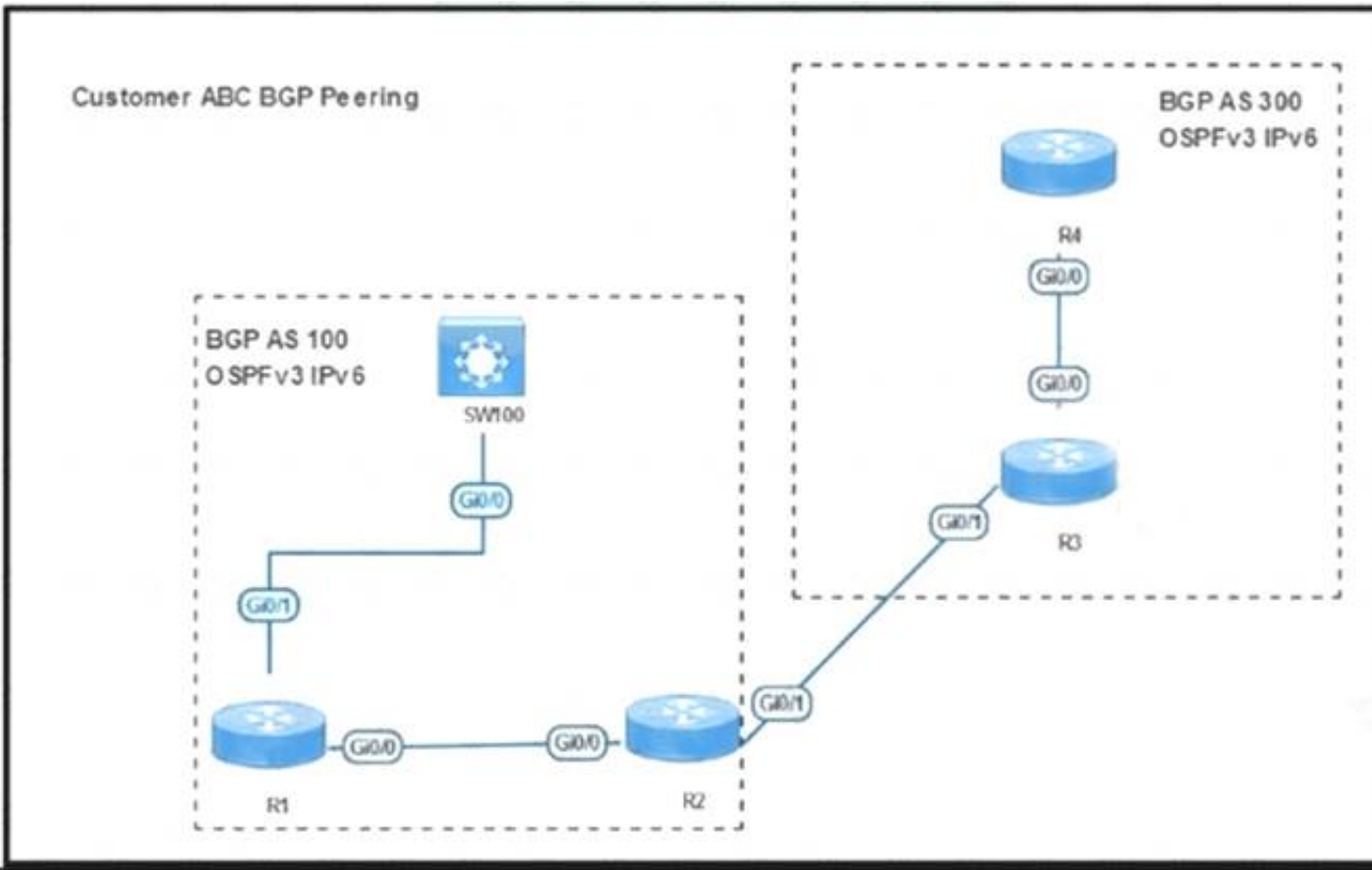
An administrator configured a Cisco router for TACACS authentication, but the router is using the local enable password instead Which action resolves the issue?

- 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 295**

- (Exam Topic 3)



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

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

SW100#sh ip bgp ipv6 unicast
SW100#

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

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



- ☐ R1  
router bgp 100  
address-family ipv6  
neighbor 2001::2 route-reflector-client  
neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client
- R2  
router bgp 100  
address-family ipv6  
neighbor 2001::2  
neighbor 2001::1 next-hop-self
- ☐ R1  
router bgp 100  
address-family ipv6  
neighbor 2001::2 route-reflector-client  
neighbor 2001:ABC:AABB:1100:1122:1111:2222:AAA2 route-reflector-client
- R2  
router bgp 100  
address-family ipv6  
neighbor 2001::2  
neighbor 2001::1 as-override
- ☐ R1  
router bgp 100  
address-family ipv6  
no synchronization
- R2  
router bgp 100  
address-family ipv6  
no synchronization  
SW100  
router bgp 100  
address-family ipv6  
no synchronization
- ☐ R1  
router bgp 100  
address-family ipv6  
redistribute connected
- R2  
router bgp 100  
address-family ipv6  
redistribute connected

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

Answer: A

#### NEW QUESTION 298

- (Exam Topic 3)

What is a function of IPv6 Source Guard?

- A. It works with address glean or ND to find existing addresses.  
B. It inspects ND and DHCP packets to build an address binding table.  
C. It denies traffic from known sources and allocated addresses.  
D. It notifies the ND protocol to inform hosts if the traffic is denied by it.

Answer: A

#### Explanation:

IPv6 source guard is an interface feature between the populated binding table and data traffic filtering. This feature enables the device to deny traffic when it is originated from an address that is not stored in the binding table. IPv6 source guard does not inspect ND or DHCP packets; rather, it works in conjunction with IPv6 neighbor discovery (ND) inspection or IPv6 address glean, both of which detect existing addresses on the link and store them into the binding table.

### NEW QUESTION 303

- (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 306

- (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:~$
```

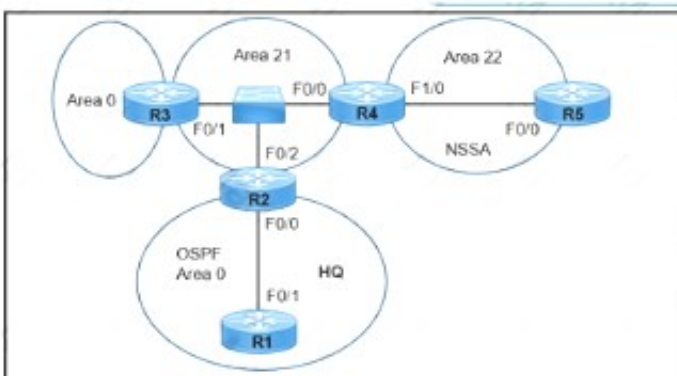
Refer to the exhibit. An administrator can log in to the device using Telnet but the attempts to log in to the same device using SSH with the same credentials fail. Which action resolves this issue?

- 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 310

- (Exam Topic 3)



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

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

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

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

**Answer: D**

### NEW QUESTION 311

- (Exam Topic 3)  
Refer to the exhibits.

**London – "show ip route" output**

Gateway of last resort is not set

```

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

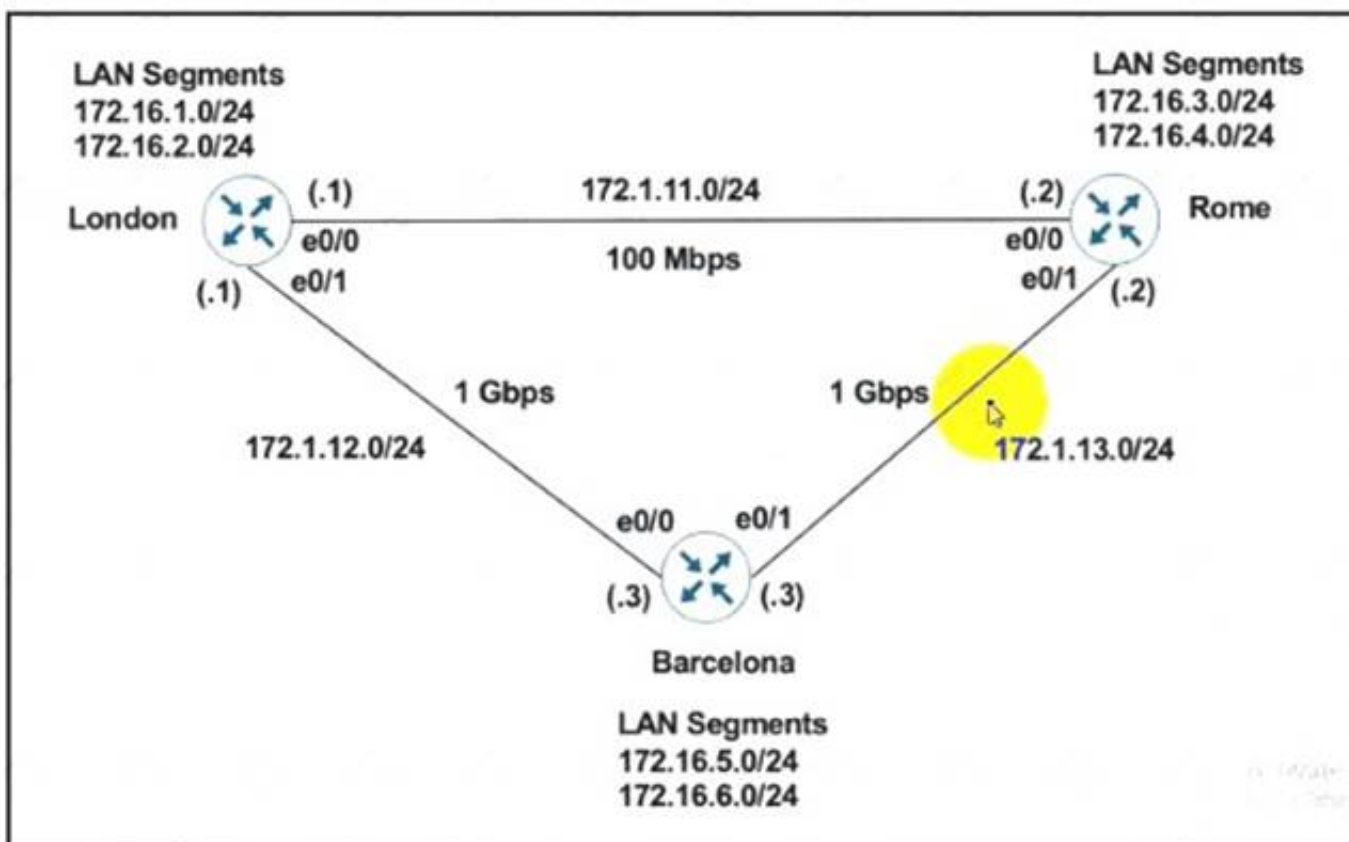
```

**Rome - "show run | section router" output**

