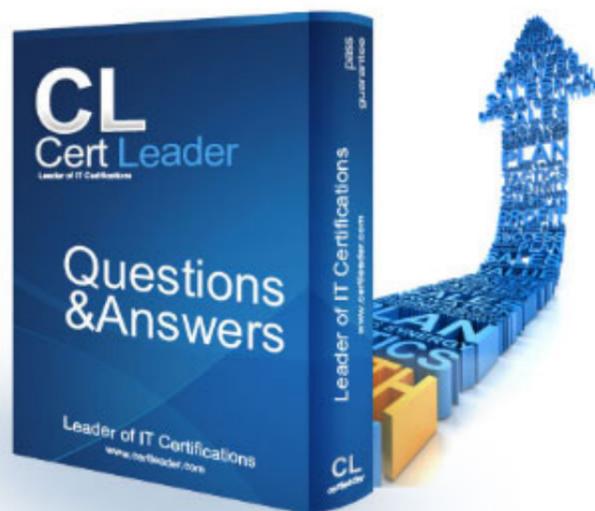


300-410 Dumps

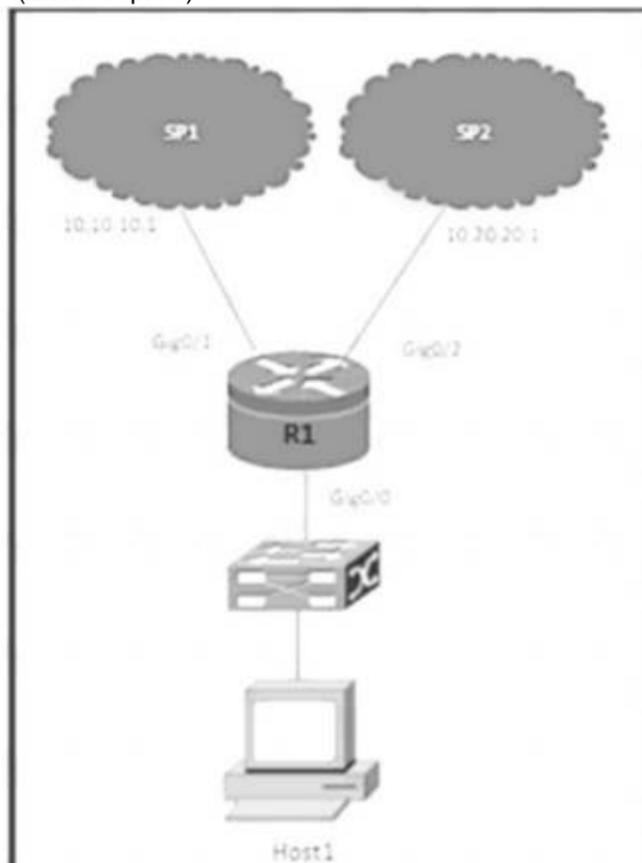
Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)

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



NEW QUESTION 1

- (Exam Topic 3)



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

A)

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 2

- (Exam Topic 3)

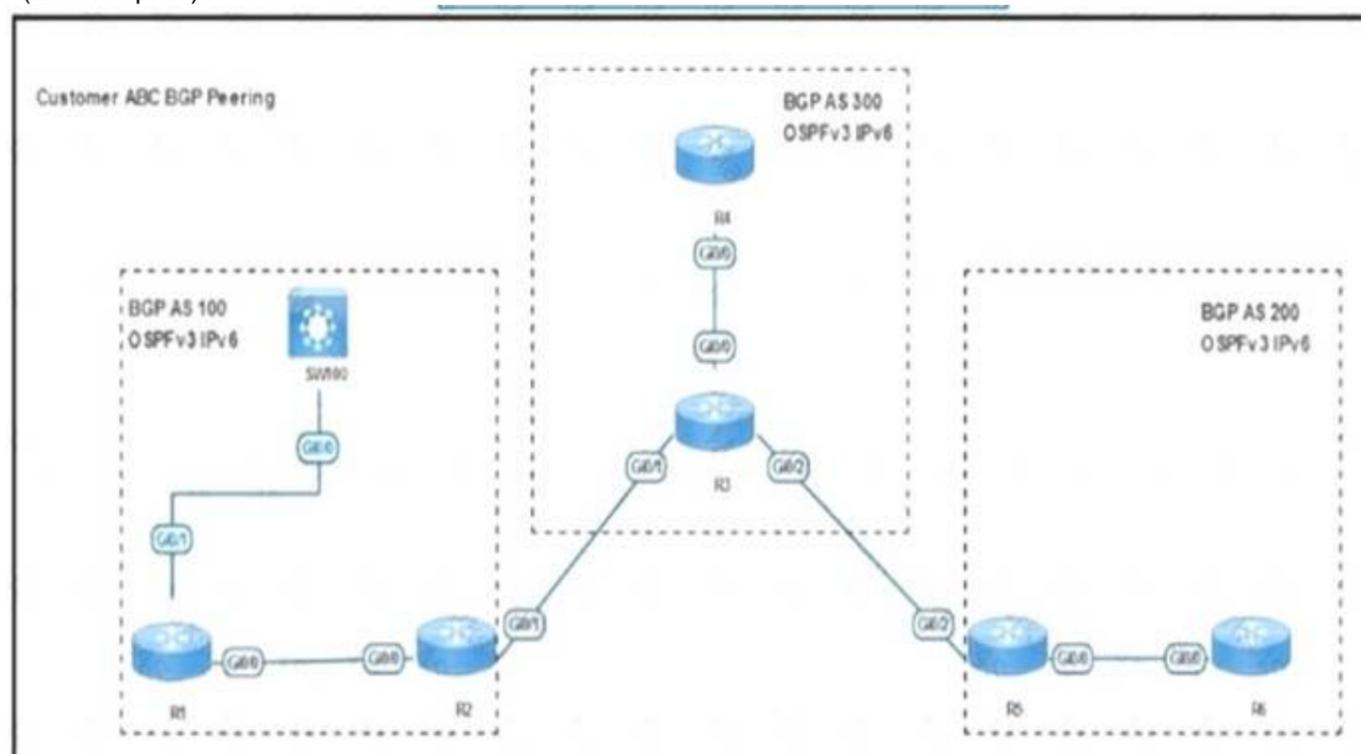
What is a characteristic of IPv6 RA Guard?

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

Answer: C

NEW QUESTION 3

- (Exam Topic 3)



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

```

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

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

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

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

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

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

- A. Replace as-path access-list 1 with the ip as-path access-list 1 permit A300\$ command
- B. Replace as-path access-list 1 with the ip as-path access-list 1 permit ..300." command
- C. Replace as-path access-list 1 with the ip as-path access-list 1 permit A300_ command.
- D. Replace as-path access-list 1 with the ip as-path access-list 1 permit A300." command

Answer: B

NEW QUESTION 4

- (Exam Topic 3)

Which router translates the customer routing information into VPNv4 routes to exchange VPNv4 routes with other devices through MP-BGP?

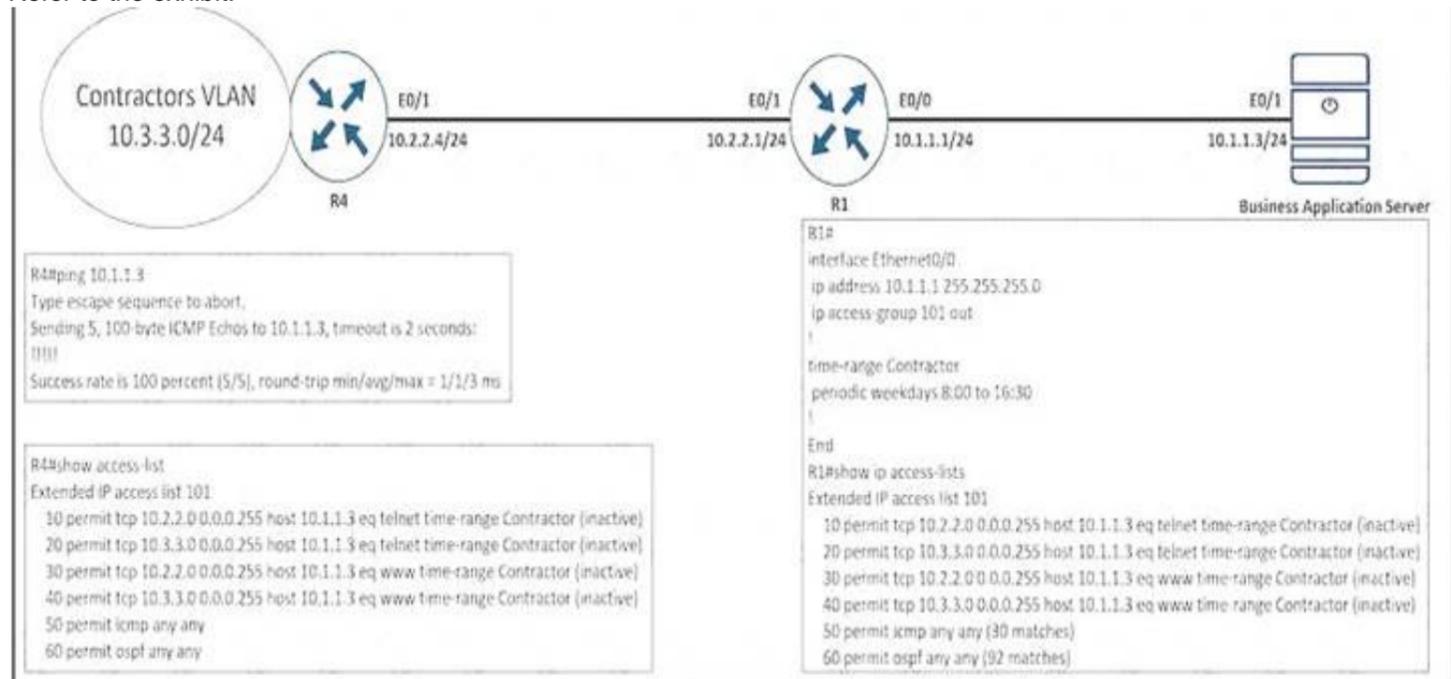
- A. PE
- B. CE
- C. P
- D. VPNv4 RR

Answer: A

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 3)

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

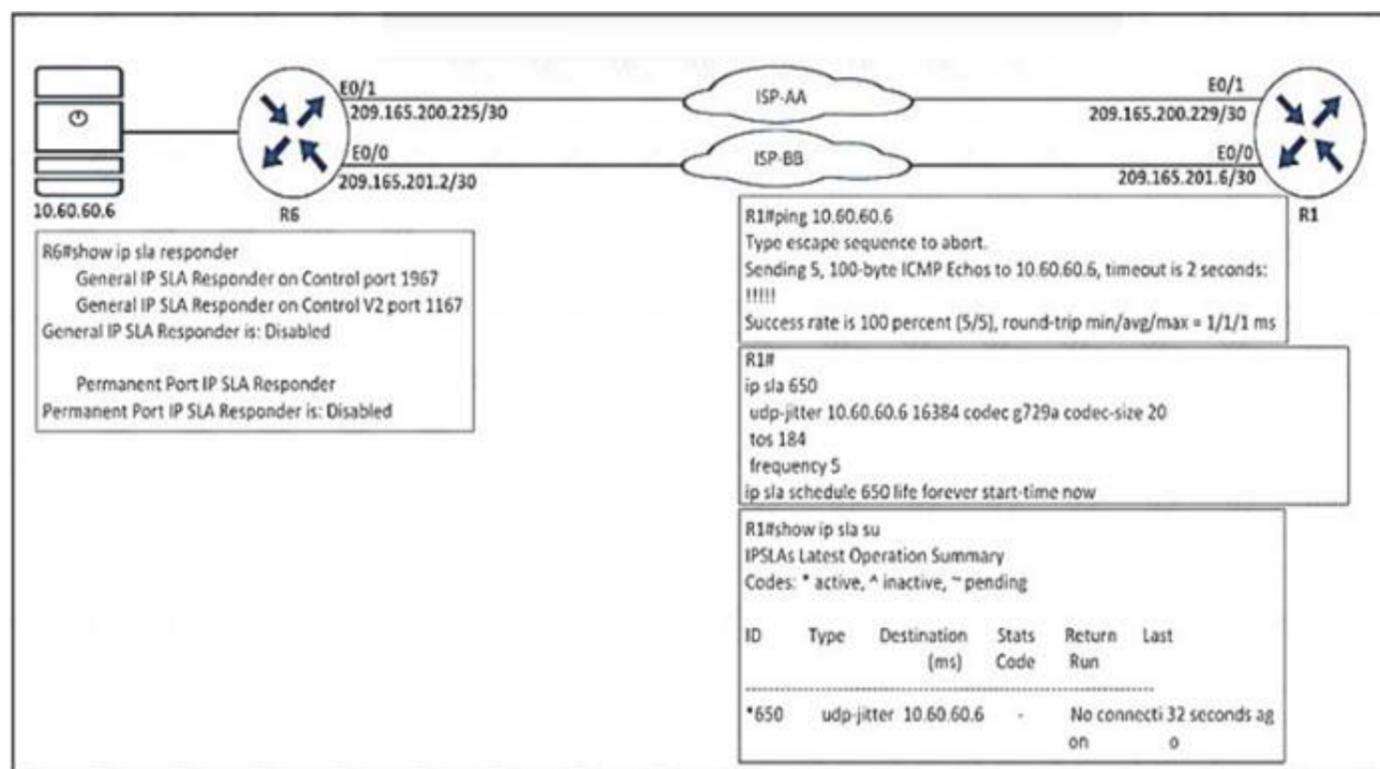
Refer to the exhibit. An engineer noticed that the router log messages do not have any information about when the event occurred. Which action should the engineer take when enabling service time stamps to improve the logging functionality at a granular level?

- A. Configure the debug uptime option
- B. Configure the msec option
- C. Configure the timezone option
- D. Configure the tog uptime option

Answer: D

NEW QUESTION 8

- (Exam Topic 3)



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

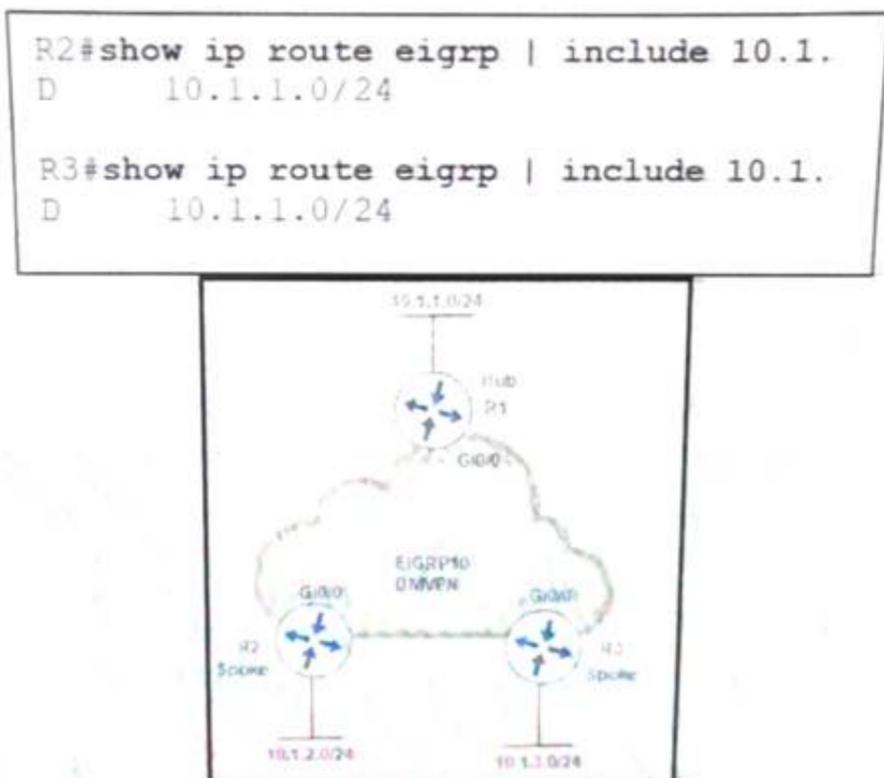
- A. R6(config)#ip sla responder
- B. R6(config)#ip sla responder udp-echo ipaddress 10.60.60.6 po 5000
- C. R6(config)#ip sla 650 R6(config-ip-sla)ff udp-jitter 10.60.60.6
- D. R6(config)#ip sla schedule 10 life forever start-time now

Answer: A

NEW QUESTION 9

- (Exam Topic 3)

Refer to the exhibit.



An engineer configures DMVPN and receives the hub location prefix of 10.1.1.0/24 on R2 and R3. The R3 prefix of 10.1.3.0/24 is not received on R2, and the R2 prefix 10.1.2.0/24 is not received on R3. Which action resolves the issue?

- A. Split horizon prevents the routes from being advertised between spoke routers; it should be disabled with the command `no ip split-horizon eigrp 10` on the tunnel interface of R1.
- B. There is no spoke-to-spoke connection; DMVPN configuration should be modified to enable a tunnel connection between R2 and R3 and neighbor relationship confirmed by use of the `show ip eigrp neighbor` command.
- C. Split horizon prevents the routes from being advertised between spoke routers; it should be disabled with the `no ip split-horizon eigrp 10` command on the Gi0/0 interface of R1.
- D. There is no spoke-to-spoke connection; DMVPN configuration should be modified with a manual neighbor relationship configured between R2 and R3 and confirmed by use of the `show ip eigrp neighbor` command.

Answer: A

Explanation:

In this topology, the Hub router will receive advertisements from R2 Spoke router on its tunnel interface. The problem here is that it also has a connection with R3 Spoke on that same tunnel interface. If we don't disable split-horizon, then the Hub will not relay routes from R2 to R3 and the other way around. That is because it received those routes on the same interface tunnel and therefore it cannot advertise back out that same interface (split-horizon rule). Therefore we must disable split-horizon on the Hub router to make sure the Spokes know about each other.

NEW QUESTION 10

- (Exam Topic 3)

Refer to the exhibit.

```
R1# show ip ospf database self-originate
OSPF Router with ID (10.255.255.1) (Process ID 1)
Router Link States (Area 0)
Link ID      ADV Router   Age         Seq#         Checksum
Link count
10.255.255.1 10.255.255.1 4           0x800003BD  0x001AD9
3
Summary Net Link States (Area 0)
Link ID      ADV Router   Age         Seq#         Checksum
10.0.34.0    10.255.255.1 3604       0x80000380  0x00275C
10.255.255.4 10.255.255.1 3604       0x80000380  0x00762B
Type-5 AS External Link States
Link ID      ADV Router   Age         Seq#         Checksum
Tag
0.0.0.0      10.255.255.1 3604       0x800001D0  0x001CBC
0
*Feb 22 22:50:39.523: %OSPF-4-FLOOD_WAR: Process 1 flushes LSA
ID 0.0.0.0 type-5 adv-rtr 10.255.255.1 in area 0
```

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 12

- (Exam Topic 3)

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

Answer: B

NEW QUESTION 17

- (Exam Topic 3)

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

```

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

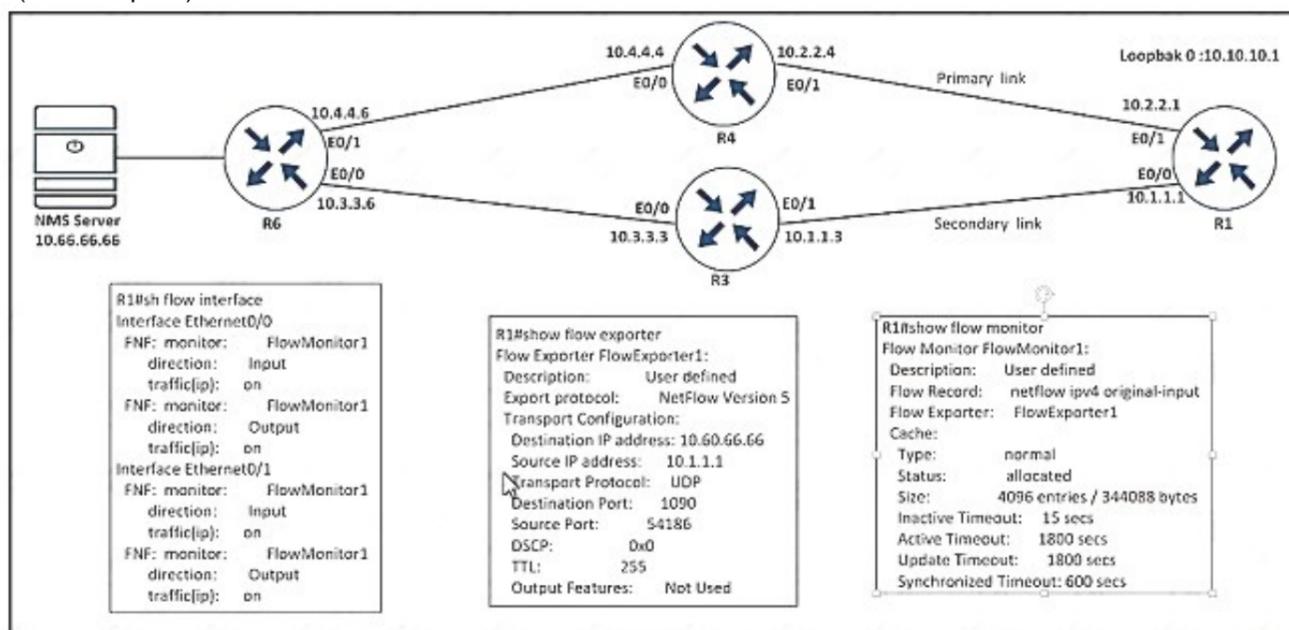
```

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

Answer: B

NEW QUESTION 18

- (Exam Topic 3)



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

- R1(config)#flow monitor FlowMonitor1
R1(config-flow-monitor)#destination 10.66.66.66
- R1(config)#flow exporter FlowExporter1
R1(config-flow-exporter)#destination 10.66.66.66
- R1(config)#interface Ethernet0/0
R1(config-if)#ip flow monitor Flowmonitor1 input
R1(config-if)#ip flow monitor Flowmonitor1 output
- R1(config)#interface Ethernet0/1
R1(config-if)#ip flow monitor Flowmonitor1 input
R1(config-if)#ip flow monitor Flowmonitor1 output

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

Answer: B

NEW QUESTION 22

- (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 25

- (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 29

- (Exam Topic 3)

Refer to the exhibit.

```

RB#
*Sep 19 00:53:43.002: BGPNSF state: 10.10.10.3 went from nsf_not_active to
nsf_not_active
*Sep 19 00:53:43.006: BGP: 10.10.10.3 went from Established to Idle
*Sep 19 00:53:43.006: BGP: 10.10.10.3 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 writes 00:01:35, hold time is 180, keepalive
interval is 60 seconds
  Default minimum time between advertisement runs is 30 seconds
  Address tracking is enabled, the RIB does have a route to 10.10.10.2
  Connections established 11; dropped 11
  Last reset 00:01:36, due to Peer closed the session
  External BGP neighbor may be up to 3 hops away.
  Transport(tcp) path-mtu-discovery is enabled
  No active TCP connection
    
```

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

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

Answer: B

NEW QUESTION 31

- (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?

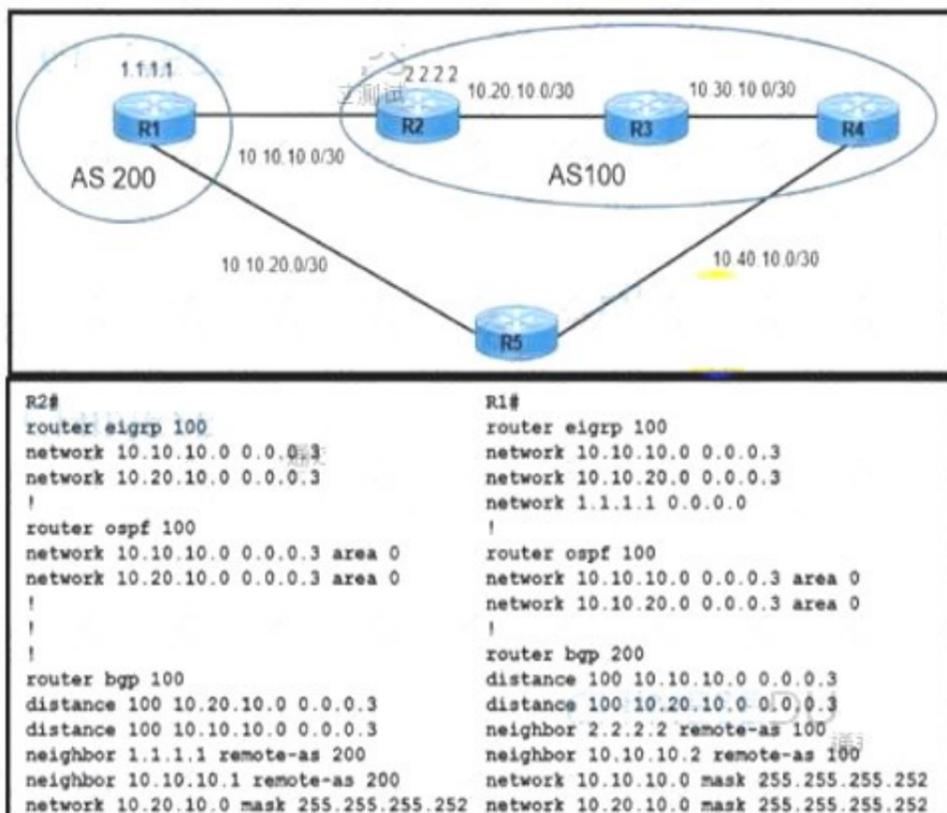
- A. Configure the snmp ifindex persist command globally.
- B. Clear the logical interfaces with snmp ifindex clear command
- C. Configure the snmp ifindex persist command on the physical interfaces.
- D. Trigger a new snmpwalk from the monitoring system to synchronize interface OIDs

Answer: A

NEW QUESTION 36

- (Exam Topic 3)

Refer to the Exhibit.



R1 and R2 use IGP protocol to route traffic between AS 100 and AS 200 despite being configured to use BGP. Which action resolves the issue and ensures the use of BGP?

- A. Configure distance to 100 under the EIGRP process of R1 and R2.
- B. Remove distance commands under BGP AS 100 and AS 200.
- C. Remove distance commands under BGP AS 100.
- D. Configure distance to 100 under the OSPF process of R1 and R2

Answer: B

NEW QUESTION 38

- (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 39

- (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

NEW QUESTION 44

- (Exam Topic 3)

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

- A. Rate-limit SSH traffic to ensure dedicated bandwidth.
- B. Apply CoPP on the control plane interface.
- C. Increase the IP precedence value of SSH traffic to 6.
- D. Apply CoPP on the WAN interface inbound direction.

Answer: B

Explanation:

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

NEW QUESTION 48

- (Exam Topic 3)

```

R6#
*Sep  5 05:31:58.891: BGP: 10.0.0.17 went from Idle to Active
*Sep  5 05:31:58.895: BGP: 10.0.0.17 open active, local address 10.0.0.18
*Sep  5 05:31:58.907: BGP: 10.0.0.17 read request no-op
*Sep  5 05:31:58.911: BGP: 10.0.0.17 went from Active to OpenSent
*Sep  5 05:31:58.911: BGP: 10.0.0.17 sending OPEN, version 4, my as: 65201, holdtime
180 seconds
*Sep  5 05:31:58.911: BGP: 10.0.0.17 send message type 1, length (incl. header) 53
*Sep  5 05:31:58.927: BGP: 10.0.0.17 remote closs
*Sep  5 05:31:58.931: BGP: 10.0.0.17 -reset the session
*Sep  5 05:31:58.931: BGPNSF state: 10.0.0.17 went from nsf_not_active to
nsf_not_active

R5#
*Sep  5 05:34:22.063: BGP: 10.0.0.18 passive open to 10.0.0.17
*Sep  5 05:34:22.063: BGP: 10.0.0.18 passive open failed - 10.0.0.17 is not update-
source Loopback0's address (10.10.10.5)
*Sep  5 05:34:22.063: BGP: 10.0.0.18 remote connection attempt failed, local address
10.0.0.17
    
```

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
            
```

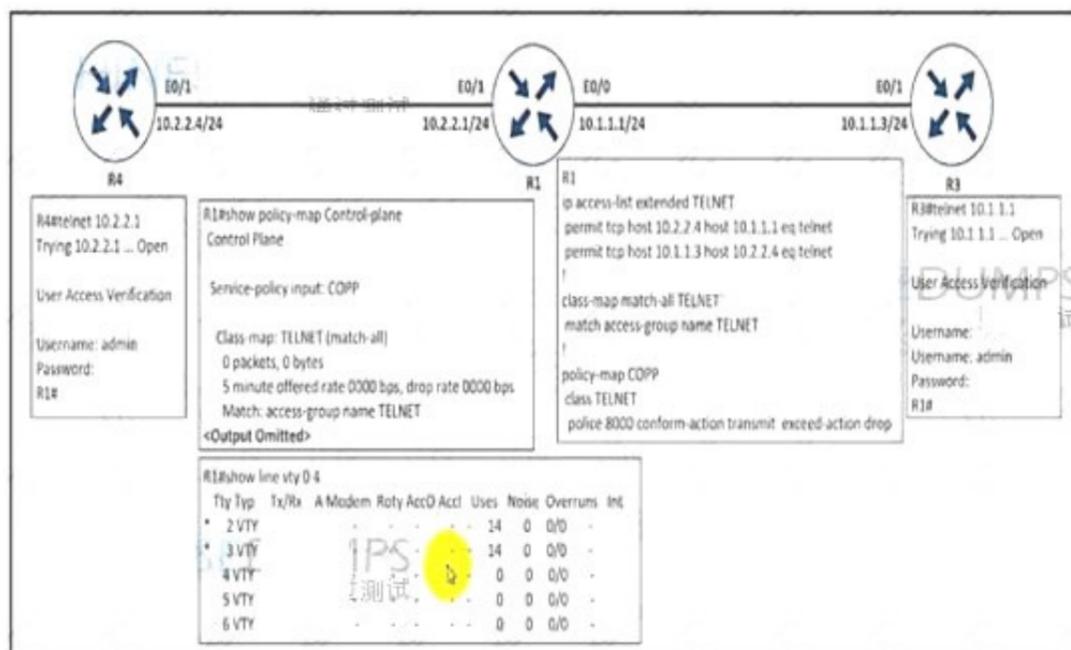
- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 50

- (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 55

- (Exam Topic 3)

What must a network architect consider for RTs when planning for a single customer full-mesh VPN in an MPLS Layer 3 network?

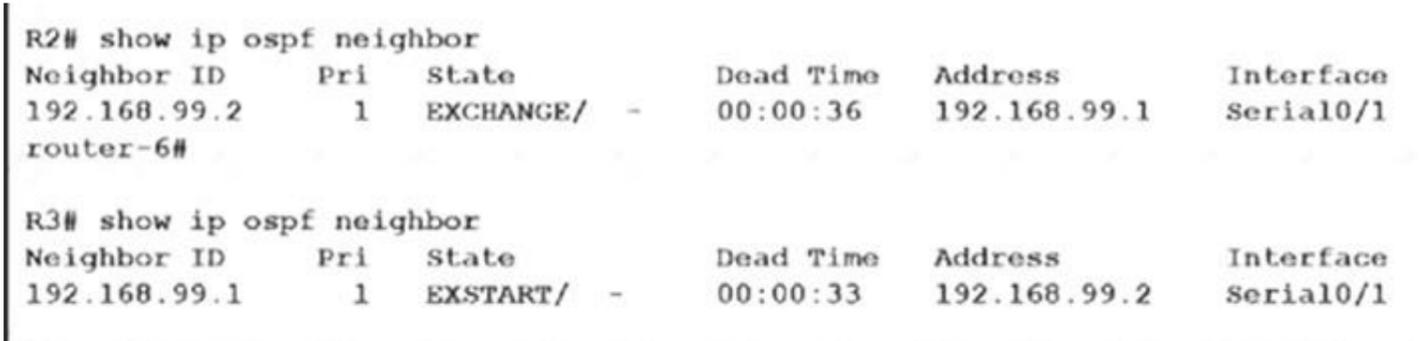
- A. RT must be globally unique within the same VPN
- B. RT must be globally identical within the same VPN
- C. RT values must be different from the RD values in the same VPN
- D. Each RT value must be identical to an RD value within the same VPN.

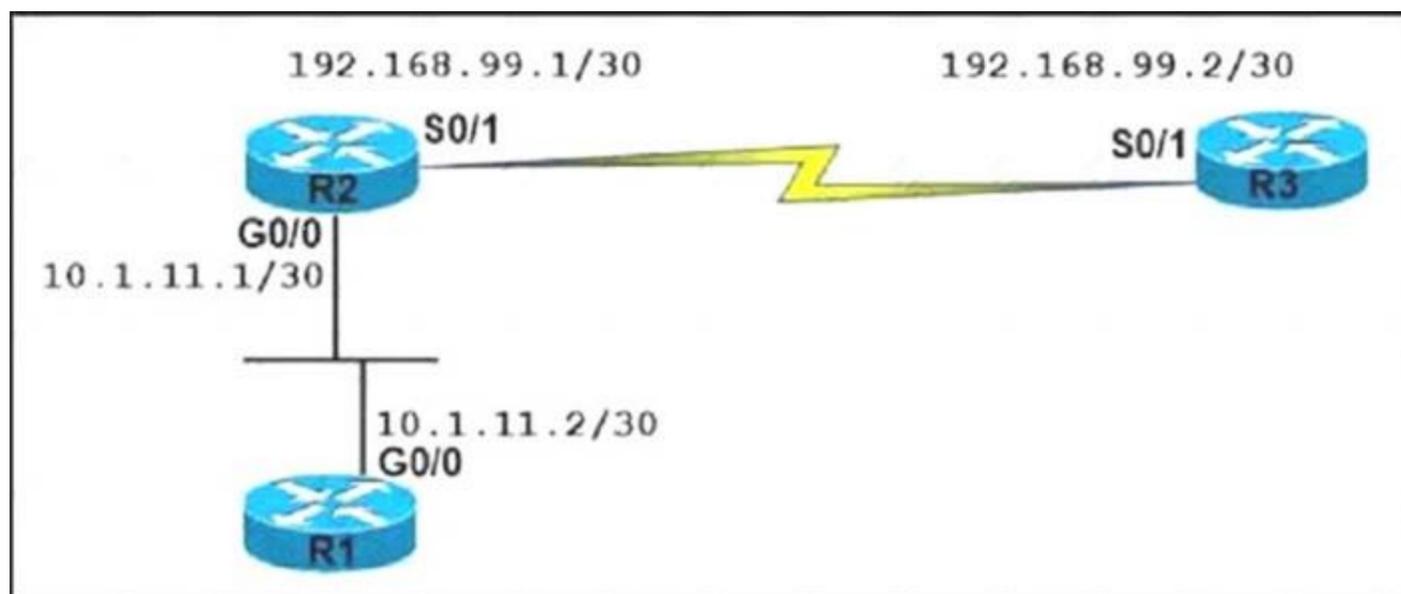
Answer: D

NEW QUESTION 57

- (Exam Topic 3)

Refer to the exhibit.