```

router eigrp 111
 network 172.1.0.0
 network 172.16.0.0
 no auto-summary

```



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

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

**Answer: D**

**NEW QUESTION 312**

- (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 314**

- (Exam Topic 3)

Refer to the exhibit.



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

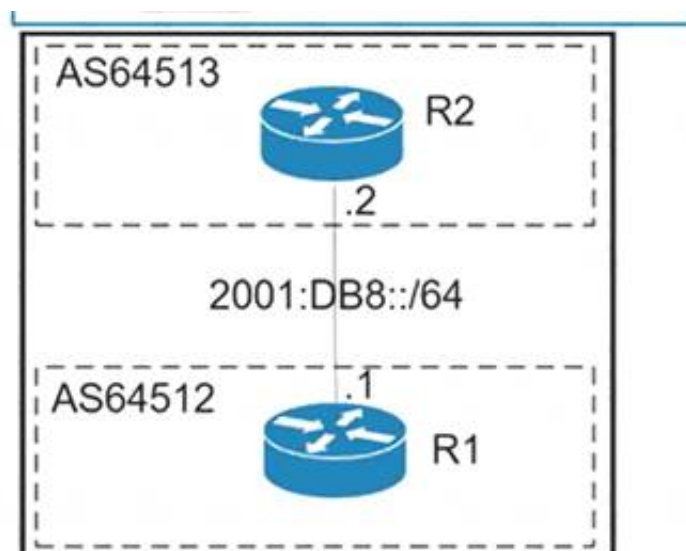
Which configuration enables OSPF for area 0 interfaces to adjacency with a neighboring router with the same VRF?

- A. router ospf 1 vrf CCNP interface Ethernet1 ip ospf 1 area 0.0.0.0 interface Ethernet2 ip ospf 1 area 0.0.0.0
- B. router ospf 1 interface Ethernet1 ip ospf 1 area 0.0.0.0 interface Ethernet2 ip ospf 1 area 0.0.0.0
- C. router ospf 1 vrf CCNP network 10.1.1.1 0.0.0.0 area 0 network 10.2.2.2 0.0.0.0 area 0
- D. router ospf 1 vrf CCNP network 10.0.0.0 0.0.255.255 area 0

**Answer: C**

#### NEW QUESTION 318

- (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 321

- (Exam Topic 3)

Refer to the exhibit.

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

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

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

**Answer: D**

#### NEW QUESTION 323

- (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 Tunnel 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 324

- (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 327

- (Exam Topic 3)

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

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

- ☒ interface Loopback0  
ip address 10.1.1.1 255.255.255.0  
vrf forwarding CCNP
- ☐ interface Loopback0  
ip address 10.1.1.1 255.255.255.0
- ☐ interface Loopback0  
vrf forwarding CCNP
- ☐ interface Loopback0  
ip address 10.1.1.1 255.255.255.0  
ip vrf forwarding CCNP

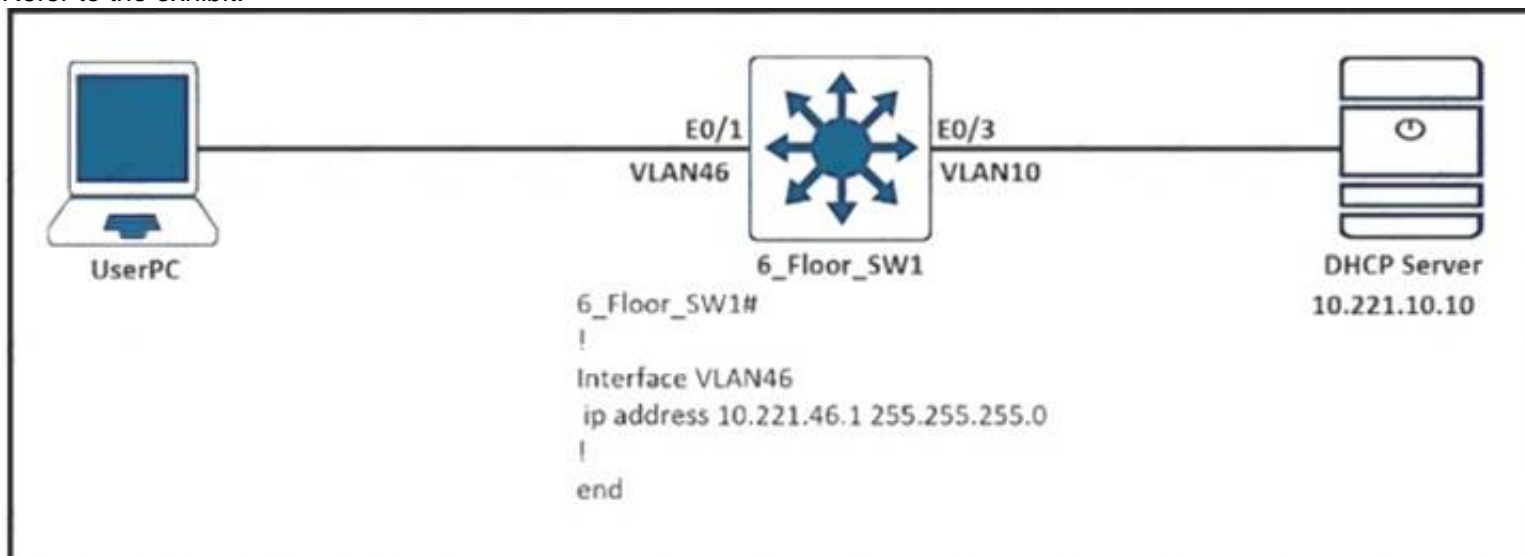
- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 329

- (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 interface 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 334

- (Exam Topic 3)

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

```
access-list 100 permit ospf any any
```

```
!
```

```
class-map CM-OSPF match access-group 100
```

```
!
```

```
policy-map PM-COPP class CM-OSPF
```

```
police 1000000 conform-action transmit
```

```
!
```

```
control-plane
```

```
service-policy output PM-COPP
```

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



```

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

```

☐ No access-list 100  
access-list 100 permit tcp any any eq 179  
access-list 100 permit tcp any any range eq 22  
access-list 100 permit tcp any any range eq 23  
access-list 100 permit ospf any any

☐ control-plane  
no service-policy output PM-COPP  
service-policy input PM-COPP

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

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

**Answer:** A

#### NEW QUESTION 339

- (Exam Topic 3)

Refer to the exhibit.

```

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

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

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

```

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

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

**Answer:** AD

#### Explanation:

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

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

```

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

```

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

#### NEW QUESTION 342

- (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 343

- (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
```

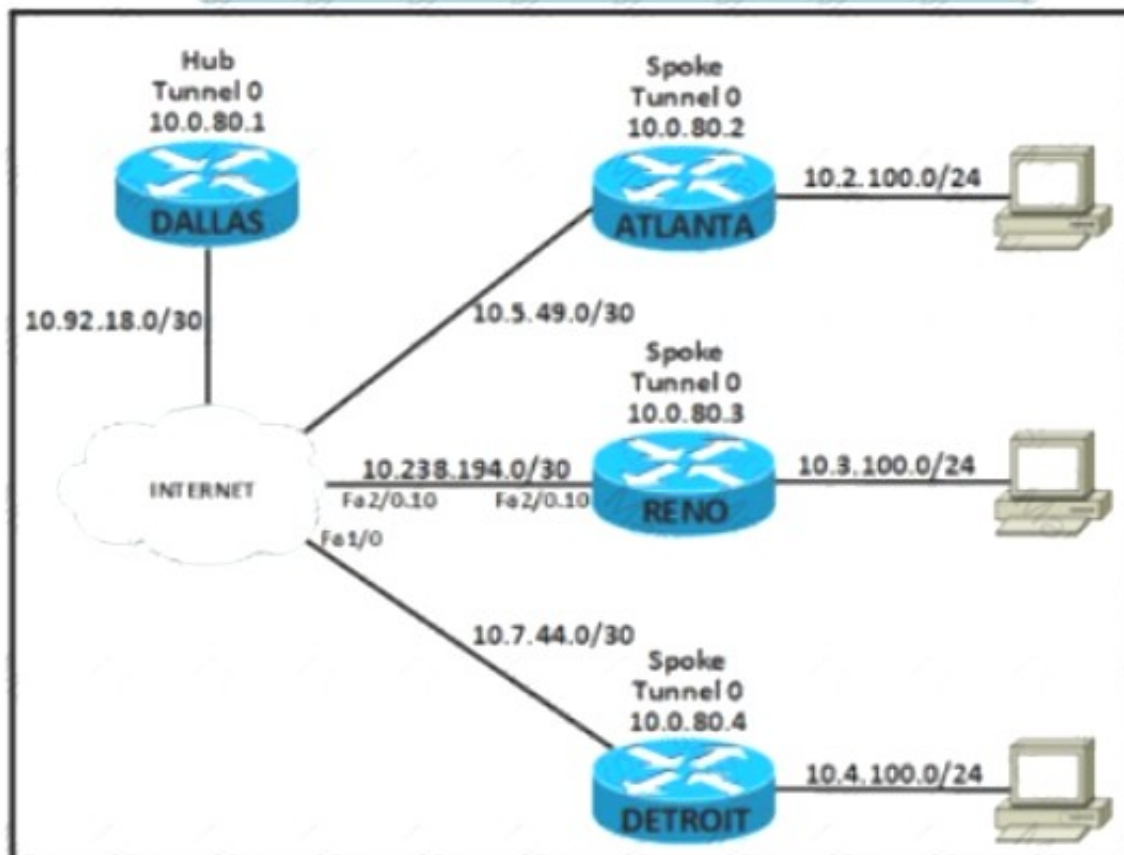
An engineer applies a prefix-list filter that filters most of the network 10 prefixes instead of allowing them. Which action resolves the issue?