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

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

Answer: B

Explanation:

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

Neighbors Stuck in Exstart/Exchange State

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

NEW QUESTION 58

- (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 60

- (Exam Topic 3)
Refer to the exhibit.

```
RR# show running-config
!
interface Ethernet0/1
 no ip address
 ipv6 address 2001:DB8:1:12::2/64
 ipv6 traffic-filter ACL in
!
ipv6 access-list ACL
 sequence 10 permit tcp any any eq 22
 sequence 20 permit tcp any eq 22 any
 sequence 30 permit tcp any any eq bgp
 sequence 40 permit tcp any eq bgp any
 sequence 50 permit udp any any eq ntp
 sequence 60 permit udp any eq ntp any
 sequence 70 permit udp any any eq snmp
 sequence 80 deny ipv6 any any log

RR# show ipv6 cef ::/0
::/0
  nexthop 2001:DB8:1:12::1 Ethernet0/1

*Feb 23 00:23:17.211: %IPV6_ACL-6-ACCESSLOGDP: list ACL/80
denied icmpv6 2001:DB8:1:12::1 -> FF02::1:FF00:2 (135/0), 7321
packets
```

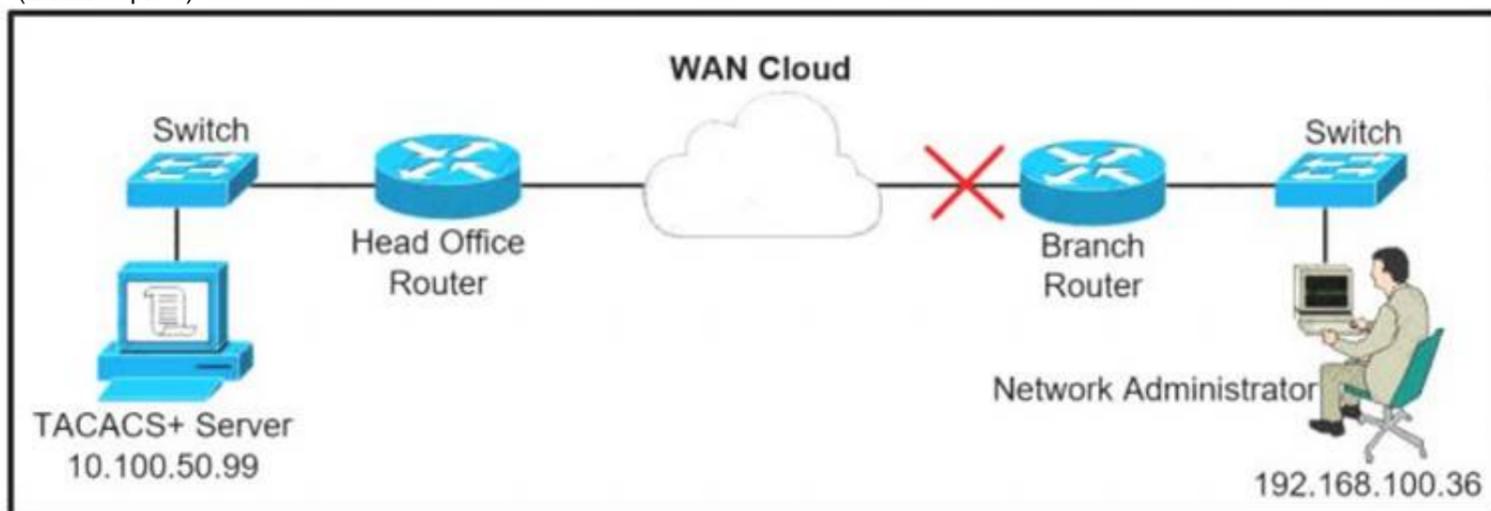
After a security audit, the administrator implemented an ACL in the route reflector. The RR became unreachable from any router in the network. Which two actions resolve the issue? (Choose two.)

- A. Enable the ND proxy feature on the default gateway.
- B. Configure a link-local address on the Ethernet0/1 interface.
- C. Permit ICMPv6 neighbor discovery traffic in the ACL.
- D. Remove the ACL entry 80.
- E. Change the next hop of the default route to the link-local address of the default gateway.

Answer: CD

NEW QUESTION 64

- (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 66

- (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 

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 customer_a
ip address 192.168.1.1 255.255.255.0
!
interface Gig0/1
ip vrf forwarding customer_b
ip address 192.168.1.2 255.255.255.0

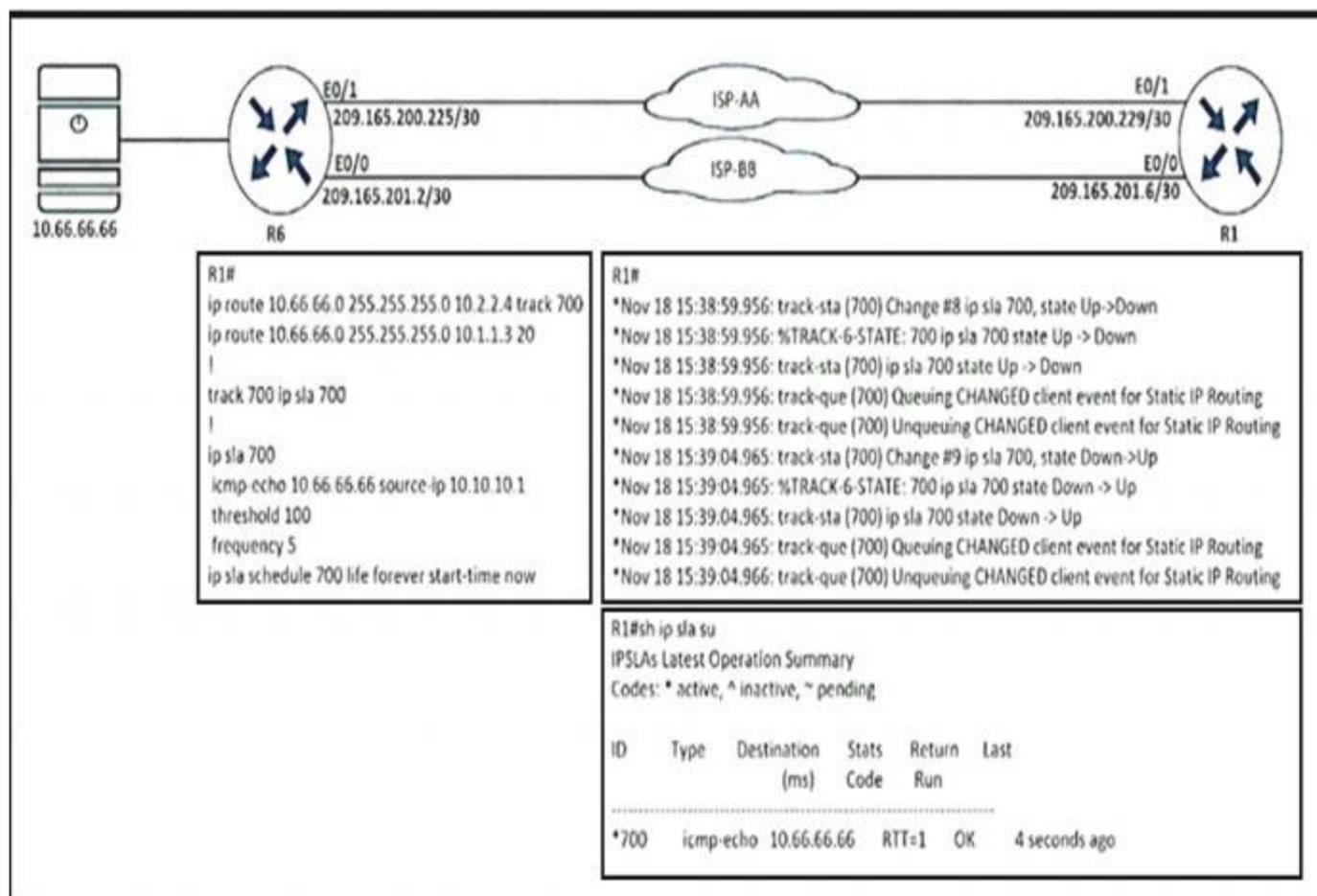
CE2
interface Gig0/0
ip vrf forwarding customer_a
ip address 192.168.1.1 255.255.255.0
!
interface Gig0/1
ip vrf forwarding customer_b
ip address 192.168.1.2 255.255.255.0
```

- customer_a
- customer_b
- 192.168.1.1 255.255.255.0
- 192.168.1.2 255.255.255.0

NEW QUESTION 71

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 73

- (Exam Topic 3)

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

```

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

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

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

Answer: C

Explanation:

The last command “aaa authentication login telnet group TAC-SERV” created the method list name telnet so we need to assign it to line vty.
Reference: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200208-Configure-ISE-2-0-IOS-TACACS-Authentic.html>

NEW QUESTION 77

- (Exam Topic 3)

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

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

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

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

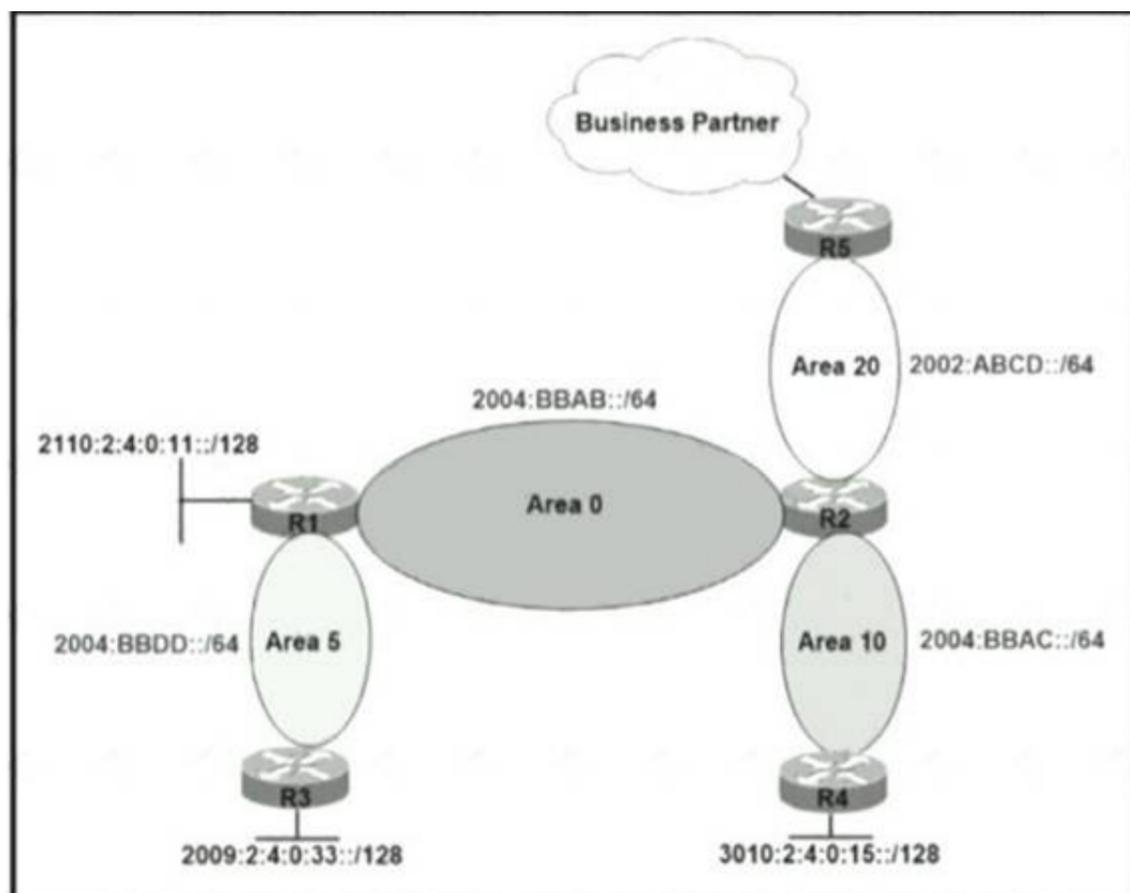
- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: CE

NEW QUESTION 81

- (Exam Topic 3)

Refer to the exhibit.



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

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

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

Answer: D

NEW QUESTION 85

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 87

- (Exam Topic 3)

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

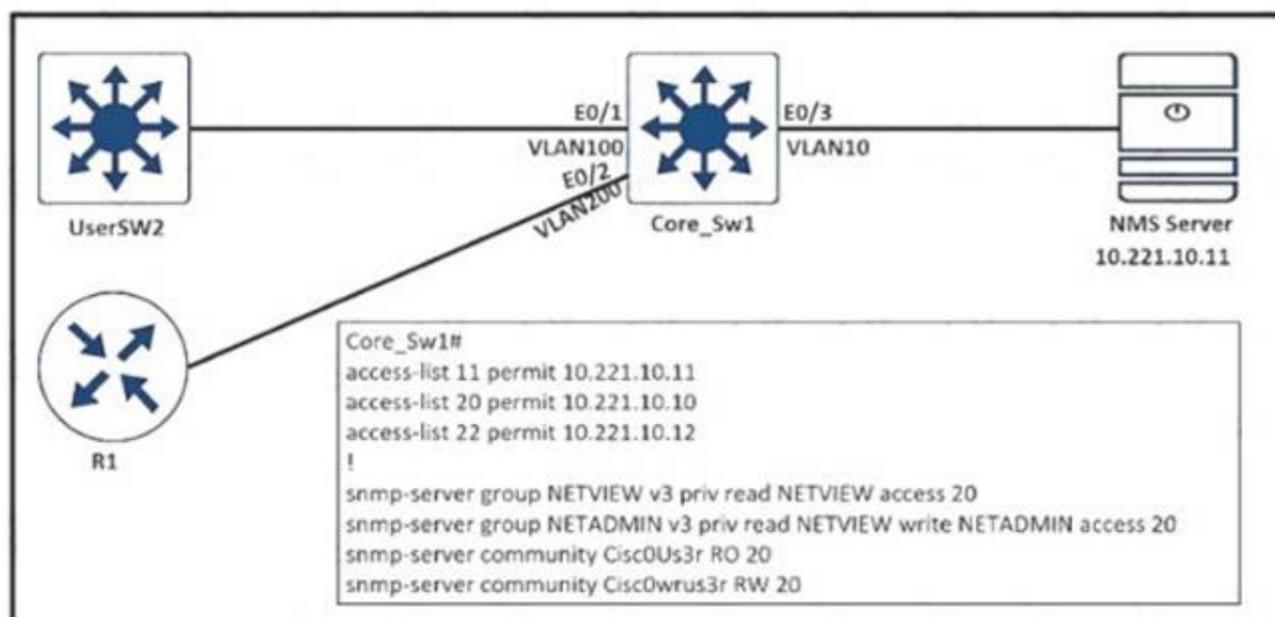
- A. 16-byte Route Distinguisher
- B. 8-byte Route Target
- C. 16-byte Route Target
- D. 8-byte Route Distinguisher

Answer: D

NEW QUESTION 92

- (Exam Topic 3)

Refer to the exhibit.



An engineer configured SNMP communities on the Core_SW1, but the SNMP server cannot obtain information from Core_SW1. Which configuration resolves this issue?

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

Answer: B

NEW QUESTION 94

- (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 99

- (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.

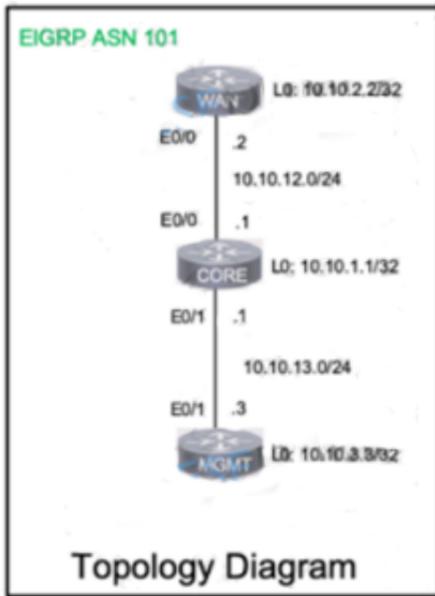
Answer: C

NEW QUESTION 102

- (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-act
tion drop
 class class-default
  police 8000 1500 1500 conform-action drop exceed-action d
rop
!
!

```

```

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

```

```

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

```

```

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

```

MGMT

WAN CORE **MGMT**

```

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

```

```

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

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

```

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

```

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

```

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

```

MGMT
 Graphical user interface, text Description automatically generated

```

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

MGMT#telnet 10.10.13.1
Trying 10.10.13.1 ... Open

Password required, but none set

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

NEW QUESTION 105

- (Exam Topic 3)

Refer to the exhibit.

```

R1#show ip route ospf

      10.0.0.0/24 is subnetted, 7 subnets
O E2   10.4.9.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0

           [110/200] via 10.4.15.5, 00:06:43,
FastEthernet0/1
O IA   10.4.27.0 [110/2] via 10.4.15.5, 00:06:44,
FastEthernet0/1
O E2   10.4.49.0 [110/200] via 10.4.17.6, 00:06:43,
FastEthernet0/0
    
```

An engineer configures two ASBRs 10.4.17.6 and 10.4.15.5 in an OSPF network to redistribute routes from EIGRP. However, both ASBRs show the EIGRP routes as equal costs even though the next-hop router 10.4.17.6 is closer to R1. How should the network traffic to the EIGRP prefixes be sent via 10.4.17.6?

- A. The administrative distance should be raised to 120 from the ASBR 10.4.15.5.
- B. The redistributed prefixes should be advertised as Type 1.
- C. The ASBR 10.4.17.6 should assign a tag to match and assign a lower metric on R1.
- D. The administrative distance should be raised to 120 from the ASBR 10.4.17.6.
- E. The administrative distance should be raised to 120 from the ASBR 10.4.15.5.
- F. The redistributed prefixes should be advertised as Type 1.
- G. The ASBR 10.4.17.6 should assign a tag to match and assign a lower metric on R1.
- H. The administrative distance should be raised to 120 from the ASBR 10.4.17.6.

Answer: B

NEW QUESTION 107

- (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?

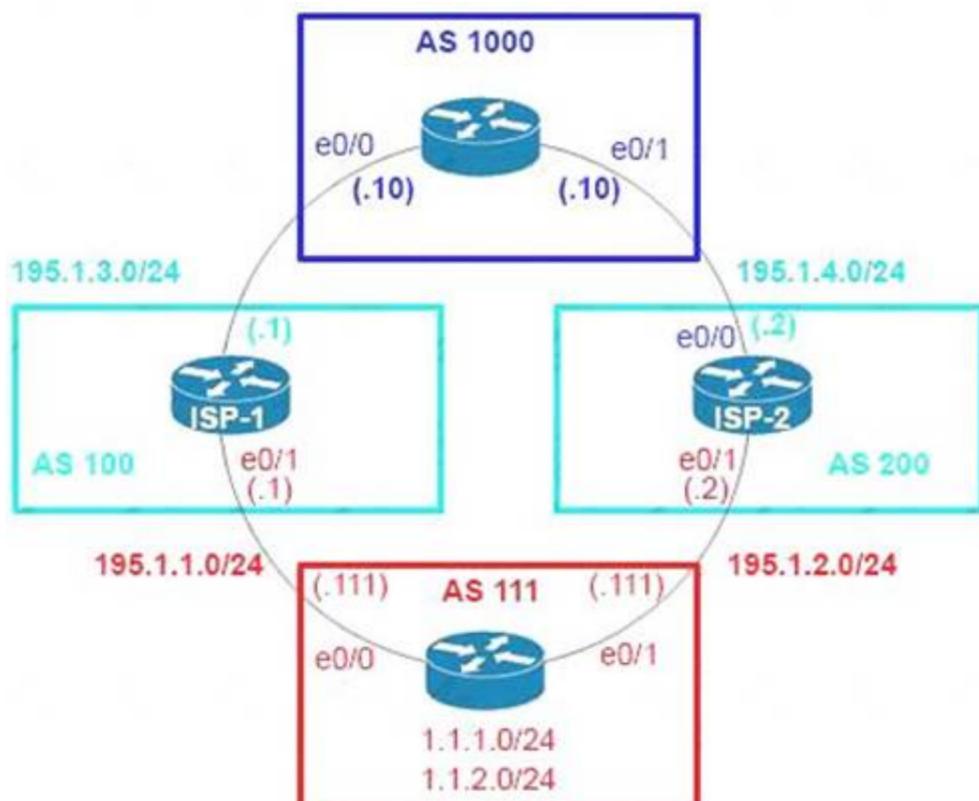
- A. Increase path bandwidth lower than 1011.2 and lower than 1012.2 between RtrA and the destination.
- B. Increase path bandwidth higher than 1011.2 and lower than 1012.2 between RtrA and the destination.
- C. Increase path bandwidth higher than 1011.2 and lower than 1012.2 between RtrA and the destination.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

Answer: A

NEW QUESTION 110

- (Exam Topic 3)

Refer to the exhibit.



```

AS111

Router bgp 111
Neighbor 195.1.1.1 remote-as 100
Neighbor 195.1.1.1 allowas-in
Neighbor 195.1.2.2 remote-as 200
Neighbor 195.1.2.2 allowas-in
    
```

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

- A)


```

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


```

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


```

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


```

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

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

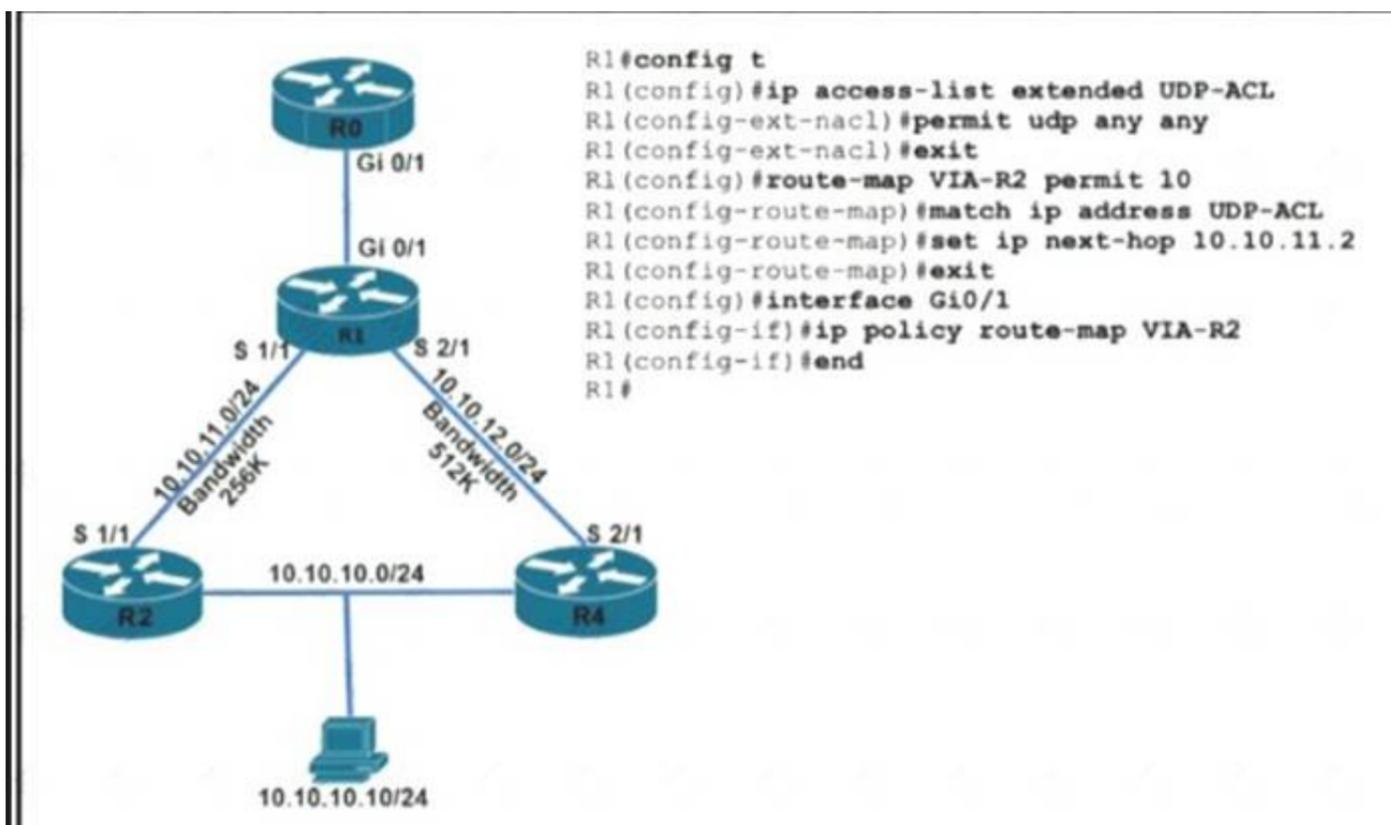
Answer: C

Explanation:

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

NEW QUESTION 113

- (Exam Topic 3)
Refer to the exhibit.



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

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

Answer: C

NEW QUESTION 118

- (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 121

- (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 125

- (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

NEW QUESTION 127

- (Exam Topic 3)

```

interface GigabitEthernet0/0
description FTP SERVER
no ip address
ipv6 address 2001:DB8::F/33
ipv6 enable
ipv6 traffic-filter FTP-SERVER in
!
interface GigabitEthernet0/1
description FTP CLIENT
no ip address
ipv6 address 2001:DB8:8000::F/33
ipv6 enable
ipv6 traffic-filter FTP-CLIENT in

ipv6 access-list FTP-CLIENT
permit tcp host 2001:DB8:8000::1 host 2001:DB8::1 eq ftp
permit tcp host 2001:DB8:8000::1 host 2001:DB8::1 eq ftp-data

ipv6 access-list FTP-CLIENT
permit tcp host 2001:DB8:8000::1 host 2001:DB8::1 eq ftp
permit tcp host 2001:DB8:8000::1 host 2001:DB8::1 eq ftp-data
!
ipv6 access-list FTP-SERVER
permit tcp host 2001:DB8::1 host 2001:DB8:8000::1 eq ftp established
permit tcp host 2001:DB8::1 host 2001:DB8:8000::1 eq ftp-data established
    
```

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 129

- (Exam Topic 3)

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

- Interface Tunnel0
tunnel mode ip
ip nhrp map multicast dynamic
- Interface Tunnel0
tunnel mode dvmrp
ip nhrp redirect
- Interface Tunnel0
tunnel mode ip
ip nhrp redirect
- Interface Tunnel0
tunnel mode gre multipoint
ip nhrp map multicast dynamic

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

Answer: D

NEW QUESTION 134

- (Exam Topic 3)

R1 and R2 are configured as eBGP neighbor, R1 is in AS100 and R2 is in AS200. R2 is advertising these networks to R1:

```
172.16.16.0/20
172.16.3.0/24
172.16.4.0/24
192.168.1.0/24
192.168.2.0/24
172.16.0.0/16
```

The network administrator on R1 must improve convergence by blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in, Which set of configurations accomplishes the task on R1?

- A. ip prefix-list PL-1 deny 172.16.0.0/16 le 23 ip prefix-list PL-1 permit 0.0.0.0/0 le 32!router bgp 100neighbor 192.168.100.2 remote-as 200 neighbor 192.168.100.2 prefix-list PL-1 in
- B. ip prefix-list PL-1 deny 172.16.0.0/16 ge 23 ip prefix-list PL-1 permit 0.0.0.0/0 le 32!router bgp 100neighbor 192.168.100.2 remote-as 200 neighbor 192.168.100.2 prefix-list PL-1 in
- C. access-list 1 deny 172.16.0.0 0.0.254.255 access-list 1 permit any!router bgp 100neighbor 192.168.100.2 remote-as 200neighbor 192.168.100.2 distribute-list 1 in
- D. ip prefix-list PL-1 deny 172.16.0.0/16 ip prefix-list PL-1 permit 0.0.0.0/0!router bgp 100neighbor 192.168.100.2 remote-as 200 neighbor 192.168.100.2 prefix-list PL-1 in

Answer: A

Explanation:

“Blocking all subnets of 172.16.0.0/16 major network with a mask lower than 23 from coming in” would block 172.16.16.0/20.

The first prefix-list “ip prefix-list PL-1 deny 172.16.0.0/16 le 23” means “all networks that fall within the 172.16.0.0/16 range AND that have a subnet mask of /23 or less” are denied.

The second prefix-list “ip prefix-list PL-1 permit 0.0.0.0/0 le 32” means allows all other prefixes.

NEW QUESTION 138

- (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 143

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 145

- (Exam Topic 3)

Refer to the exhibit.