- 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 348

- (Exam Topic 3)



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

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

Which configuration accomplishes the task?

☐ Reno

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

Detroit

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

☐ Reno

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

Detroit

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

☐ Reno

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

Detroit

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



```

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

```

```

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

```

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

**Answer: C**

#### NEW QUESTION 351

- (Exam Topic 3)

Refer to the exhibit.

```

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

Gateway of last resort is not set

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

```

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 355

- (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?

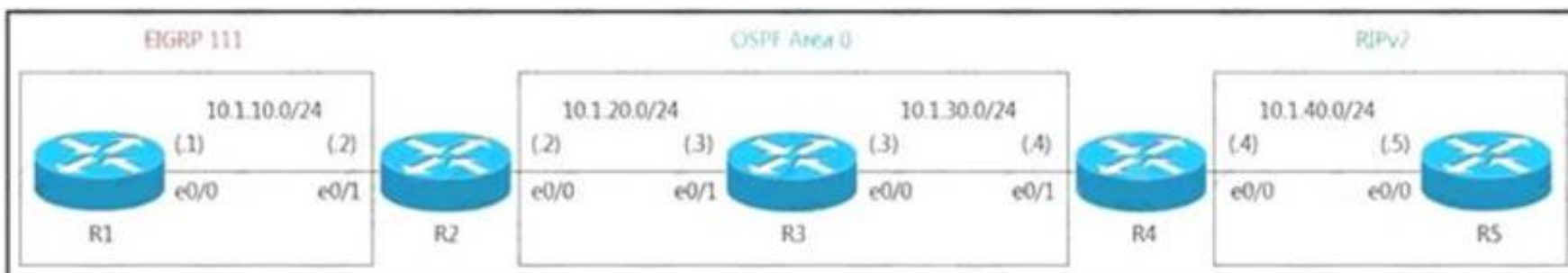
- A. Configure AS\_PATH prepend for the desired best path
- B. Configure higher MED to select as the best path.
- C. Configure lower LOCAL\_PREF to select as the best path.
- D. Configure AS\_PATH prepend for the current best path

**Answer: D**

#### NEW QUESTION 358

- (Exam Topic 3)

Refer to the exhibit.



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

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

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

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

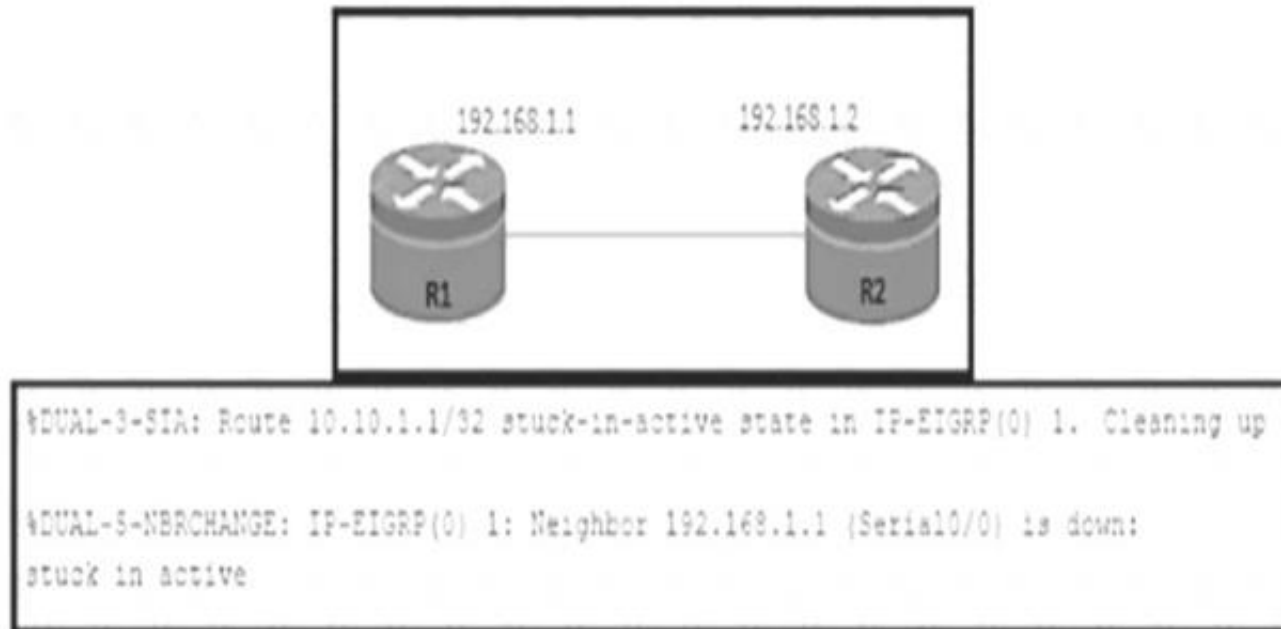
**Answer: A**

**Explanation:**

In this question, routes from EIGRP domain are redistributed into OSPF (with tag 111) then RIPv2 but without any filtering so R5 learns all routes from both EIGRP and OSPF domain. If we only want R5 to learn routes from OSPF domain then we must filter out routes with tag 111 and permit other routes. The line "route-map O2R permit 20" is important to allow other routes because of the implicit deny all at the end of each route-map.

**NEW QUESTION 360**

- (Exam Topic 3)



Refer to the exhibit. An engineer notices a connectivity problem between routers R1 and R2. The frequency of this problem is high during peak business hours. Which action resolves the issue?

- A. Increase the MTU on the interfaces that connect R1 and R2.
- B. Increase the available bandwidth between R1 and R2.
- C. Decrease the EIGRP keepalive and hold down timers on R1 and R2.
- D. Set static EIGRP neighborship between R1 and R2.

**Answer: B**

**NEW QUESTION 364**

- (Exam Topic 3)

Refer to the exhibit.

```
interface GigabitEthernet2
  no ip address
  ip helper-address 192.168.255.3
  no shutdown
!
interface GigabitEthernet2.10
  encapsulation dot1Q 210
  ip address 192.168.210.1 255.255.255.0
  ip ospf 1 area 0
  no shutdown
```

With the partial configuration of a router-on-a-stick. Clients in VLAN 10 on Gi2 cannot obtain IP configuration from the central DHCP server is reachable by a successful ping from the route. Which action resolves the issue?

- A. Configure the ip/ip/dhcp pool f and network 192.168..210.0.255.255/0 commands.
- B. Configure the ip header-address 192-168.265.3 command on the Gi2 10 subinterface.
- C. Configure a valid IP address on the Gi2 interface so that DHCP requests can be forwarded.
- D. Configure the Ip dhcp excluded-address 192.168.255.3 command on the Gi1.10 subinterface.

**Answer: B**

**NEW QUESTION 367**

- (Exam Topic 3)

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

```
access-list 100 permit tcp any any eq 179 access-list 100 permit tcp any any range 22 23 access-list 100 permit ospf any any
!
class-map CM-ROUTING match access-group 100
class-map CM-MGMT match access-group 100
!
```



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

control-plane

service-policy output PM-COPP

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

A. no access-list 100access-list 100 permit tcp any any eq 179 access-list 100 permit ospf any anyaccess-list 101 Permit tcp any any range 22 23!class-map CM-MGMTno match access-group 100 match access-group 101

B. control-planeno service-policy output PM-COPP service-policy input PM-COPP

C. No access-list 100access-list 100 permit tcp any any eq 179access-list 100 permit tcp any any range eq 22 access-list 100 permit tcp any any range eq 23 access-list 100 permit ospf any any

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

**Answer: D**

#### NEW QUESTION 370

- (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 373

- (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 377

- (Exam Topic 3)

```
R1# configure terminal
R1(config)# hostname CPE1
CPE1(config)# ip domain-name example.com
CPE1(config)# crypto key generate rsa
The name for the keys will be: CPE1.example.com
Choose the size of the key modulus in the range of 360 to 4096
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

CPE1(config)# service password-encryption
CPE1(config)# username csadmin secret Secur3p4s$w0rd
CPE1(config)# line vty 0 4
CPE1(config-line)# transport input telnet ssh
CPE1(config-line)# login local
CPE1(config-line)# end
CPE1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CPE1# ssh 10.0.0.1
% No user specified nor available for SSH client
```

Refer to the exhibit. An administrator must harden a router, but the administrator failed to test the SSH access successfully to the router. Which action resolves the issue?