```

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

```

An administrator must configure the router with OSPF for IPv4 and IPv6 networks under a single process. The OSPF adjacencies are not established and did not meet the requirement. Which action resolves the issue?

- A. Replace OSPF process 10 on the interface with OSPF process 1, and configure an additional router IDwith IPv6 address.

- B. Replace OSPF process 10 on the interface with OSPF process 1, for the IPv6 address and remove process route ID with IPv6 address.
- C. Replace OSPF process 10 on the interface with OSPF process 1, and remove process 10 from the global configuration.
- D. Replace OSPF process 10 on the interface with OSPF process 1 for the IPv4 address, and remove process 10 from the global configuration.

Answer: C

NEW QUESTION 146

- (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 150

- (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 154

- (Exam Topic 3)

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

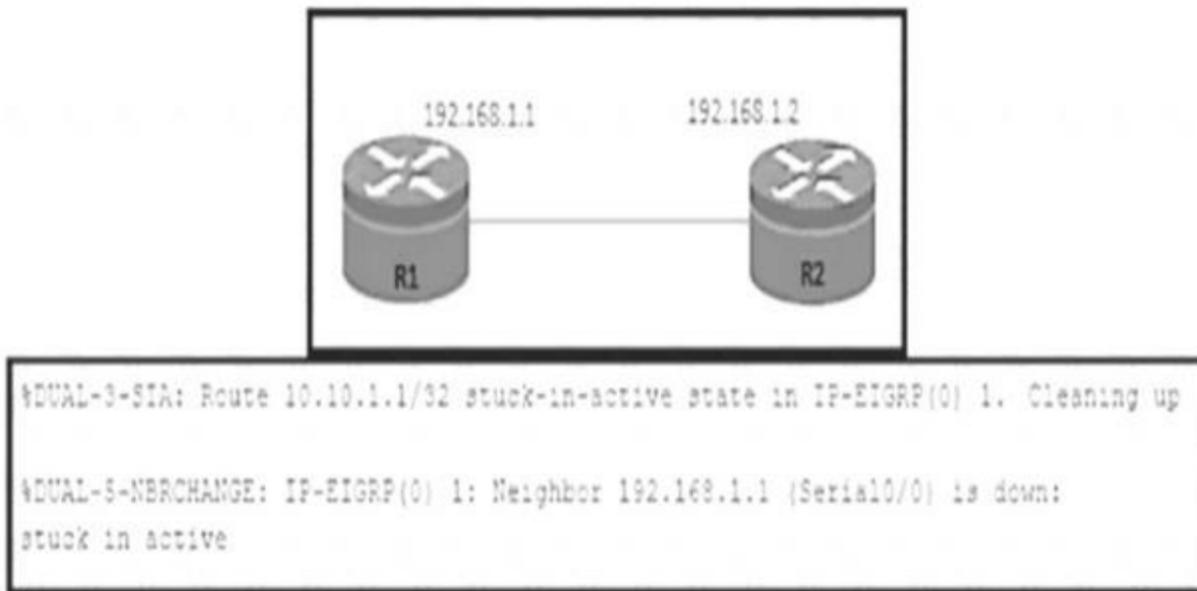
- A. no ip eigrp 1 mode multipoint
- B. no ip eigrp 1 split-horizon
- C. no ip eigrp 1 tunnel-redirect

D. no ip eigrp 1 mode mgre

Answer: B

NEW QUESTION 155

- (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 159

- (Exam Topic 3)

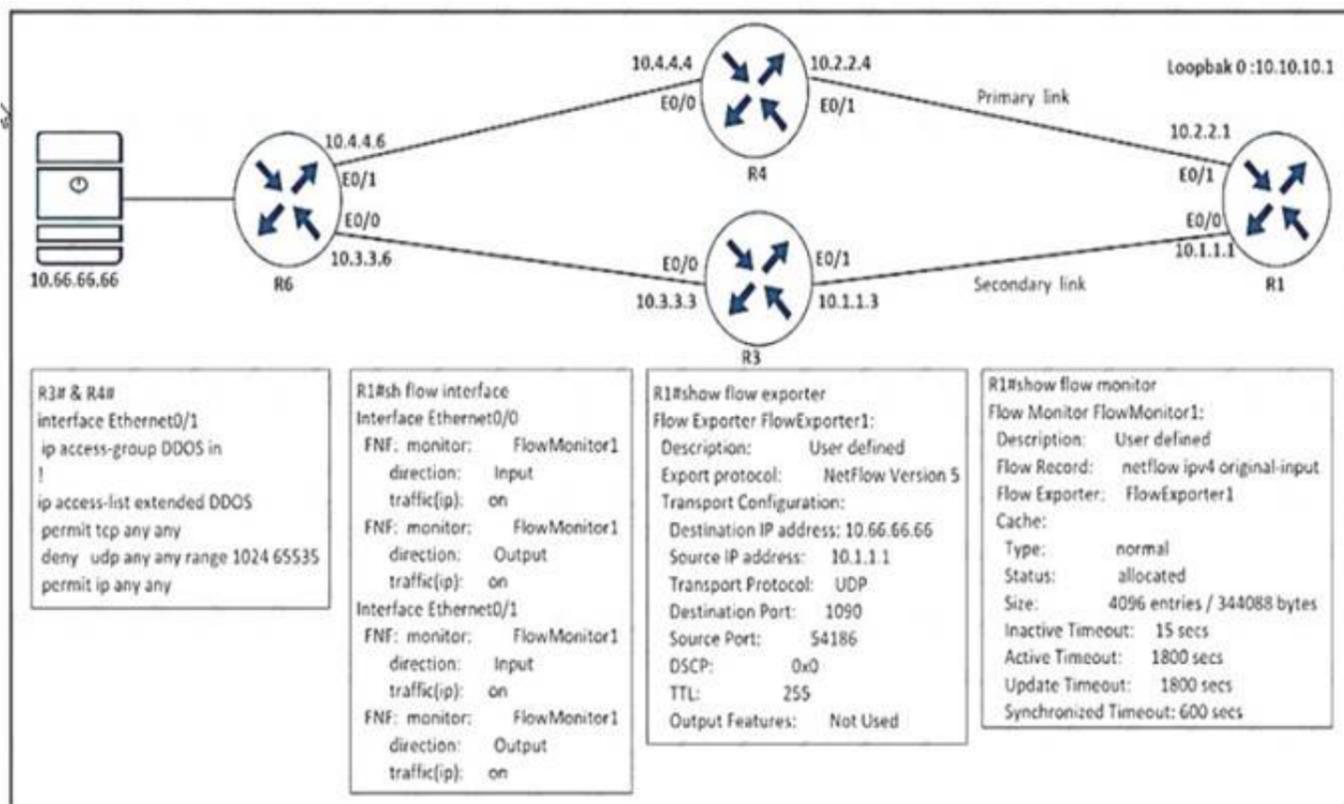
How is a preshared key "Test" for all the remote VPN routers configured in a DMVPN using GRE over IPsec set up?

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

Answer: D

NEW QUESTION 163

- (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 166

- (Exam Topic 3)

An engineer creates a Cisco DNA Center cluster with three nodes, but all the services are running on one host node. Which action resolves this issue?

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

Answer: C

Explanation:

To deploy Cisco DNA Center on a three-node cluster with High Availability (HA) enabled, complete the following procedure:

Step 1: Configure Cisco DNA Center on the first node in your cluster...

Step 2: Configure Cisco DNA Center on the second node in your cluster... Step 3: Configure Cisco DNA Center on the third node in your cluster... Step 4: Enable high availability on your cluster:

* a. In the Cisco DNA Center GUI, click and choose System Settings. The System 360 tab is displayed by default.

* b. In the Hosts area, click Enable Service Distribution.

After you click Enable Service Distribution, Cisco DNA Center enters into maintenance mode. In this mode, Cisco DNA Center is unavailable until the redistribution of services is completed. You should take this into account when scheduling an HA deployment.

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automationand-management/dna-center/1-3-3-0/ha_guide/b_cisco_dna_center_ha_guide_1_3_3_0.html

Therefore we can choose "Enable Service Distribution" to distribute services to other host nodes.

NEW QUESTION 170

- (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 175

- (Exam Topic 3)

What is the purpose of the DHCPv6 Guard?

- A. It messages between a DHCPv6 server and a DHCPv6 client (or relay agent).
- B. It shows that clients of a DHCPv5 server are affected.
- C. It block DHCPv6 messages from relay agents to a DHCPv6 server.
- D. It allows DHCPv6 replay and advertisements from (rouge) DHCPv6 servers.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6fxe-16-book/ip6-dhcpv6-guard.html

NEW QUESTION 178

- (Exam Topic 3)

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

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

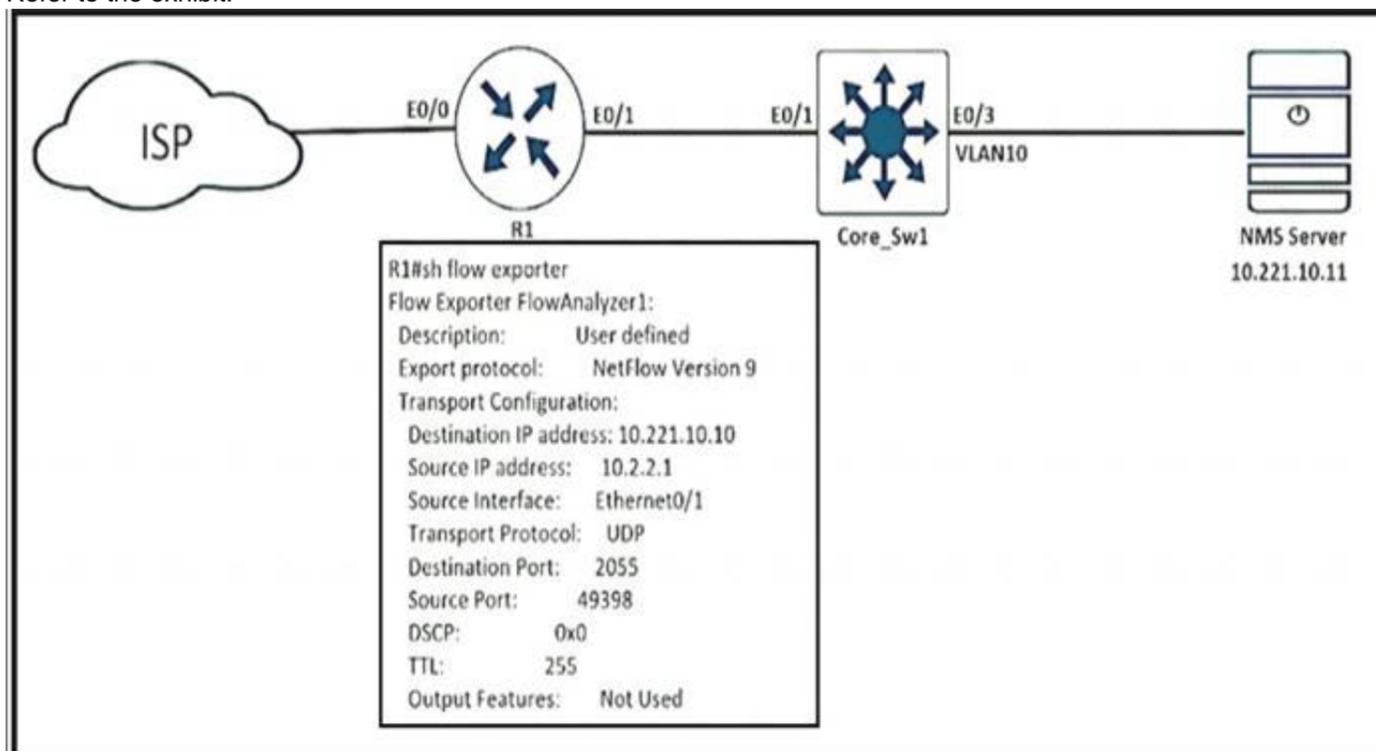
- A. R1 is a route reflector client of a RR with a router ID of 1.1.1.1, and the originator of the prefix has a router ID of 3.3.3.3. Both routers belong to different AS
- B. The prefix is not advertised to any peer and must be advertised using the network statement on R3.
- C. R1 is a route reflector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

Answer: D

NEW QUESTION 179

- (Exam Topic 3)

Refer to the exhibit.



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

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

Answer: B

Explanation:

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

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

NEW QUESTION 184

- (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?

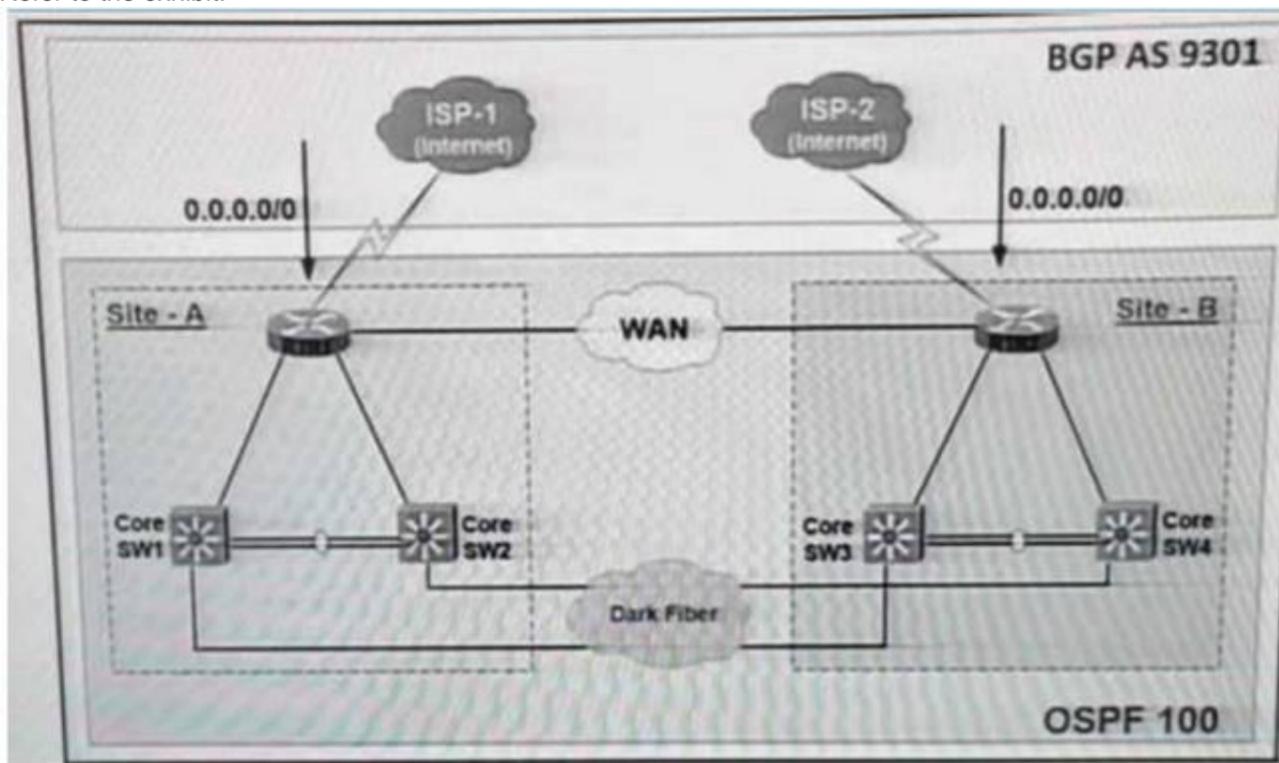
- A. Configure the redistribute static metric 200 subnets command under OSPF.
- B. Configure OSPF on the Dialer0 interface.
- C. Configure the network 0.0.0.0 255.255.255.255 area 0 command under OSPF.
- D. Configure the default-information originate command under OSPF.

Answer: D

NEW QUESTION 188

- (Exam Topic 3)

Refer to the exhibit.



The Internet traffic should always prefer Site-A ISP-1 if the link and BGP connection are up; otherwise, all Internet traffic should go to ISP-2. Redistribution is configured between BGP and OSPF routing protocols and it is not working as expected. What action resolves the issue?

- A. Set metric-type 2 at Site-A RTR1, and set metric-type 1 at Site-B RTR2
- B. Set OSPF cost 100 at Site-A RTR1, and set OSPF Cost 200 at Site-B RTR2
- C. Set OSPF cost 200 at Site-A RTR1 and set OSPF Cost 100 at Site-B RTR2
- D. Set metric-type 1 at Site-A RTR1, and set metric-type 2 at Site-B RTR2

Answer: D

Explanation:

OSPF type 1 route is always preferred over a type 2 route for the same destination so we can set metric-type 1 at Site-A RTR1 so that it is preferred over Site-B RTR2.

Note:

Routes are redistributed in OSPF as either type 1 (E1) routes or type 2 (E2) routes, with type 2 being the default.

- A type 1 route has a metric that is the sum of the internal OSPF cost and the external redistributed cost.
- A type 2 route has a metric equal only to the redistributed cost.
- If routes are redistributed into OSPF as type 2 then every router in the OSPF domain will see the same cost to reach the external networks.
- If routes are redistributed into OSPF as type 1, then the cost to reach the external networks could vary from router to router.

NEW QUESTION 192

- (Exam Topic 3)

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

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

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

Answer: A

NEW QUESTION 195

- (Exam Topic 2)

```
ip prefix-list DefaultRouteOnly seq 5 deny 0.0.0.0/0 le 32
ip prefix-list DefaultRouteOnly seq 10 permit 0.0.0.0/0

router eigrp ccnp
 address-family ipv4 unicast autonomous-system 1
 topology base
 distribute-list prefix DefaultRouteOnly out Tunnel0
```

Refer to the exhibit. The administrator configured route advertisement to a remote low resources router to use only the default route to reach any network but failed. Which action resolves this issue?

- A. Change the direction of the distribute-list command from out to in.
- B. Remove the line with the sequence number 5 from the prefix list.
- C. Remove the prefix keyword from the distribute-list command.
- D. Remove the line with the sequence number 10 from the prefix list.

Answer: B

NEW QUESTION 200

- (Exam Topic 2)

An engineer configured a DHCP server for Cisco IP phones to download its configuration from a TFTP server, but the IP phones failed to load the configuration. What must be configured to resolve the issue?

- A. BOOTP port 67
- B. DHCP option 66
- C. BOOTP port 68
- D. DHCP option 69

Answer: B

Explanation:

Command	Purpose
<code>dhcpd option 66 ascii server_name</code>	Provides the IP address or name of a TFTP server for option 66.
Example:	
<code>hostname(config)# dhcpd option 66 ascii exampleserver</code>	

DHCP options 3, 66, and 150 are used to configure Cisco IP Phones. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information. + DHCP option 150 provides the IP addresses of a list of TFTP servers. + DHCP option 66 gives the IP address or the hostname of a single TFTP server.

Reference:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/basic_dhcp.pdf

NEW QUESTION 203

- (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

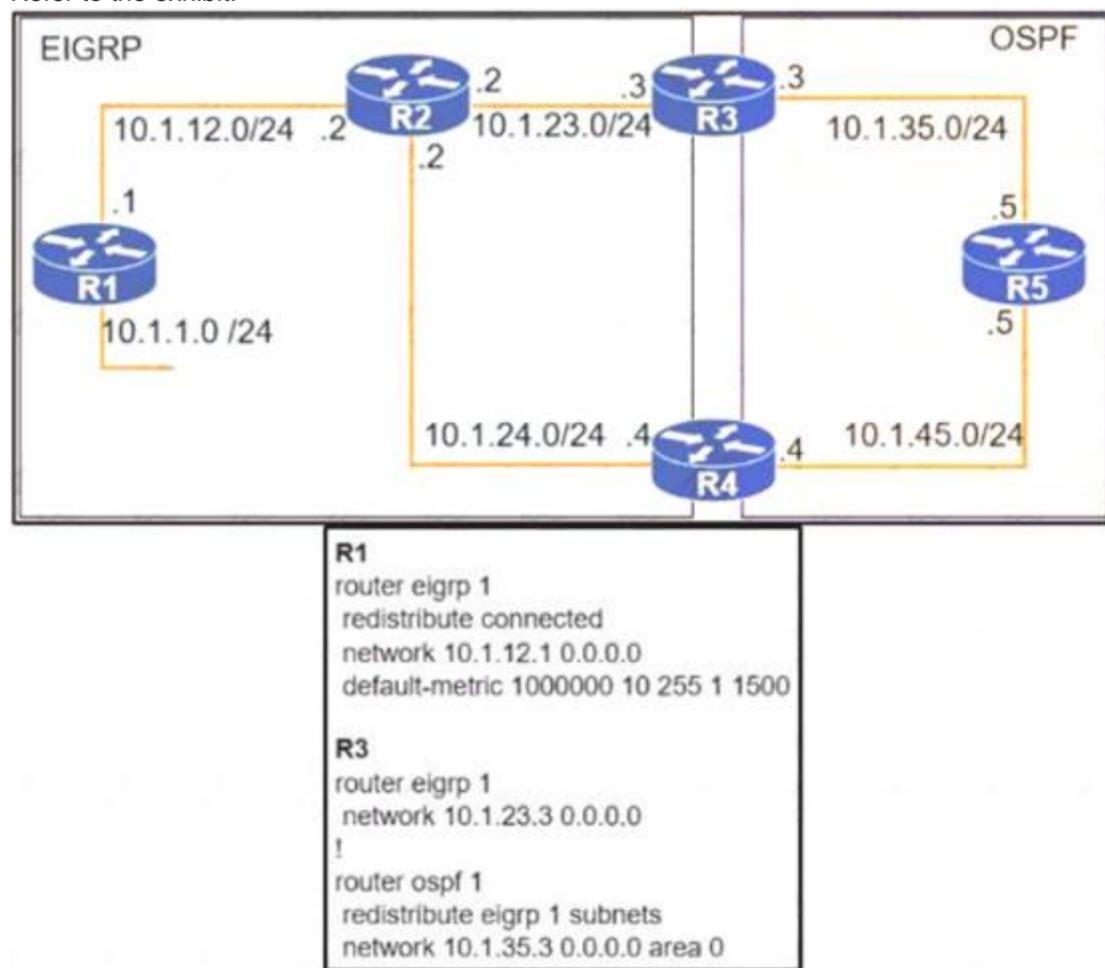
Explanation:

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 208

- (Exam Topic 2)

Refer to the exhibit.



To provide reachability to network 10.1.1.0 /24 from R5, the network administrator redistributes EIGRP into OSPF on R3 but notices that R4 is now taking a path through R5 to reach 10.1.1.0/24 network. Which action fixes the issue while keeping the reachability from R5 to 10.1.1.0/24 network?

- A. Change the administrative distance of the external EIGRP to 90.
- B. Apply the outbound distribution list on R5 toward R4 in OSPF.
- C. Change the administrative distance of OSPF to 200 on R5.
- D. Redistribute OSPF into EIGRP on R4

Answer: A

NEW QUESTION 209

- (Exam Topic 2)

Refer to the exhibit.

```

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

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

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

Answer: C

NEW QUESTION 214

- (Exam Topic 2)

Refer to the exhibit.

```

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

```

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

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

Answer: A

Explanation:

In order to use a prefix-list in a route-map, we must use the keyword "prefix-list" in the "match" statement. . For example:
 match ip address prefix-list WAN_PREFIXES
 Without this keyword, the router will try to find an access-list with the same name instead.

NEW QUESTION 215

- (Exam Topic 2)
Refer to Exhibit.

```

HQ_R2 9000
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.2 track 1
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.16.35.6 5
 |
BRANCH(config)# ip sla 1
BRANCH(config-ip-sla)# icmp-echo 172.16.35.6
BRANCH(config-ip-sla)# timeout 200
BRANCH(config-ip-sla)# frequency 5
 |
BRANCH(config)# ip sla schedule 1 life forever start-time now
 |
BRANCH(config)# track 1 ip sla 1 reachability

```

Traffic from the branch network should route through HQ R1 unless the path is unavailable. An engineer tests this functionality by shutting down interface on the BRANCH router toward HQ_R1 router but 192.168.20.0/24 is no longer reachable from the branch router. Which set of configurations resolves the issue?

- A. HQ_R1(config)# ip sla responderHQ_R1(config)# ip sla responder icmp-echo 172.16.35.2
- B. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 172.16.35.1
- C. HQ_R2(config)# ip sla responderHQ_R2(config)# ip sla responder icmp-echo 172.16.35.5
- D. BRANCH(config)# ip sla 1BRANCH(config-ip-sla)# icmp-echo 172.16.35.2

Answer: D

Explanation:

In the configuration above, the engineer has made a mistake as he was tracking 172.16.35.6 (the backup path) instead of tracking the main path (172.16.35.2). Therefore,when he shut down the main path, the track 1 was still up so traffic still went through the main path -> it failed. To fix this issue, we just need to correct the tracking interface of the main path.

NEW QUESTION 218

- (Exam Topic 2)
Drag and drop the MPLS VPN device types from the left onto the definitions on the right.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 219

- (Exam Topic 2)

```

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

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

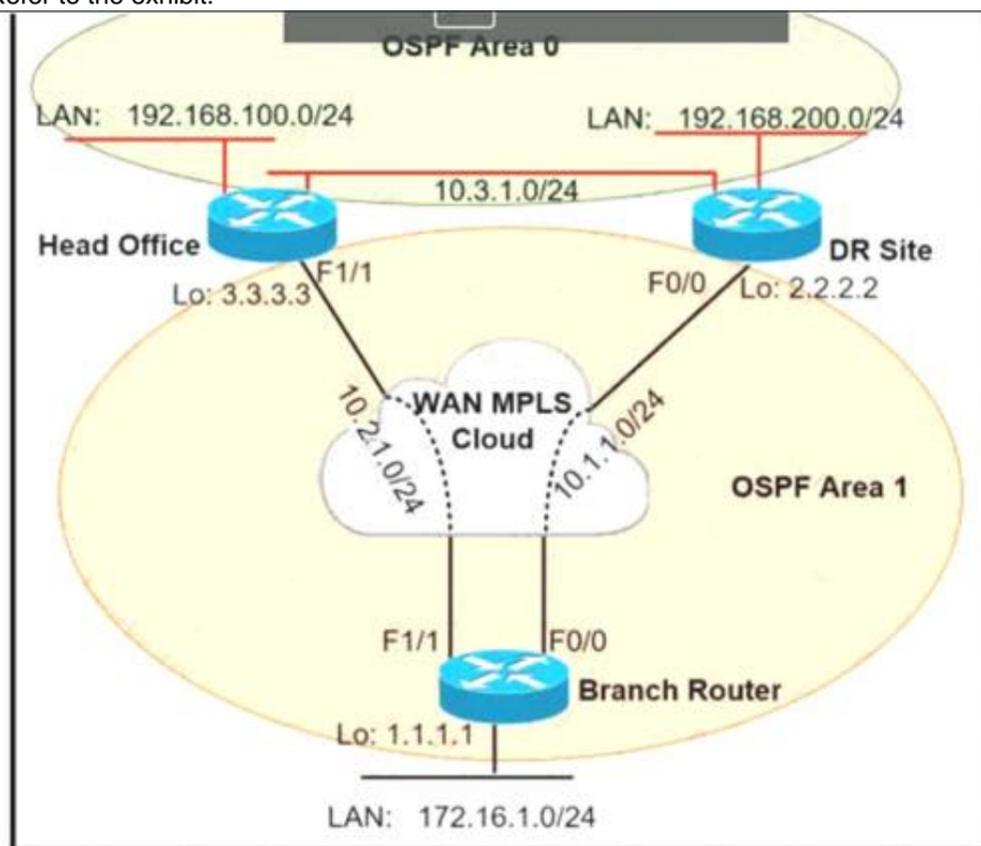
- A. ipv6 access-list inbound permit tcp any any syn deny ipv6 any any log!interface gi0/0ipv6 traffic-filter inbound out
- B. ipv6 access-list inbound permit tcp any any syn deny ipv6 any any log!interface gi0/0ipv6 traffic-filter inbound in
- C. ipv6 access-list inbound permit tcp any any establisheddeny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

Answer: C

NEW QUESTION 220

- (Exam Topic 2)

Refer to the exhibit.



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

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

Answer: A

NEW QUESTION 225

- (Exam Topic 2)

Refer to the exhibit.

```

Configuration Output:
aaa new-model
!
aaa authentication login default local
aaa authentication login VTY_AUTH local
aaa authorization exec default none
aaa authorization exec VTY_AUTH local
aaa accounting exec default start-stop group radius
!

password 7 K0AyUubDrfOgO4s
authorization exec VTY_AUTH
login authentication VTY_AUTH
!

Debug Output:
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x4B6): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
    
```

Which action resolves the failed authentication attempt to the router?

- A. Configure aaa authorization login command on line vty 0 4
- B. Configure aaa authorization login command on line console 0
- C. Configure aaa authorization console global command
- D. Configure aaa authorization console command on line vty 0 4

Answer: C

Explanation:

In the debug output, we see that the Authorization (not Authentication) failed so we need to correct the authorization. In order to enable authorization, we must use the global command “aaa authorization console” first.

Reference:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-a1.html>

NEW QUESTION 228

- (Exam Topic 2)

Refer to Exhibit.

```

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

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

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

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

- A. Configure access-list 100 permit udp any any eq 61 as the first line
- B. Configure access-list 100 permit udp any any eq 86 as the first line
- C. Configure access-list 100 permit udp any any eq 68 as the first line
- D. Configure access-list 100 permit udp any any eq 69 as the first line

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

Answer: CE

Explanation:

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

...

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

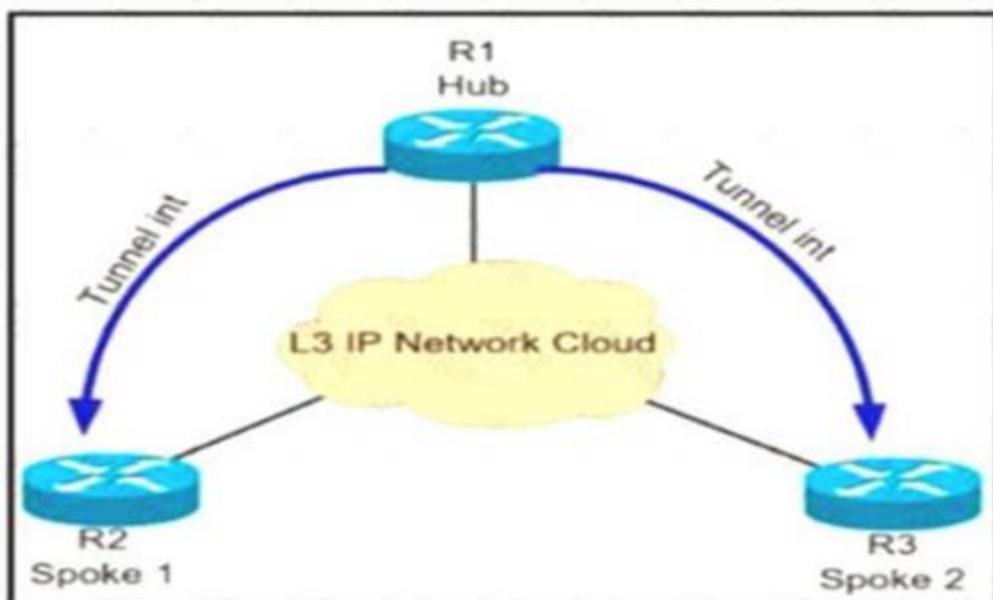
Reference:

<https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html>

NEW QUESTION 231

- (Exam Topic 2)

Refer to Exhibit.



A network administrator has successfully configured DMVPN topology between a hub and two spoke routers. Which two configuration commands should establish direct communications between spoke 1 and spoke 2 without going through the hub? (Choose two).

- A. At the hub router, configure the ip nhrp shortcut command.
- B. At the spoke routers, configure the ip nhrp spoke-tunnel command.
- C. At the hub router, configure ip nhrp redirect the command
- D. At the spoke routers, configure the ip nhrp shortcut command.
- E. At the hub router, configure the ip nhrp spoke-tunnel command

Answer: CD

Explanation:

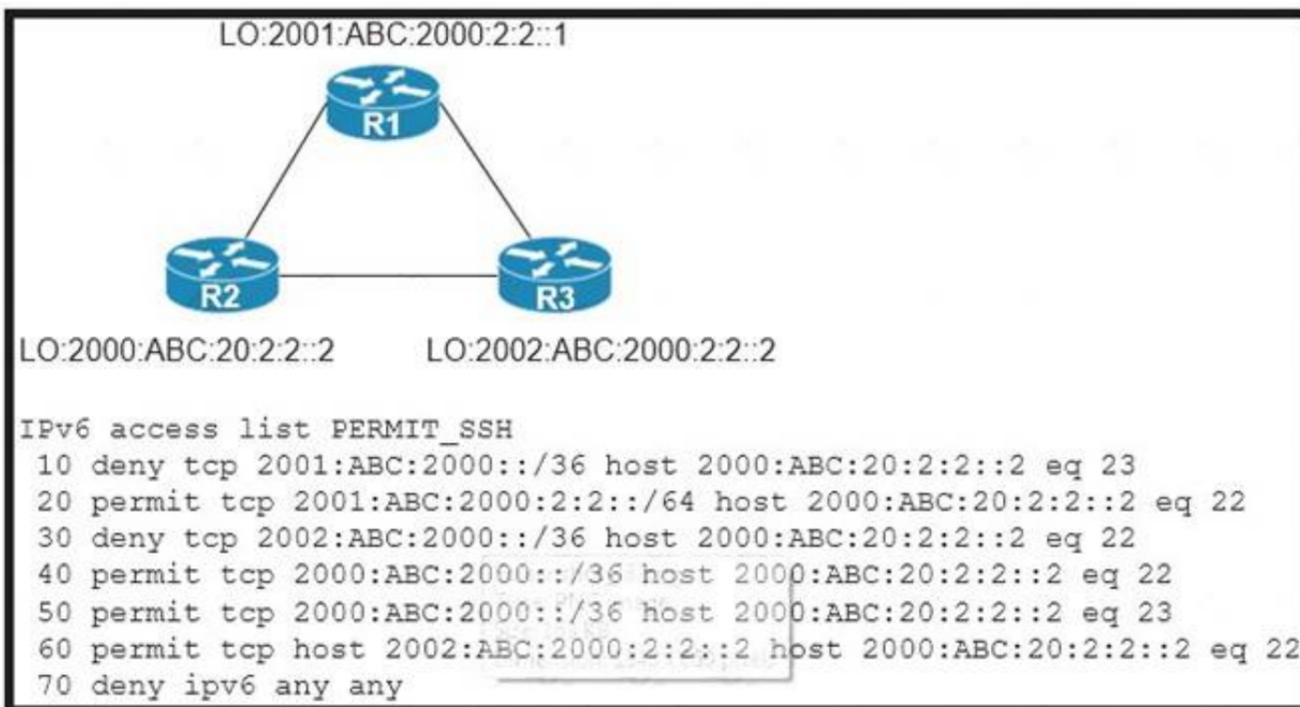
To configure Spoke to Spoke communication we can configure DMVPN Phase II or Phase III. But in Phase II, the first few packets would go through Hub. In order to totally ignore the hub, we have to use DMVPN Phase III:

DMVPN Phase III is same as Phase 2 but removes some restrictions and complexities of Phase 2. Also allows greater variety of DMVPN network designs we use:
 + ip nhrp redirect in hub: tells the initiator spoke to look for a better path to the destination spoke than through the Hub. Upon receiving the NHRP redirect message the spokes communicate with each other over the hub and they have their NHRP replies for the NHRP Resolution Requests that they sent out.
 + ip nhrp shortcut in spokes: overwrite the CEF table on the spoke. It basically overrides the next-hop value for a remote spoke network from the default initial hubtunnel IP address to the NHRP resolved remote spoke tunnel IP address)

NEW QUESTION 232

- (Exam Topic 2)

Refer to the exhibit.



An IPv6 network was newly deployed in the environment and the help desk reports that R3 cannot SSH to the R2s Loopback interface. Which action resolves the

issue?

- A. Modify line 10 of the access list to permit instead of deny.
- B. Remove line 60 from the access list.
- C. Modify line 30 of the access list to permit instead of deny.
- D. Remove line 70 from the access list.

Answer: C

NEW QUESTION 233

- (Exam Topic 2)

Which two components are needed for a service provider to utilize the LVPN MPLS application? (Choose two.)

- A. The P routers must be configured for MP-iBGP toward the PE routers
- B. The P routers must be configured with RSVP.
- C. The PE routers must be configured for MP-iBGP with other PE routers
- D. The PE routers must be configured for MP-eBGP to connect to CEs
- E. The P and PE routers must be configured with LDP or RSVP

Answer: CE

Explanation:

MPLS Network Protocols

+ IGP: OSPF, EIGRP, IS-IS on core facing and core links+ RSVP and/or LDP on core and/or core facing links

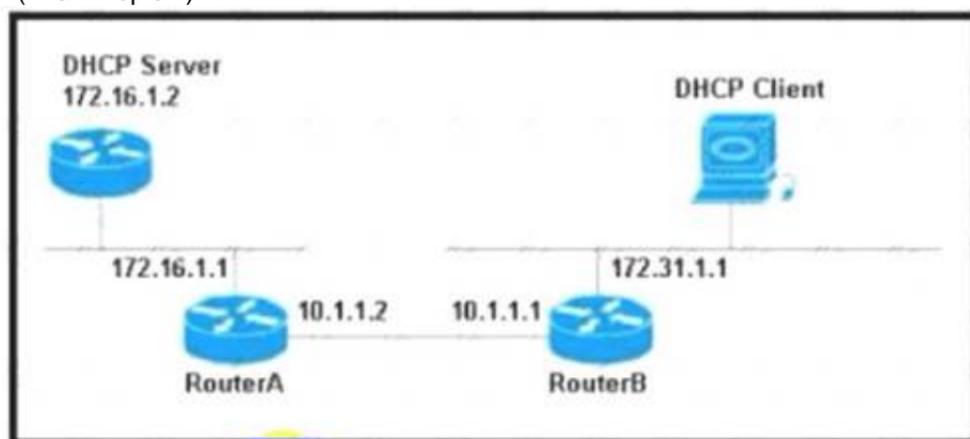
->

+ MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN -> .