A. Configure SSH on the remote device to log in using SSH

B. SSH syntax must be ssh -l user ip to log in to the remote device

C. Configure enable secret to log in to the device

D. SSH must be allowed with the transport output ssh command

**Answer: B**

**NEW QUESTION 380**

- (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 2 name ISP2
```

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

- A. Include a valid source-interface keyword in the icmp-echo statement.
- B. Reference the track object 1 on the default route through ISP2 instead of ISP1.
- C. Modify the static routes to refer both to the next hop and the outgoing interface.
- D. Modify the threshold to match the administrative distance of the ISP2 route.

**Answer:** A

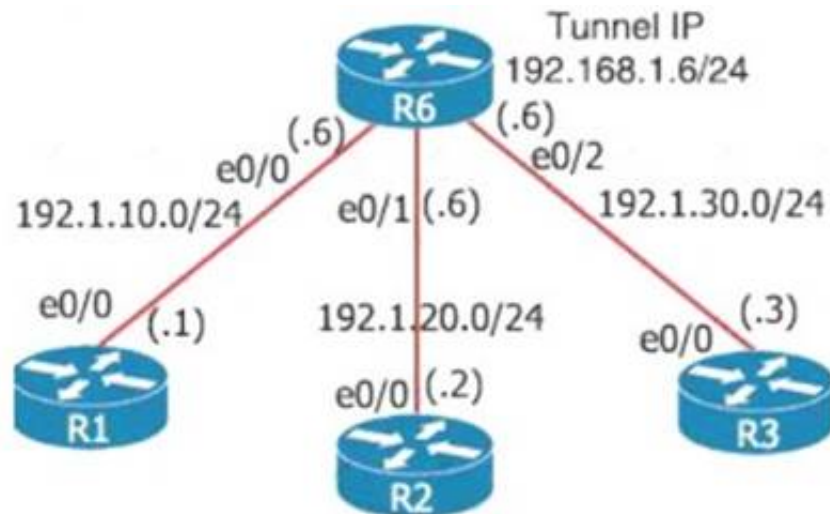
**Explanation:**

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

**NEW QUESTION 381**

- (Exam Topic 3)

Refer to the exhibit.



An engineer must establish multipoint GRE tunnels between hub router R6 and branch routers R1, R2, and R3. Which configuration accomplishes this task on R1?

A)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.6
```

B)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/1
 tunnel mode gre multipoint
 ip nhrp network-id 1
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```

C)

```
interface Tunnel 1
 ip address 192.168.1.1 255.255.255.0
 tunnel source e0/0
 tunnel mode gre multipoint
 ip nhrp nhs 192.168.1.6
 ip nhrp map 192.168.1.6 192.1.10.1
 ip nhrp map 192.168.1.2 192.1.20.2
 ip nhrp map 192.168.1.3 192.1.30.3
```

D)

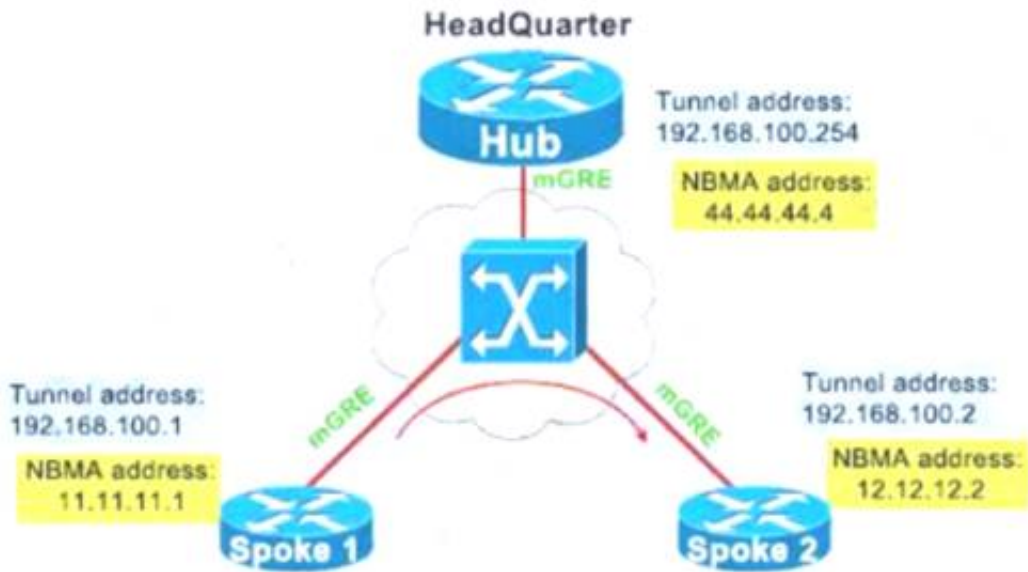
```
interface Tunnel 1
ip address 192.168.1.1 255.255.255.0
tunnel source e0/0
tunnel mode gre multipoint
ip nhrp network-id 1
ip nhrp nhs 192.168.1.6
ip nhrp map 192.168.1.6 192.1.10.6
```

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

Answer: D

Explanation:

We have an example of how to configure DMVPN Phase II and we show the configuration here for your reference:  
Diagram Description automatically generated



DMVPN Phase II – Dynamic Mapping  
Text Description automatically generated

| Hub                                                                                                                                            | Spoke 1                                                                                                                                                                                                               | Spoke 2                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface tunnel 1<br>ip address 192.168.100.254 255.255.255.0<br>tunnel source 44.44.44.4<br>tunnel mode gre multipoint<br>ip nhrp network 10 | interface tunnel 1<br>ip address 192.168.100.1 255.255.255.0<br>tunnel source 11.11.11.1<br>tunnel mode gre multipoint<br>ip nhrp network 10<br>ip nhrp map 192.168.100.254 44.44.44.4<br>ip nhrp nhs 192.168.100.254 | interface tunnel 1<br>ip address 192.168.100.2 255.255.255.0<br>tunnel source 12.12.12.2<br>tunnel mode gre multipoint<br>ip nhrp network 10<br>ip nhrp map 192.168.100.254 44.44.44.4<br>ip nhrp nhs 192.168.100.254 |

Note: Although Phase II – Dynamic Mapping is “dynamic” but we still need to add a static entry for the hub because without that entry, the NHRP registration cannot be sent.

NEW QUESTION 384

- (Exam Topic 3)  
Refer to the exhibit.



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

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

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

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

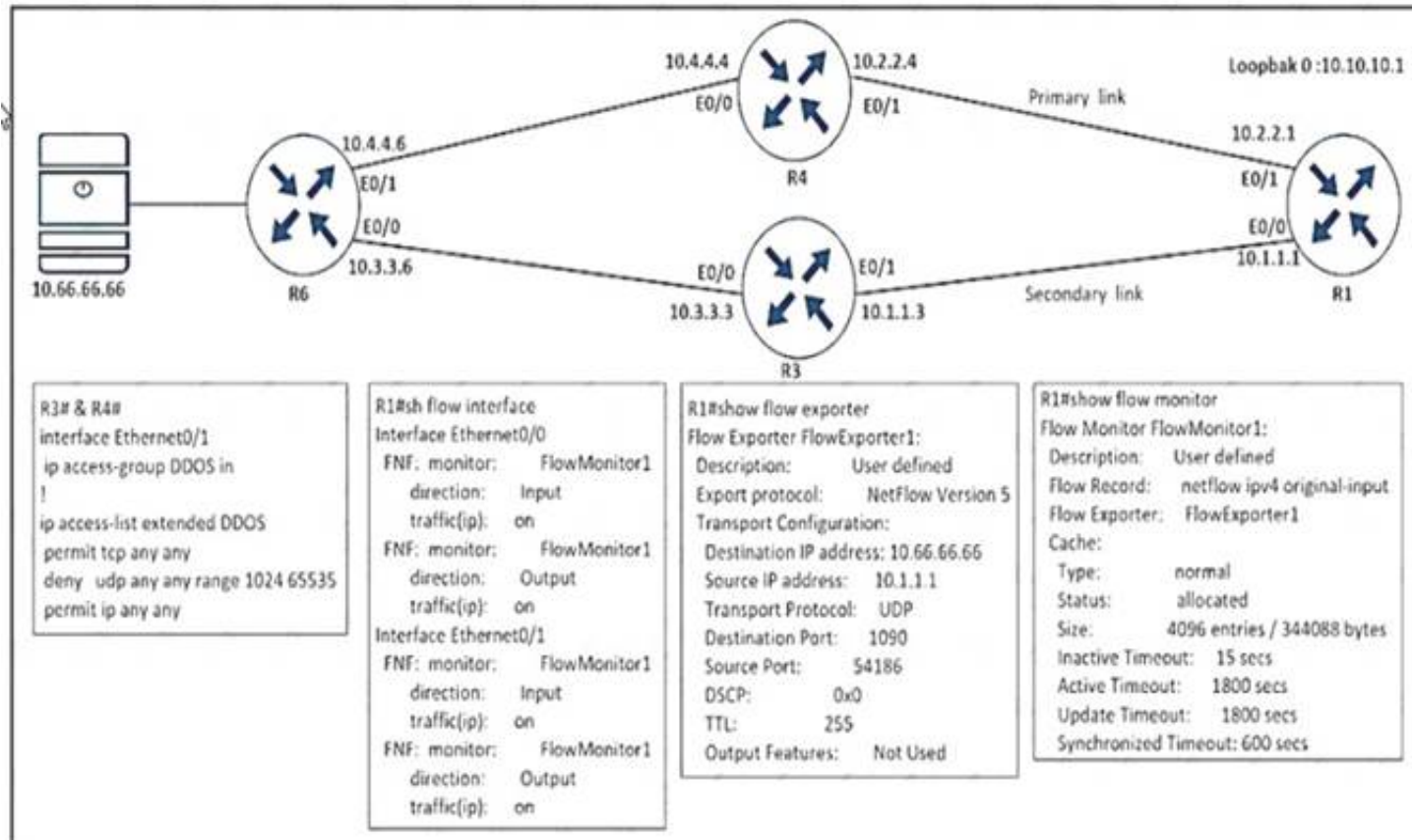
**Answer: D**

**Explanation:**

From the output, we learn that the current best path is from 10.57.255.11 (which includes "...valid, confed-external, best") and this path is 2 ASes away (64955 65003). Although there are some paths with only 1 AS away (path from 172.16.254.234 for example) but they were not chosen the best path so AS\_PATH was not used to determine the best path -> Answers A and answer C are not correct. All the paths in the output have metric of 0 and this is the lowest (best) value for this attribute. If we configure higher MED then it is less preferred over other paths -> Answer B is not correct. Only answer D is left but LOCAL\_PREF attribute should be configured with higher value to be preferred so we hope "lower LOCAL\_PREF" here means higher value. But this is the best answer.

#### NEW QUESTION 387

- (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 388

- (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.

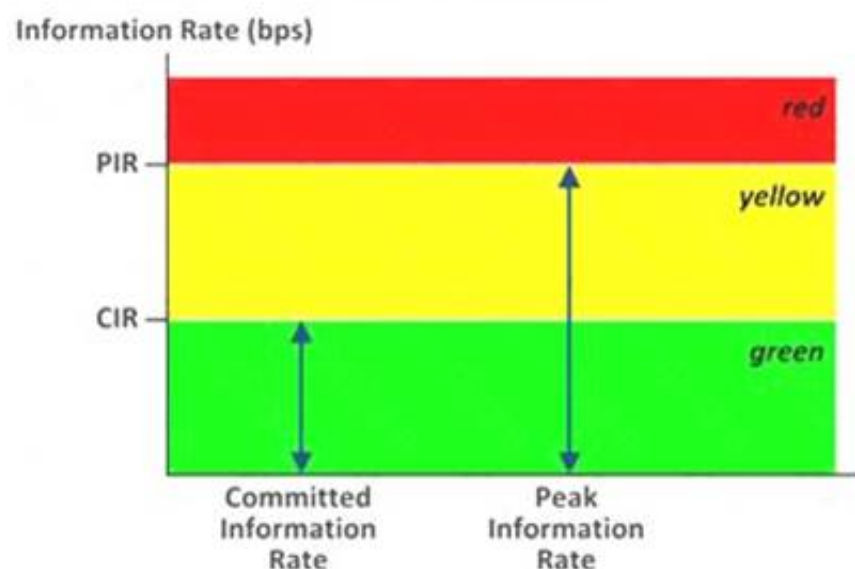
**Answer: D**

#### Explanation:

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

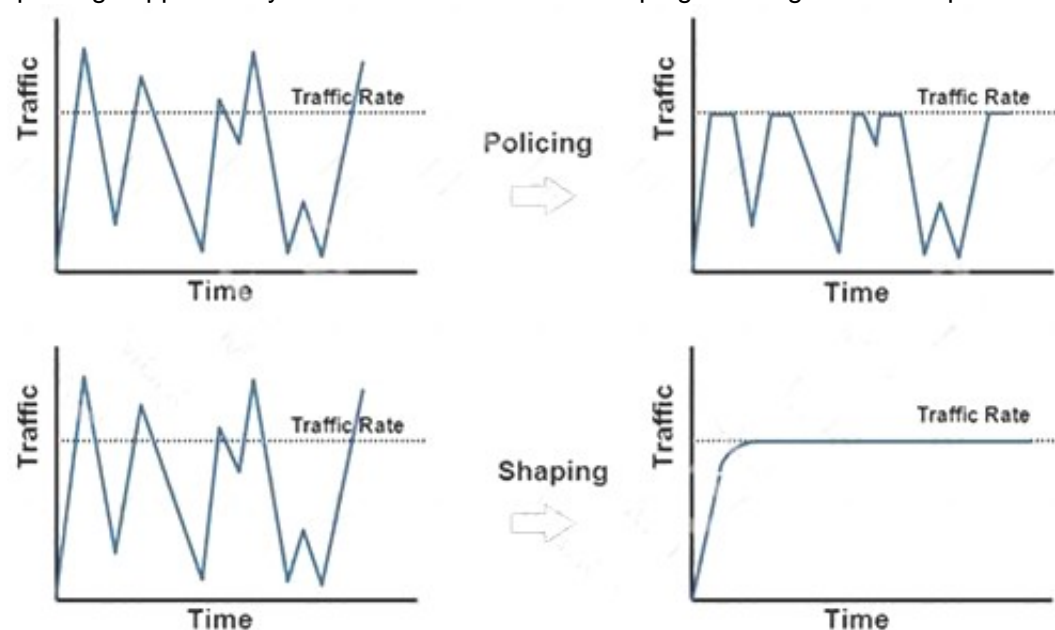
PIR (Peak Information Rate) is the top bandwidth point of allowed traffic in a non busy times without any guarantee.

## 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 392

- (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 396

- (Exam Topic 3)

What is an MPLS LDP targeted session?

- A. session between neighbors that are connected no more than one hop away
- B. LDP session established between LSRs by exchanging TCP hello packets
- C. label distribution session between non-directly connected neighbors
- D. LDP session established by exchanging multicast hello packets

**Answer: C**

### NEW QUESTION 401

- (Exam Topic 3)

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



Comment

Guidelines
Topology
Tasks

R1
R2
SW1
SW2
SW3
SW4

Topology Diagram

```

R1>
R1>
R1>
R1>
R1>
R1>

```

Guidelines
Topology
Tasks

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

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

```

R1>
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
!
!
!
!
!
ip vrf cu-green
  rd 65000:200
!
ip vrf cu-red
  rd 65000:100
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```

```

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

```

```

R1  R2  SW1  SW2  SW3  SW4
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

```

R1  R2  SW1  SW2  SW3  SW4
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

```



A screenshot of a network simulator interface showing the configuration of router R2. The top bar has tabs for R1, R2 (selected), SW1, SW2, SW3, and SW4. On the left, there are several exclamation marks (!) representing other devices. In the center, there is a blue circular icon with a white 'g' symbol. The main area shows the command-line interface for R2 with the following commands entered:

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

```
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 terminal window titled "SW1". The command prompt is "`>`". The user has entered the following commands:

```
spanning-tree mode pvst  
spanning-tree extend system-id
```

The second command, "spanning-tree extend system-id", is highlighted with a blue circle. Below it are several blank lines, followed by the configuration for interface Ethernet0/0:

```
interface Ethernet0/0  
no switchport  
ip address 192.168.2.1 255.255.255.0
```

Below this are the configurations for interfaces Ethernet0/1, Ethernet0/2, and Ethernet0/3, each starting with "interface" followed by the interface name.



```

R1  R2  SW1  SW2  SW3  SW4
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

```

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

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

```

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

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

SW3

```

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

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