Reference: <https://www.uio.no/studier/emner/matnat/ifi/IN3230/h19/kursmaterieell/mpls-lecture.pdf>

NEW QUESTION 234

- (Exam Topic 2)



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

Interface fastethernet 0/0

description Client DHCP ID 394482431 Ip address 172 31 11 255 255.255 0

!

ip route 172.16.1.0 255 255 255.0 10.1.1.2

Which command is required on the fastethernet 0/0 interface of RouterB to resolve this issue?

- A. RouterB(config-if)#ip helper-address 172.31.1.1
- B. RouterB(config-if)#ip helper-address 255.255.255.255
- C. RouterB(config-if)#ip helper-address 172.16.1.1
- D. RouterB(config-if)#ip helper-address 172.16.1.2

Answer: D

NEW QUESTION 236

- (Exam Topic 2)

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

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

Answer: CD

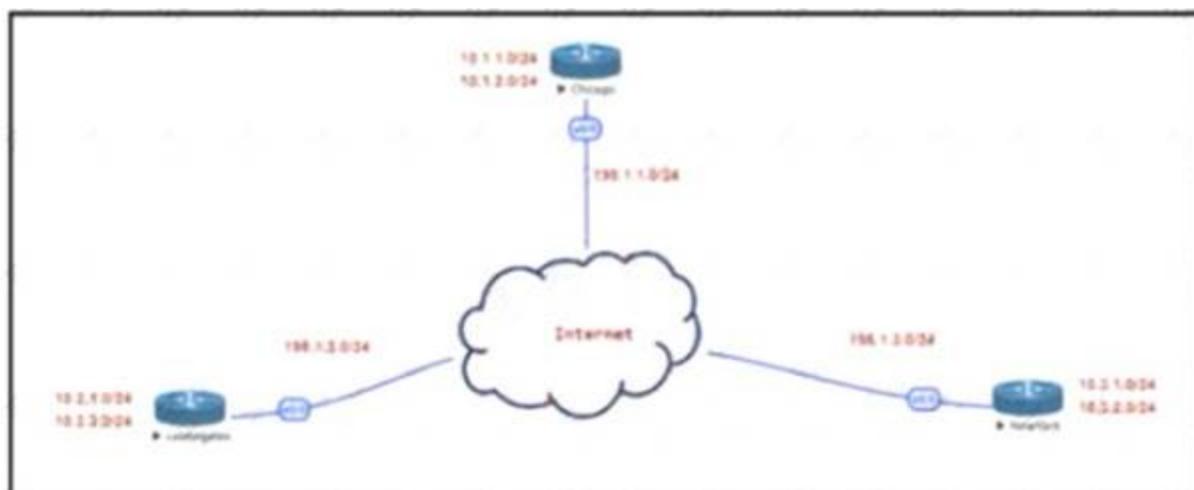
Explanation:

Reference:

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

NEW QUESTION 238

- (Exam Topic 2)



```
Chicago

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 map multicast dynamic
no ip next-hop-self eigrp 111
tunnel protection ipsec profile IPsec-PROFILE
!
router eigrp 111
network 192.168.1.0
network 10.0.0.0
```

Refer to the exhibit. The Los Angeles and New York routers are receiving routes from Chicago but not from each other Which configuration fixes the issue?

- A. Interface Tunnel1 no ip split-horizon eigrp 111
- B. Interface Tunnel1 ip next-hop-self eigrp 111
- C. Interface Tunnel1 tunnel mode ipsec ipv4
- D. Interface Tunnel1 tunnel protection ipsec profile IPsec-PROFILE

Answer: A

Explanation:

In this topology, Chicago router (Hub) will receive advertisements from Los Angeles (Spoke1) router on its tunnel interface. The problem here is that it also has a connection with New York (Spoke2) on that same tunnel interface. If we don't disable EIGRP split-horizon, then the Hub will not relay routes from Spoke1 to Spoke2 and the other way around. That is because it received those routes on interface Tunnel1 and therefore it cannot advertise back out that same interface (split-horizon rule). Therefore we must disable split-horizon on the Hub router to make sure the Spokes know about each other.

NEW QUESTION 242

- (Exam Topic 2)

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

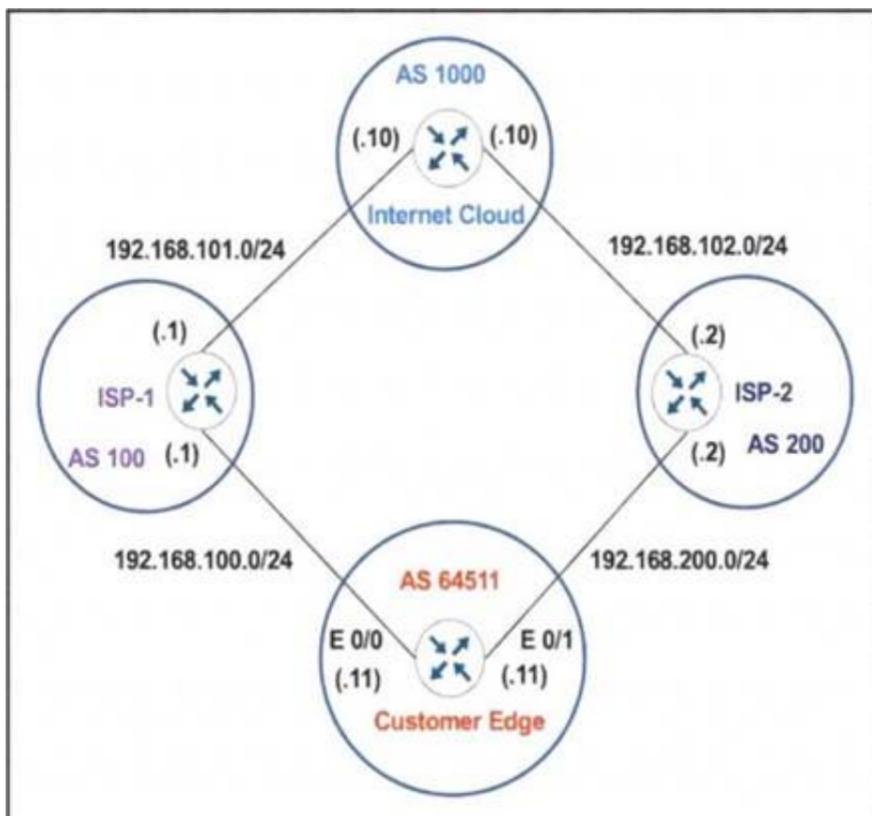
Refer to the exhibit. Which action restores the routes from neighbors while still filtering 1.1.1.0/24?

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

Answer: D

NEW QUESTION 247

- (Exam Topic 2)



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

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

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

- A. router bgp 64511 aggregate-address 172.16.20.0 255.255.252.0 summary-only
- B. router bgp 64511 neighbor 192.168.100.1 summary-only neighbor 192.168.200.2 summary-only
- C. interface E 0/0 ip bgp suppress-map BLOCK_SPECIFIC ! interface E 0/1 ip bgp suppress-map BLOCK_SPECIFIC ! ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22 ge 24 ! route-map BLOCK_SPECIFIC permit 10 match ip address prefix-list PL_BLOCK_SPECIFIC
- D. ip prefix-list PL_BLOCK_SPECIFIC deny 172.16.20.0/22 ge 22 ip prefix-list PL_BLOCK_SPECIFIC permit 172.16.20.0/22 ! route-map BLOCK_SPECIFIC permit 10 match ip address prefix-list PL_BLOCK_SPECIFIC ! router bgp 64511 aggregate-address 172.16.20.0 255.255.252.0 suppress-map BLOCK_SPECIFIC

Answer: A

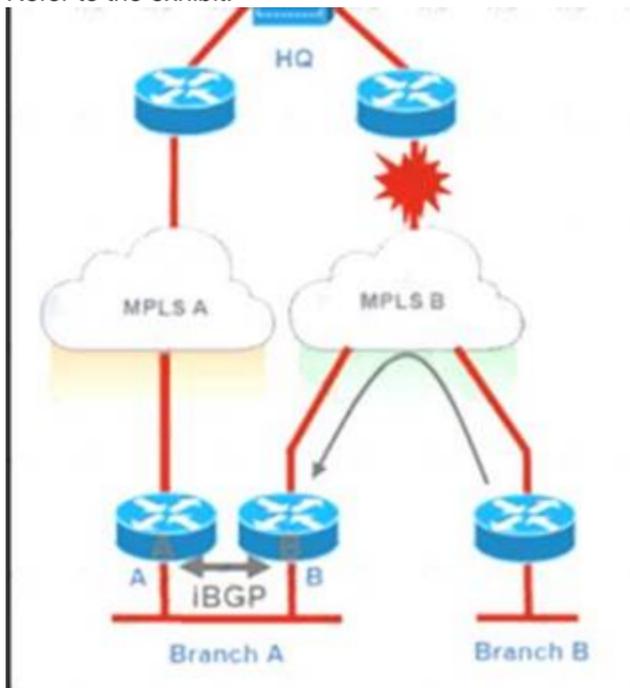
Explanation:

When the aggregate-address command is used within BGP routing, the aggregated address is advertised, along with the more specific routes. The exception to this rule is through the use of the summary-only command. The "summary-only" keyword suppresses the more specific routes and announces only the summarized route.

NEW QUESTION 251

- (Exam Topic 2)

Refer to the exhibit.



Troubleshoot and ensure that branch B only ever uses the MPLS B network to reach HQ. Which action achieves this requirement?

- A. Introduce an AS path filter on branch A routers so that only local prefixes are advertised into BGP
- B. increase the local preference for all HQ prefixes received at branch B from the MPLS B network to be higher than the local preferences used on the MPLS A network
- C. Introduce AS path prepending on the branch A MPLS B network connection so that any HQ advertisements from branch A toward the MPLS B network are prepended three times

D. Modify the weight of all HQ prefixes received at branch B from the MPLS B network to be higher than the weights used on the MPLS A network

Answer: A

Explanation:

If we modify the weight, increase local preference or use AS path prepending then we can only make MPLS B prefer over MPLS A. But when MPLS B is down then MPLS A will be used which does not meet the requirement of this question. Only with AS path filtering we can deny prefixes from certain AS and make sure branch B never uses MPLS A to reach HQ.

NEW QUESTION 254

- (Exam Topic 1)

Refer to the exhibit.

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

An engineer is trying to configure local authentication on the console line, but the device is trying to authenticate using TACACS+. Which action produces the desired configuration?

- A. Add the aaa authentication login default none command to the global configuration.
- B. Replace the capital "C" with a lowercase "c" in the aaa authentication login Console local command.
- C. Add the aaa authentication login default group tacacs+ local-case command to the global configuration.
- D. Add the login authentication Console command to the line configuration

Answer: D

Explanation:

Reference:

<https://community.cisco.com/t5/switching/how-to-define-login-local-for-console-0/td-p/2949493>

NEW QUESTION 255

- (Exam Topic 1)

Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface on the hub, to support multiple connections from multiple spoke devices?

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

Answer: A

NEW QUESTION 259

- (Exam Topic 1)

Drag and drop the addresses from the left onto the correct IPv6 filter purposes on the right.

permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443	Permit NTP from this source 2001:0D8B:0800:200c::1f
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514	Permit syslog from this source 2001:0D88:0800:200c::1c
permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80	Permit HTTP from this source 2001:0D8B:0800:200c::0fff
permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123	Permit HTTPS from this source 2001:0D8B:0800:200c::07ff

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

HTTP and HTTPS run on TCP port 80 and 443, respectively and we have to remember them.

Syslog runs on UDP port 514 while NTP runs on UDP port 123 so if we remember them we can find out the matching answers easily. But maybe there is some typos in this question as 2001:d88:800:200c::c/126 only ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f (4 hosts in total). It does not cover host 2001:0D88:0800:200c::1f. Same for 2001:D88:800:200c::e/126, which also ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f and does not cover host 2001:0D88:0800:200c::1c.

NEW QUESTION 263

- (Exam Topic 1)

Refer to the exhibit.

```
ip dhcp pool 1
network 200.30.30.0/24
default-router 200.30.30.100
lease 40
!
ip dhcp pool 2
network 200.30.40.0/24
default-router 200.30.40.100
lease 40
!
```

The server for the finance department is not reachable consistently on the 200.30.40.0/24 network and after every second month it gets a new IP address. Which two actions must be taken to resolve this Issue? (Choose two.)

- A. Configure the server to use DHCP on the network with default gateway 200 30.40.100.
- B. Configure the server with a static IP address and default gateway.
- C. Configure the router to exclude a server IP address.
- D. Configure the server to use DHCP on the network with default gateway 200 30.30.100.
- E. Configure the router to exclude a server IP address and default gateway.

Answer: BC

NEW QUESTION 268

- (Exam Topic 1)

Refer to the exhibit.

```
R1#show policy-map control-plane
Control Plane
  Service-policy input: CoPP-BGP
  Class-map: BGP (match all)
    2716 packets, 172071 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: access-group name BGP
  drop

  Class-map: class-default (match-any)
    5212 packets, 655966 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
```

What is the result of applying this configuration?

- A. The router can form BGP neighborships with any other device.
- B. The router cannot form BGP neighborships with any other device.
- C. The router cannot form BGP neighborships with any device that is matched by the access list named "BGP".
- D. The router can form BGP neighborships with any device that is matched by the access list named "BGP".

Answer: C

Explanation:

after bgp session are UP.I configured the CoPP to drop 10.3.3.3 bgp traffic (R3). R3 bgp traffic that matched the ACL 100 is dropped and the state is in IDLE

```
access-list 100 permit tcp host 10.3.3.3 any eq bgp
access-list 100 permit tcp host 10.3.3.3 eq bgp any
!
class-map match-all class-bgp match access-group 100
!
policy-map policy-bgp class class-bgp
drop
!
control-plane
service-policy input policy-bgp
```

! The 10.3.3.3 neighbor goes to IDLE

NEW QUESTION 272

- (Exam Topic 1)

Refer to the exhibit.

```
R1#show policy-map control-plane
Control Plane
Class-map: NMS (match-all)
500461 packets, 24038351 bytes
5 minute offered rate 1390000 bps, drop rate 0 bps
police:
  cir 50000 bps, bc 5000 bytes
conformed 50444 packets, 24031001 bytes; actions:
transmit
exceeded 990012 packets, 94030134 bytes; actions
drop conformed 4000 bps, exceed 0 bps
R1#
```

A company is evaluating multiple network management system tools. Trending graphs generated by SNMP data are returned by the NMS and appear to have multiple gaps. While troubleshooting the issue, an engineer noticed the relevant output. What solves the gaps in the graphs?

- A. Remove the exceed-rate command in the class map.
- B. Remove the class map NMS from being part of control plane policing.
- C. Configure the CIR rate to a lower value that accommodates all the NMS tools
- D. Separate the NMS class map in multiple class maps based on the specific protocols with appropriate CoPP actions

Answer: D

Explanation:

Reference: https://tools.cisco.com/security/center/resources/copp_best_practices

The class-map NMS in the exhibit did not classify traffic into specific protocols so many packets were dropped. We should create some class-map to classify the receiving traffic. It is also a recommendation of CoPP/ CPP policy:

“Developing a CPP policy starts with the classification of the control plane traffic. To that end, the control plane traffic needs to be first identified and separated into different class maps.”

NEW QUESTION 275

- (Exam Topic 1)

What is an advantage of using BFD?

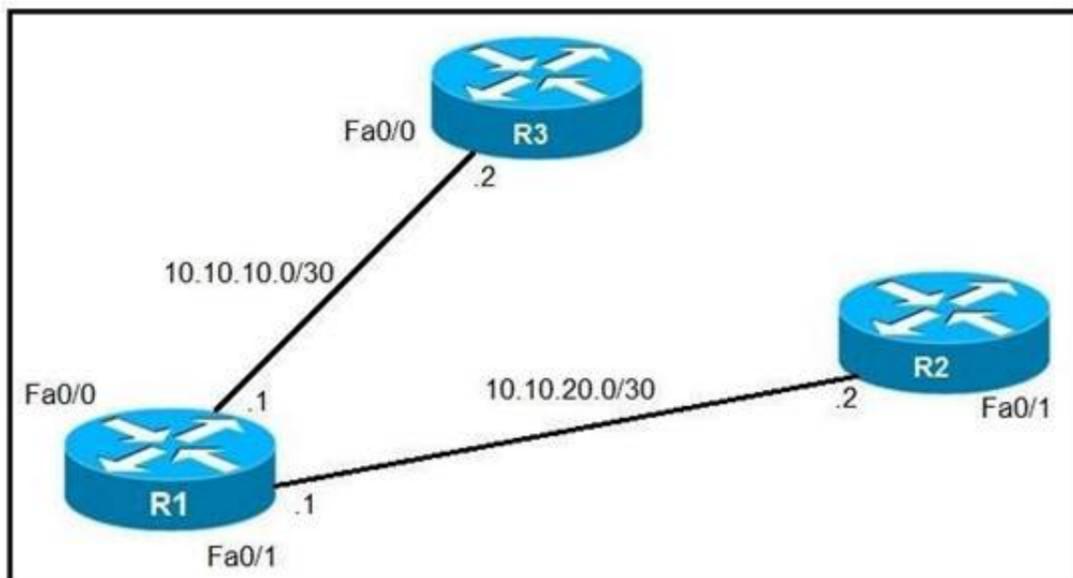
- A. It detects local link failure at layer 1 and updates routing table.
- B. It detects local link failure at layer 2 and updates routing protocols.
- C. It has sub-second failure detection for layer 1 and layer 3 problems.
- D. It has sub-second failure detection for layer 1 and layer 2 problems.