```

```
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
```



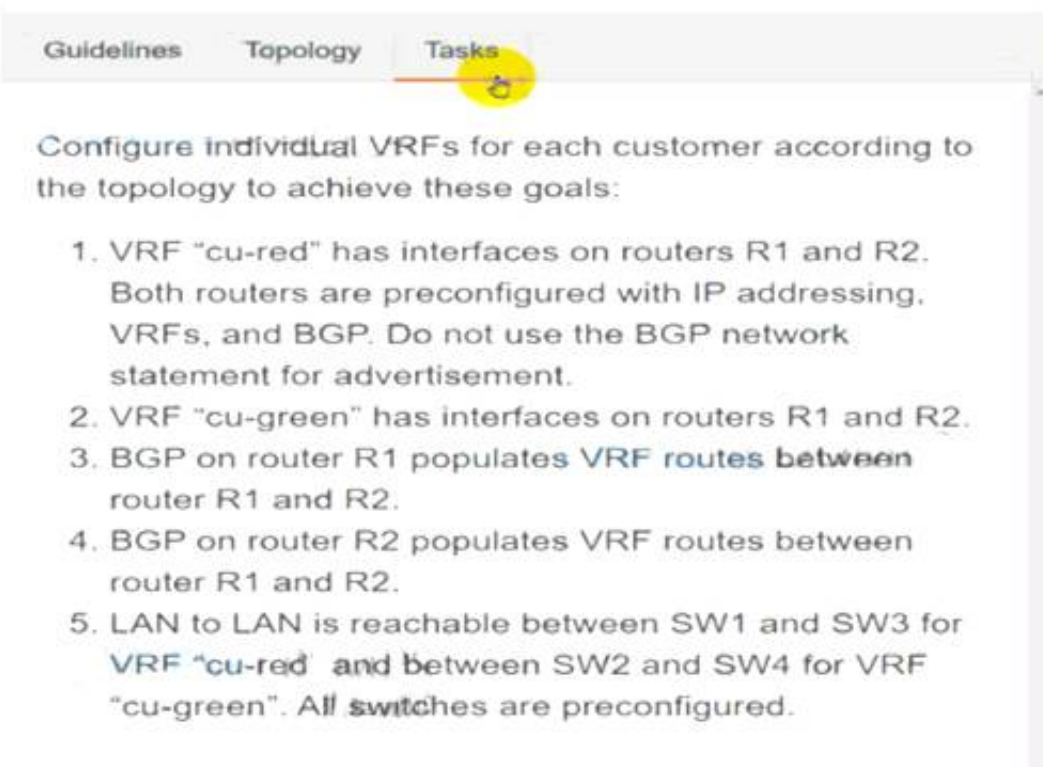
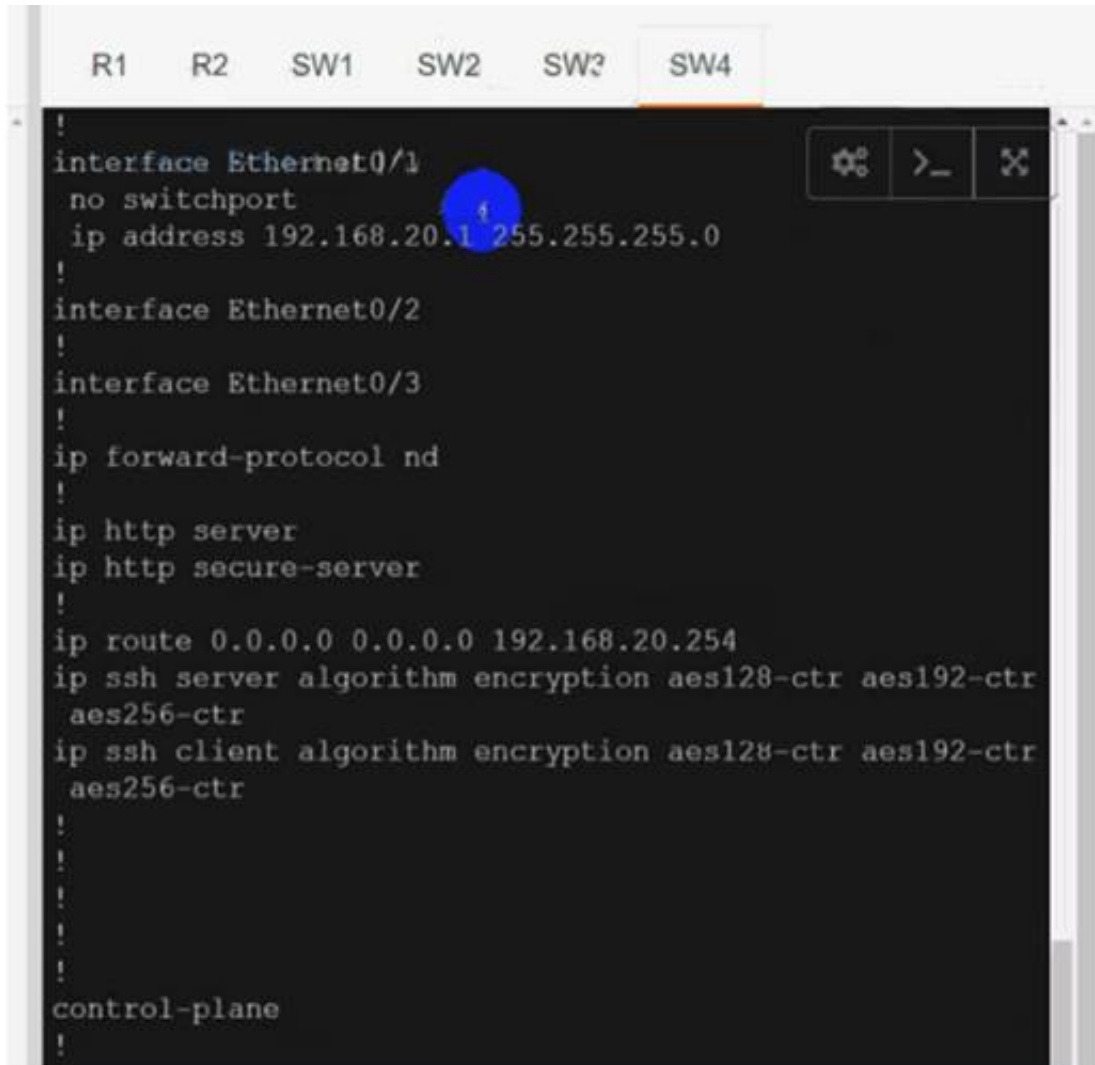
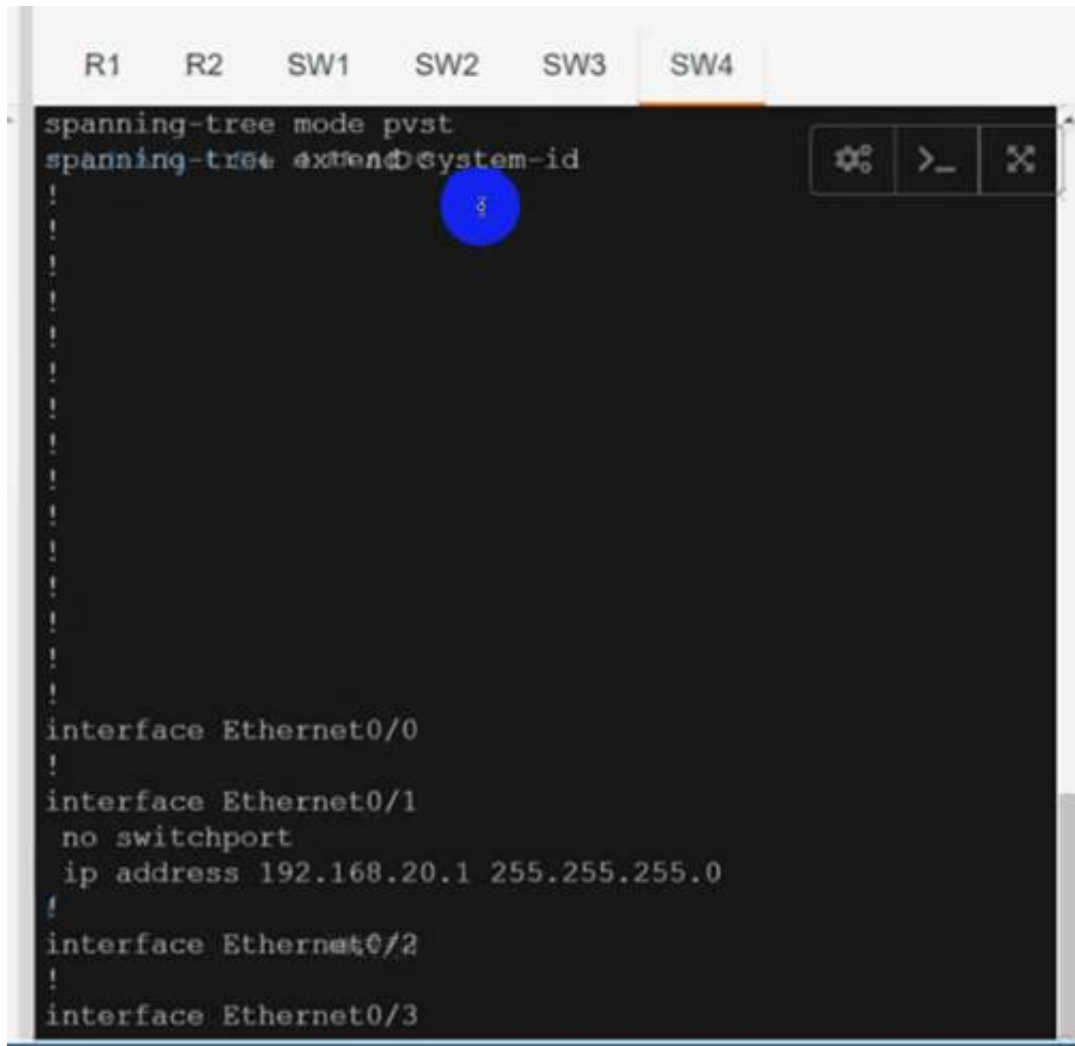
```

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
!
```



- 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 405**

- (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 408**

- (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 412

- (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 413

- (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?

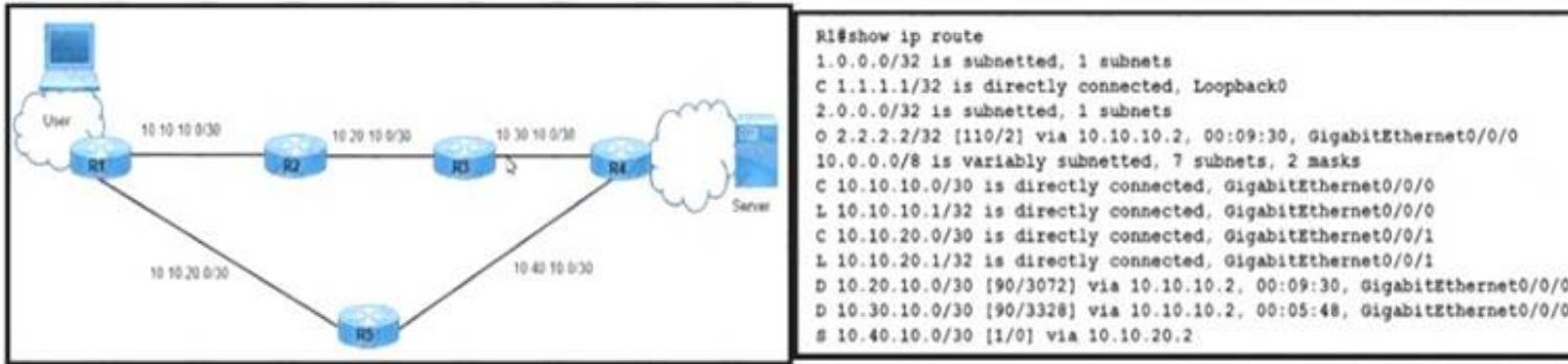
- A. Configure route summarization on OSPF-enabled interfaces.
- B. Summarize by using the summary-address 10.1.0.0 255.255.252.0 command.
- C. Summarize by using the area range command on ABRs
- D. Configure the summary-address 10.1.0.0 255.255.252.0 command under OSPF process.

Answer: C

**NEW QUESTION 415**

- (Exam Topic 3)

Refer to the exhibit.



Routers R1, R2, R3, and R4 use EIGRP However, traffic always prefers R1 to R5 backup links in nonfailure scenarios. Which configuration resolves the issue?

A)

```
R1(config)#no ip route 10.40.10.0 255.255.255.252 10.10.20.2
R1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

B)

```
R1(config)#int gigabitEthernet 0/0/0
R1(config-if)#bandwidth 10000000
```

C)

```
R1(config)#no ip route 10.40.10.0 255.255.255.252 10.10.20.2
R1(config)#ip route 10.40.10.0 255.255.255.252 10.10.20.2 115
```

D)

```
R1(config)#int gigabitEthernet 0/0/0
R1(config-if)#bandwidth 10000
```

A. Option A

B. Option B

C. Option C

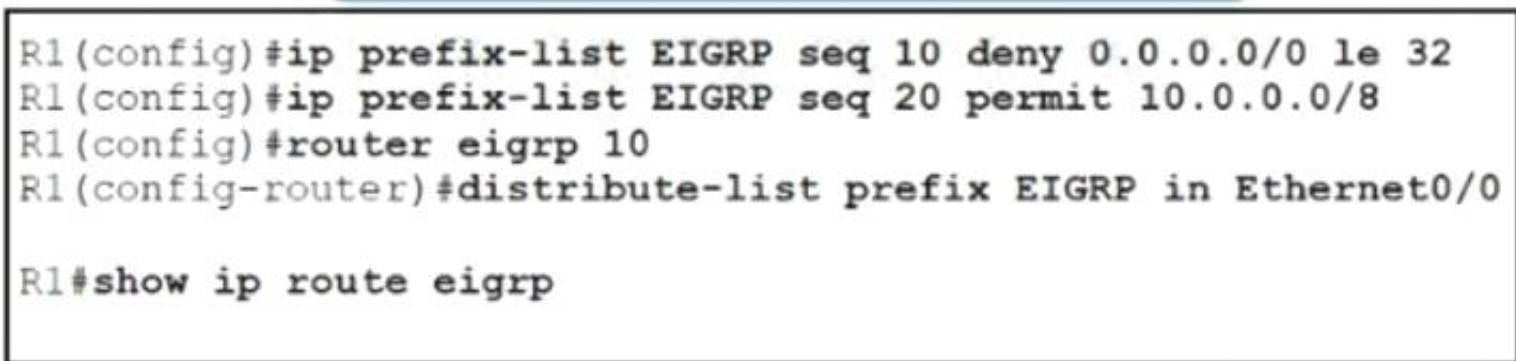
D. Option D

**Answer: A**

**NEW QUESTION 417**

- (Exam Topic 3)

Refer to the exhibit.



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

A. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9.

B. ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32

C. ip prefix-list EIGRP seq 5 permit 10.0.0.0/8 ge 9 no ip prefix-list EIGRP seq 20 permit 10.0.0.0/8

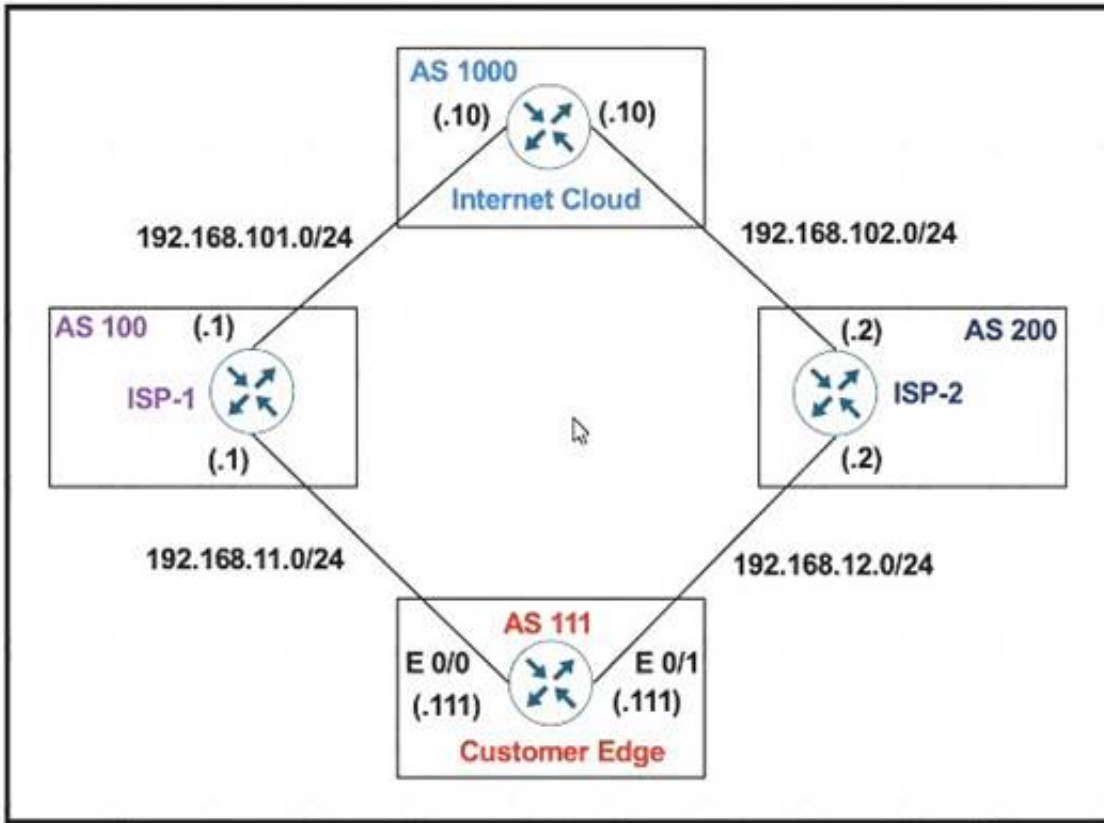
D. ip prefix-list EIGRP seq 20 permit 10.0.0.0/8 ge 9 ip prefix-list EIGRP seq 10 permit 0.0.0.0/0 le 32

**Answer: C**

**NEW QUESTION 420**

- (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?

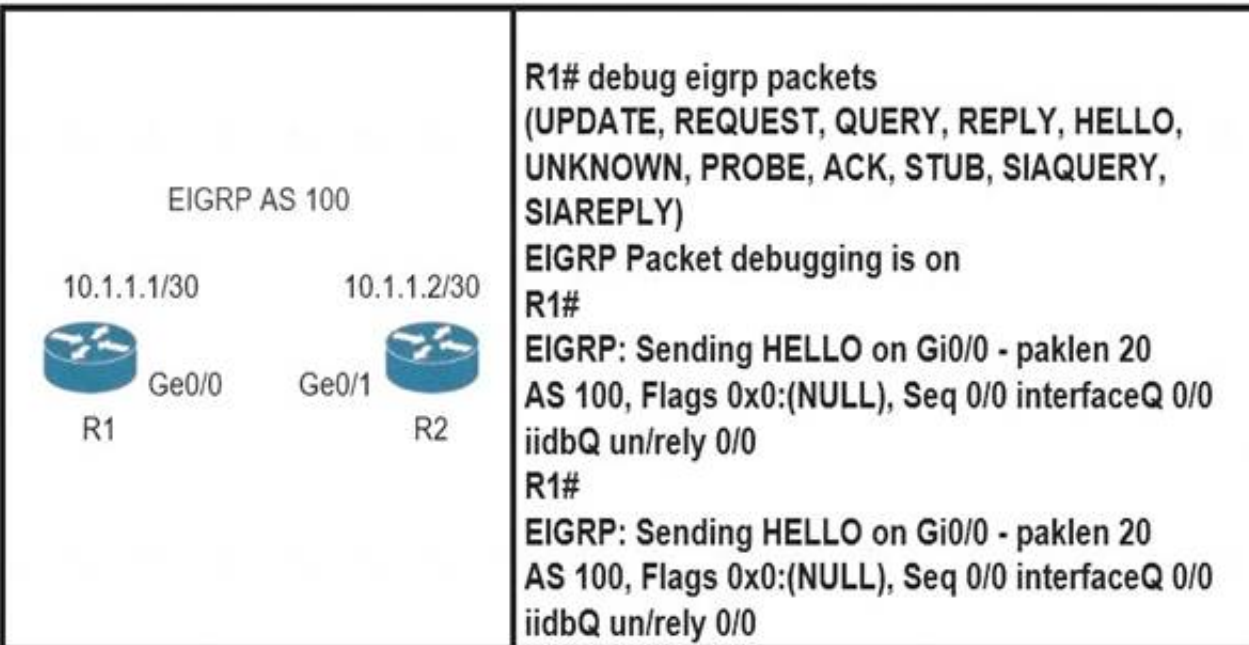
- A. ip as-path access-list 1 permit ^\$
- B. ip as-path access-list 1 permit \_111\_
- C. ip as-path access-list 1 permit "
- D. ip as-path access-list 1 permit ^111\$

**Answer: A**

#### NEW QUESTION 425

- (Exam Topic 2)

Refer to the exhibit.



Which action resolves the adjacency issue?

- A. Match the hello interval timers.
- B. Configure the same EIGRP process IDs.
- C. Match the authentication keys.
- D. Configure the same autonomous system numbers.

**Answer: D**

#### Explanation:

EIGRP does not have process ID as it uses Autonomous System (AS) numbers only. This is not an authentication problem or we would see this error from the debug:

EIGRP: Ethernet0/0: ignored packet from 10.1.1.3, opcode = 1 (missing authentication or key-chain missing) If the AS numbers between two routers are different then the neighbor relationship cannot be formed.

#### NEW QUESTION 430

- (Exam Topic 2)

Filtered

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up  
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up  
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up

Desired

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up  
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up  
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up  
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down  
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down  
2 \*Mar 1 18:46:11: %SYS-5-CONFIG\_I: Configured from console by vty2

Refer to the exhibits. An engineer filtered messages based on severity to minimize log messages. After applying the filter, the engineer noticed that it filtered required messages as well. Which action must the engineer take to resolve the issue?

- A. Configure syslog level 2.
- B. Configure syslog level 3.
- C. Configure syslog level 4.
- D. Configure syslog level 5.

Answer: D

NEW QUESTION 434

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 435

- (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 437

- (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 439**

- (Exam Topic 2)

Refer to the exhibit.