Answer: D

NEW QUESTION 279

- (Exam Topic 1)

Refer to the exhibit.



An IP SLA was configured on router R1 that allows the default route to be modified in the event that Fa0/0 loses reachability with the router R3 Fa0/0 interface. The route has changed to flow through router R2. Which debug command is used to troubleshoot this issue?

- A. debug ip flow
- B. debug ip sla error
- C. debug ip routing
- D. debug ip packet

Answer: C

Explanation:

debug ip routing This command enables debugging messages related to the routing table.

NEW QUESTION 282

- (Exam Topic 1)

An engineer is configuring a network and needs packets to be forwarded to an interface for any destination address that is not in the routing table. What should be configured to accomplish this task?

- A. set ip next-hop
- B. set ip default next-hop
- C. set ip next-hop recursive
- D. set ip next-hop verify-availability

Answer: B

Explanation:

The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

- if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.
- if the destination IP address **does not exist**, the command policy routes the packet by **sending it to the specified next hop**.

NEW QUESTION 286

- (Exam Topic 1)

Which protocol is used to determine the NBMA address on the other end of a tunnel when mGRE is used?

- A. NHRP
- B. IPsec
- C. MP-BGP
- D. OSPF

Answer: A

NEW QUESTION 290

- (Exam Topic 1)

While troubleshooting connectivity issues to a router, these details are noticed:

- Standard pings to all router interfaces, including loopbacks, are successful.
- Data traffic is unaffected.
- SNMP connectivity is intermittent.
- SSH is either slow or disconnects frequently.

Which command must be configured first to troubleshoot this issue?

- A. show policy-map control-plane
- B. show policy-map
- C. show interface | inc drop
- D. show ip route

Answer: A

NEW QUESTION 293

- (Exam Topic 1)

Refer to the exhibit.

```
Global RADIUS shared secret:*****
retransmission count:5
timeout value:10
following RADIUS servers are configured:
  myradius.cisco.users.com:
    available for authentication on port:1814
    available for accounting on port:1813
  10.1.1.1:
    available for authentication on port:1814
    available for accounting on port:1813
    RADIUS shared secret:*****
  10.2.2.3:
    available for authentication on port:1814
    available for accounting on port:1813
    RADIUS shared secret:*****
```

AAA server 10.1.1.1 is configured with the default authentication and accounting settings, but the switch cannot communicate with the server Which action resolves this issue?

- A. Match the authentication port
- B. Match the accounting port
- C. Correct the timeout value.
- D. Correct the shared secret.

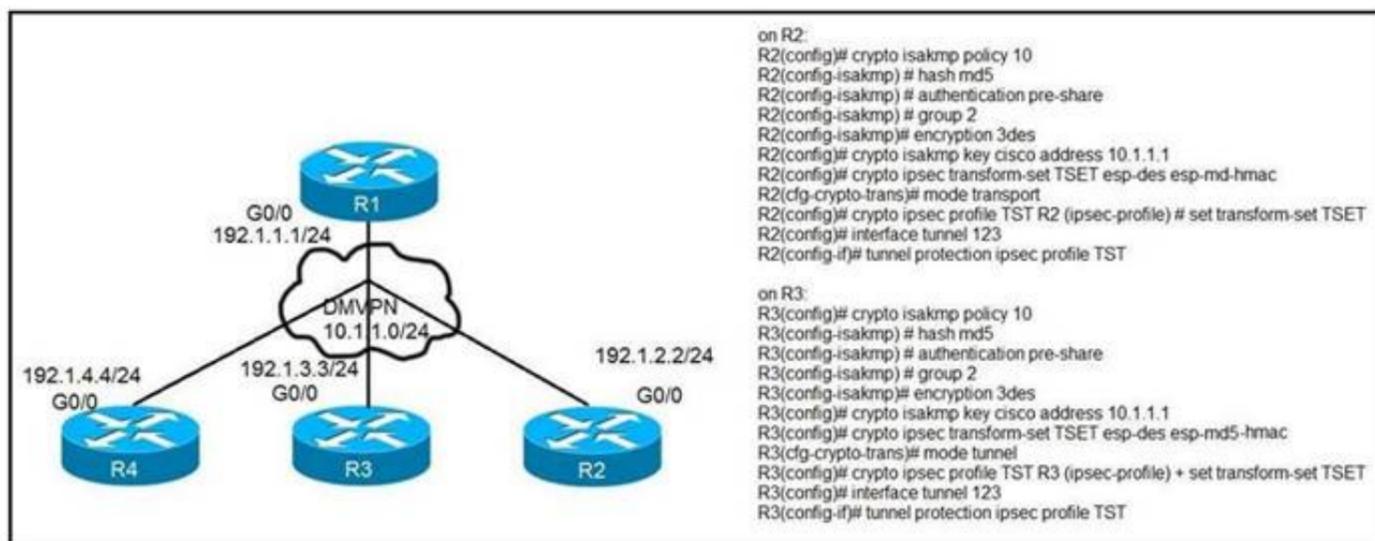
Answer: A

Explanation:

Command Default Accounting port: 1813
 Authentication port: 1812 Accounting: enabled Authentication: enabled Retransmission count: 1
 Idle-time: 0
 Server monitoring: disabled Timeout: 5 seconds
 Test username: test Test password: test Reference:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/radius-server-host.html By default, RADIUS uses UDP port 1812 for authentication and port 1813 for accounting. In the exhibit above we see port 1814 is being used for authentication to AAA server at 10.1.1.1 which is not the default port so we must adjust the authentication port to the default value 1812.

NEW QUESTION 298

- (Exam Topic 1)
Refer to the exhibit.



After applying IPsec, the engineer observed that the DMVPN tunnel went down, and both spoke-to-spoke and hub were not establishing. Which two actions resolve the issue? (Choose two.)

- A. Configure the crypto isakmp key cisco address 192.1.1.1 on R2 and R3
- B. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.
- C. Change the mode from mode tunnel to mode transport on R3
- D. Change the mode from mode transport to mode tunnel on R2.
- E. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3

Answer: AD

Explanation:

*When using DMVPN with IPsec, it is unnecessary to use tunnel mode. Because DMVPN uses GRE which means that a new IP header is already added by GRE. The GRE encapsulation happens on the tunnel interface before the encryption process takes place.

NEW QUESTION 301

- (Exam Topic 1)
Refer to the exhibit.

```

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

An engineer is trying to block the route to 192.168.2.2 from the routing table by using the configuration that is shown. The route is still present in the routing table as an OSPF route. Which action blocks the route?

- A. Use an extended access list instead of a standard access list.
- B. Change sequence 10 in the route-map command from permit to deny.
- C. Use a prefix list instead of an access list in the route map.
- D. Add this statement to the route map: route-map RM-OSPF-DL deny 20.

Answer: B

NEW QUESTION 303

- (Exam Topic 1)

Which two statements about redistributing EIGRP into OSPF are true? (Choose two)

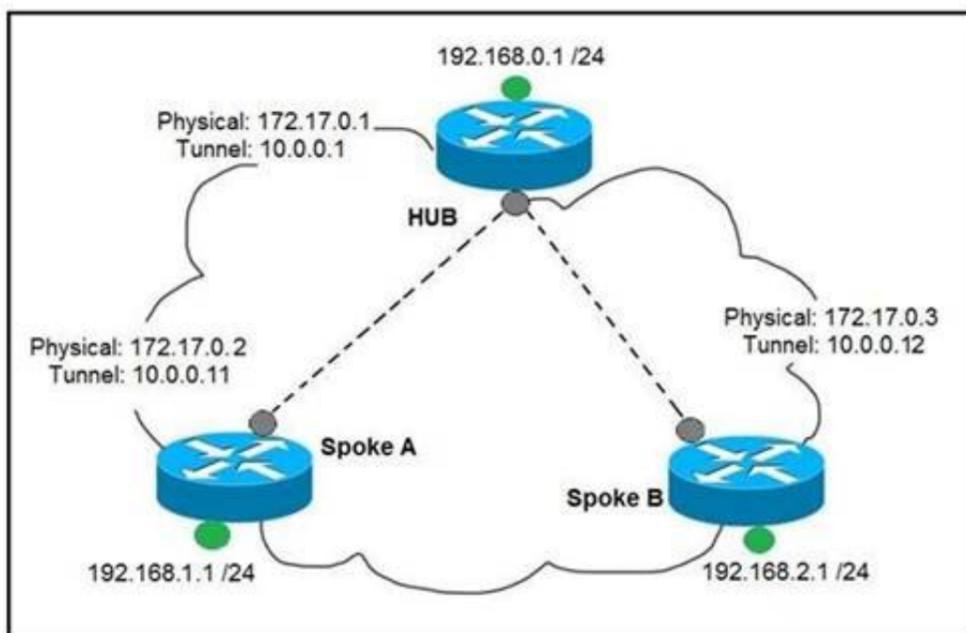
- A. The redistributed EIGRP routes appear as type 3 LSAs in the OSPF database
- B. The redistributed EIGRP routes appear as type 5 LSAs in the OSPF database
- C. The administrative distance of the redistributed routes is 170
- D. The redistributed EIGRP routes appear as OSPF external type 1
- E. The redistributed EIGRP routes as placed into an OSPF area whose area ID matches the EIGRP autonomous system number
- F. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table

Answer: BF

NEW QUESTION 306

- (Exam Topic 1)

Refer to the exhibit.



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

- A. interface Tunnel0
description mGRE – DMVPN Tunnel
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination FastEthernet 0/0
tunnel mode gre multipoint
- B. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1
- C. interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.11 172.17.0.2
tunnel mode gre
- D. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint

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

Answer: B

NEW QUESTION 307

- (Exam Topic 1)

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

- A. DMVPN
- B. MPLS VPN
- C. Virtual Tunnel Interface (VTI)
- D. SSL VPN
- E. PPPoE

Answer: AC

NEW QUESTION 308

- (Exam Topic 1)

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

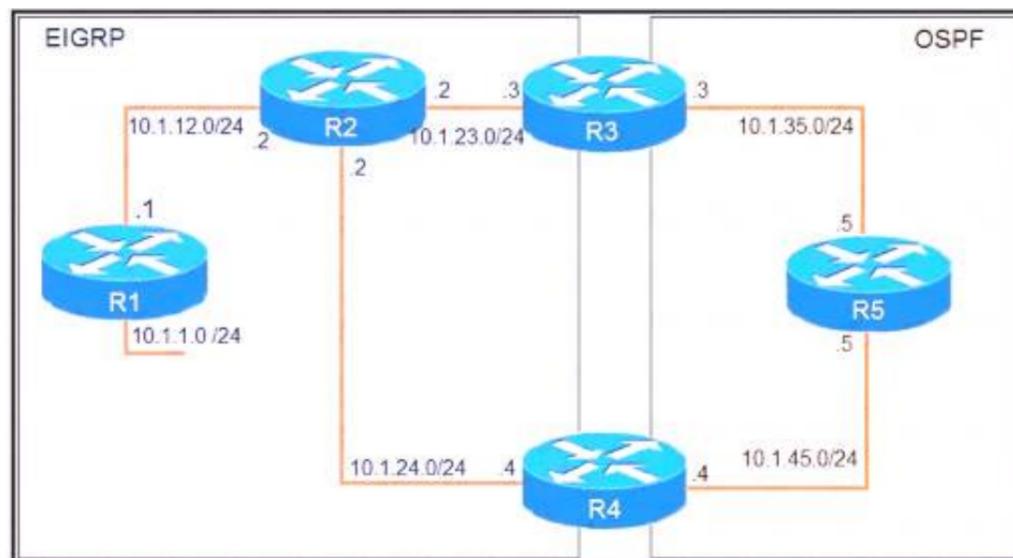
- A. Copy the file to the destination router with the copy tftp: flash: command
- B. Enable the TFTP server on the source router with the tftp-server flash: <filename> command
- C. TFTP is not supported in recent IOS versions, so an alternative method must be used
- D. Configure a user on the source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

Answer: AB

NEW QUESTION 311

- (Exam Topic 1)

Refer to the exhibit.



```

R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0

R3
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
 network 10.1.45.4 0.0.0.0 area 0

R5#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1 10.1.35.3 80 msec 44 msec 20 msec
 2 10.1.23.2 44 msec 104 msec 64 msec
 3 10.1.24.4 44 msec 64 msec 40 msec
 4 10.1.45.5 24 msec 40 msec 20 msec
 5 10.1.35.3 92 msec 144 msec 148 msec
 6 10.1.23.2 108 msec 76 msec 80 msec
 <output truncated>
    
```

The output of the trace route from R5 shows a loop in the network. Which configuration prevents this loop?

- A)


```

R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
      
```
- B)


```

R3
router eigrp 1
 redistribute OSPF 1 route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
 network 10.1.24.4 0.0.0.0
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
      
```

C)

```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1
```

```
R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG permit 10
 match tag 1
```

```
D)
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG deny 10
 set tag 1
```

```
R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
```

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

Answer: A

Explanation:

The reason for the loop is that R2 is forwarding the packets destined to 10.1.1.1 to R4, instead of R1. This is because in the redistribute OSPF statement, BW metric has a higher value and delay has a value of 1. So, R2 chooses R4 over R1 for 10.1.1.0/24 subnet causing a loop. Now, R5 learns 10.1.1.0/24 from R3 and advertises the same route to R4, that R4 redistributes back in EIGRP. If R3 sets a tag of 1 while redistributing EIGRP in OSPF, and R4 denies all the OSPF routes with tag 1 while redistributing, it will not advertise 10.1.1.0/24 back into EIGRP. Hence, the loop will be broken.

NEW QUESTION 314

- (Exam Topic 1)

Refer to the exhibit.

```
!
neighbor 10.222.1.1 route-map SET-WEIGHT in
neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map SET-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight 200
```

A router receiving BGP routing updates from multiple neighbors for routers in AS 690. What is the reason that the router still sends traffic that is destined to AS 690 to a neighbor other than 10.222.1.1?

- A. The local preference value in another neighbor statement is higher than 250.
- B. The local preference value should be set to the same value as the weight in the route map.
- C. The route map is applied in the wrong direction.
- D. The weight value in another neighbor statement is higher than 200.

Answer: C

NEW QUESTION 318

- (Exam Topic 1)

R2 has a locally originated prefix 192.168.130.0/24 and has these configurations:

```
ip prefix-list test seq 5 permit 192.168.130.0/24
```

```
!
```

```
route-map OUT permit10
```

```
match ip address prefix-list test
```

```
set as-path prepend 65000
```

What is the result when the route-map OUT command is applied toward an eBGP neighbor R1 (1.1.1.1) by using the neighbor 1.1.1.1 route-map OUT out command?

- A. R1 sees 192.168.130.0/24 as two AS hops away instead of one AS hop away.
- B. R1 does not accept any routes other than 192.168.130.0/24
- C. R1 does not forward traffic that is destined for 192.168.30.0/24
- D. Network 192.168.130.0/24 is not allowed in the R1 table

Answer: A

NEW QUESTION 319

- (Exam Topic 1)

Refer the exhibit.

```
R3#show policy-map control-plane
Control Plane

Service-policy output: R3_CoPP

Class-map: mgmt (match-all)
 361 packets, 73858 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: access-group 120
  police:
   cir 8000 bps, bc 1500 bytes, be 1500 bytes
   conformed 8 packets, 1506 bytes; actions:
    transmit
   exceeded 353 packets, 72352 bytes; actions:
    drop
   violated 0 packets, 0 bytes; actions:
    drop
   conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any)
 124 packets, 10635 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: any
R3#show access-lists 120
Extended IP access list 120
 10 permit udp any any eq snmptrap (361 matches)
```

Which action resolves intermittent connectivity observed with the SNMP trap packets?

- A. Decrease the committed burst Size of the mgmt class map
- B. Increase the CIR of the mgmt class map
- C. Add a new class map to match TCP traffic
- D. Add one new entry in the ACL 120 to permit the UDP port 161

Answer: B

NEW QUESTION 321

- (Exam Topic 1)

Refer to the exhibit.

```

Router Configuration:

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

```

The network administrator configured VRF lite for customer A. The technician at the remote site misconfigured VRF on the router. Which configuration will resolve connectivity for both sites of customer_a?

- ip vrf customer_a
rd 1:1
route-target export 1:2
route-target import 1:2
- ip vrf customer_a
rd 1:1
route-target import 1:1
route-target export 1:2
- ip vrf customer_a
rd 1:2
route-target both 1:2
- ip vrf customer_a
rd 1:2
route-target both 1:1

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

Answer: D

Explanation:

From the exhibit, we learned:

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

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

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

NEW QUESTION 323

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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