```
router# show running-config
Building configuration
!
<output omitted ----->
!
hostname R1
!
ip domain-name cisco.com
!
crypto key generate rsa modulus 2048
!
username admin privilege 15 secret cisco123
!
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 deny any log
!
line vty 0 15
access-class 1 in
login local
!
<output omitted ----->
!
end
```

A user cannot SSH to the router. What action must be taken to resolve this issue?

- A. Configure transport input ssh
- B. Configure transport output ssh
- C. Configure ip ssh version 2
- D. Configure ip ssh source-interface loopback0

**Answer:** A

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0\\_2\\_EX/security/configuration\\_](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_)

**NEW QUESTION 444**

- (Exam Topic 2)

Refer to the exhibit.



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

Service-policy output: CoPP

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

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

R1 is being monitored using SNMP and monitoring devices are getting only partial information. What action should be taken to resolve this issue?

- A. Modify the CoPP policy to increase the configured exceeded limit for SNMP.
- B. Modify the access list to include snmptrap.
- C. Modify the CoPP policy to increase the configured CIR limit for SNMP.
- D. Modify the access list to add a second line to allow udp any any eq snmp

**Answer:** D

#### NEW QUESTION 448

- (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

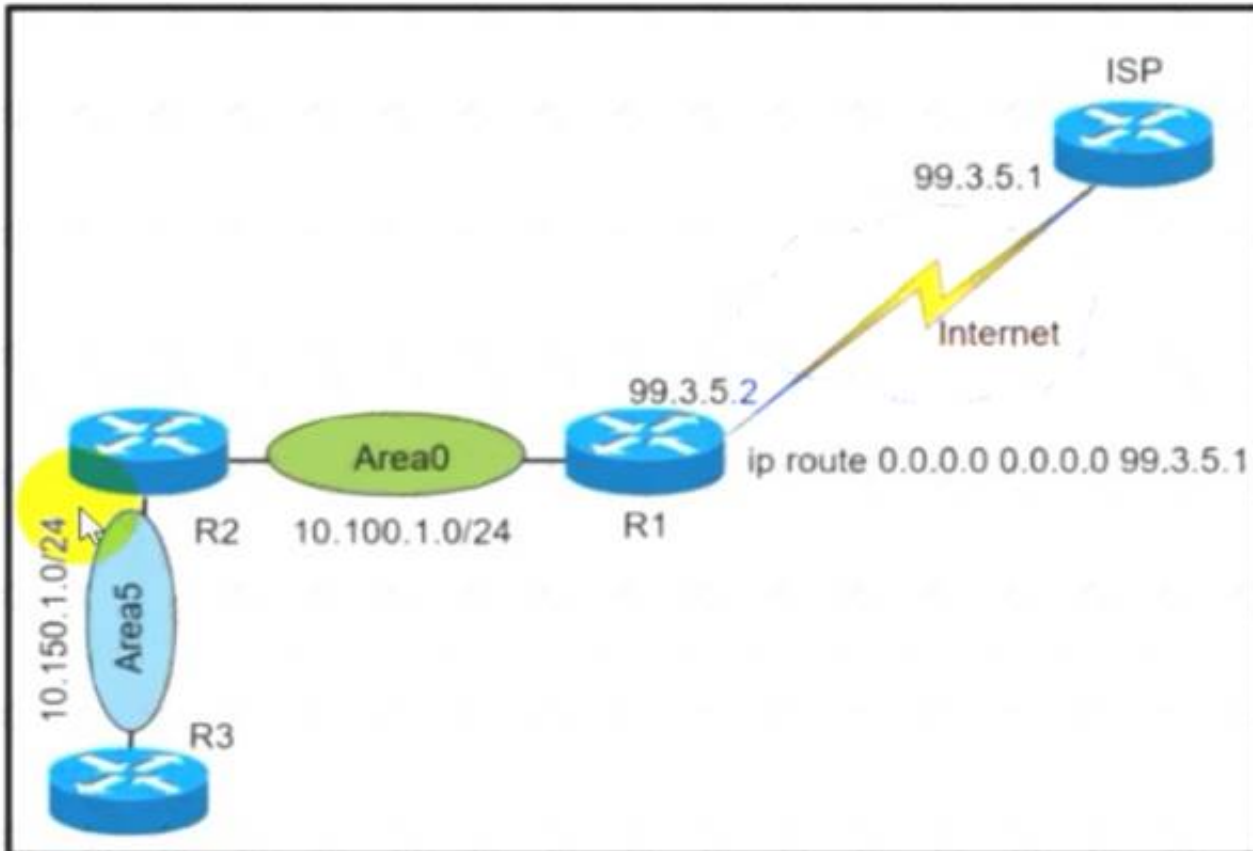
The MPLS LDP Inbound Label Binding Filtering feature can be used to control the amount of memory used to store Label Distribution Protocol (LDP) label bindings advertised by other devices. For example, in a simple Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment, the VPN 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 453

- (Exam Topic 2)



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

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

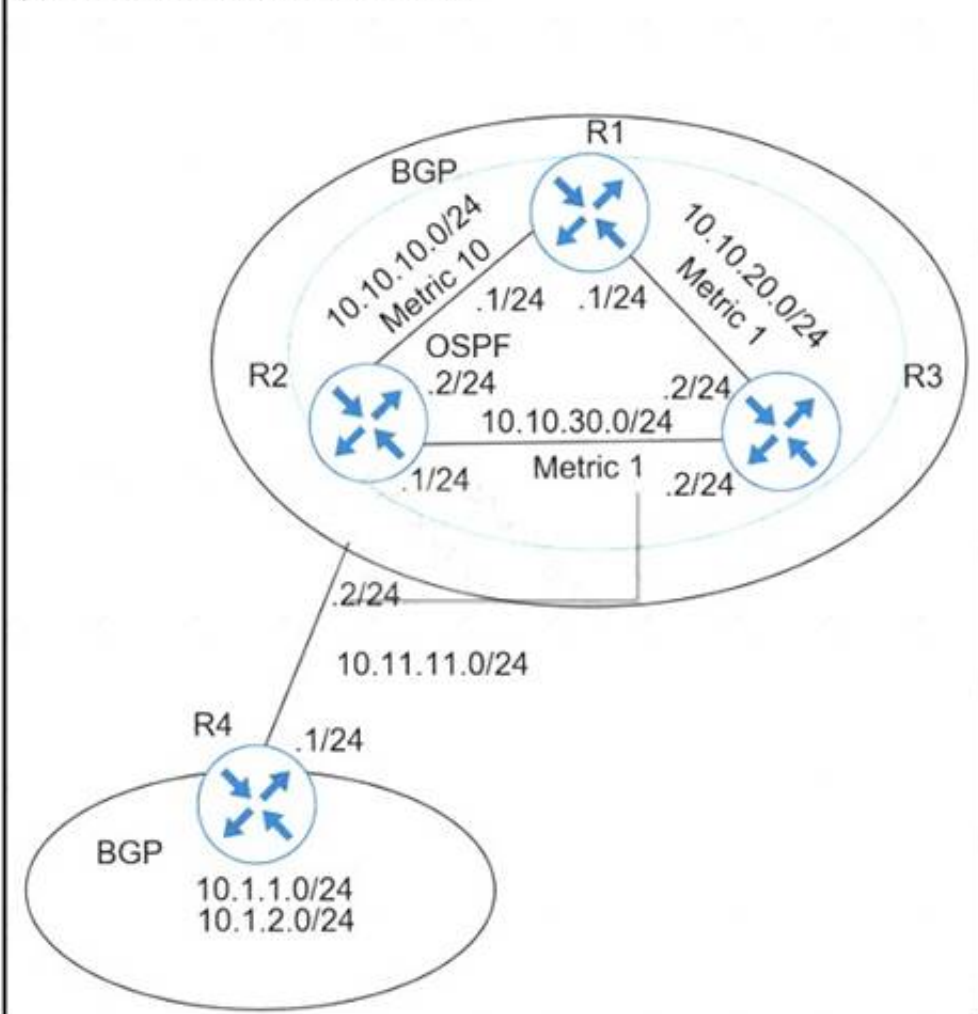
**Answer: A**

#### NEW QUESTION 454

- (Exam Topic 2)

Refer to the exhibit.

```
ip sla 10
tcp connect 10.1.1.1 80
ip sla schedule 10 life 30 start time now
```



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 455

- (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 456

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### 300-410 Practice Exam Features:

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

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