

➤ **Vendor: Cisco**➤ **Exam Code: 2V0-71.21**➤ **Exam Name: Professional VMware Application Modernization**➤ **New Updated Questions from [Braindump2go](#) (Updated in [April/2022](#))****Visit Braindump2go and Download Full Version 2V0-71.21 Exam Dumps****QUESTION 309**

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

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

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

Answer: B**QUESTION 310**

Refer to the exhibit. Router R2 should be learning the route for 10.123.187.0/24 via EIGRP. Which action resolves the issue without introducing more issues?

```
R2#show ip route
```

```
Gateway of last resort is not set
 10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
C    10.1.3.0/30 is directly connected, FastEthernet0/1
C    10.1.2.0/30 is directly connected, FastEthernet0/0
C    10.1.1.0/30 is directly connected, FastEthernet1/0
O E2 10.19.0.0/24 [110/20] via 10.1.3.2, 00:02:04, FastEthernet0/1
D    10.55.13.0/24 (90/4096001 via 10.1.2.2. 00:01:00. FastEthernet0/0
D    10.37.100. 0/24 (90/4096001 via 10.1.2.2. 00:01:00. FastEthernet0/0
C    10.100.10.0/29 is directly connected, FastEthernet2/0.10
D    10.55.72.0/24 (90/409600] via 10.1.2.2. 00:01:01. FastEthernet0/0
C    10.100.20.0/29 is directly connected. FastEthernet2/0.20
O E2 10.144.1.0/24 /110/201 via 10.1.3.2. 00:12:51. FastEthernet0/1
D    10.55.144.0/24 (90/4096001 via 10.1.2.2. 00:01:01. FastEthernet0/0
O E2 10.123.187.0/24 [110/20] via 10.1.3.2. 00:12:51, FastEthernet0/1
```

```
R2#sh ip eigrp topology
```

```
IP-EIGRP Topology Table for AS(100)/ID(10.100.20.2)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r- reply Status, s - sia Status
P 10.1.3.0/30, 1 successors, FD is 281600 via Connected, FastEthernet0/1
P 10.1.2.0/30, 1 successors, FD is 281600 via Connected, FastEthernet0/0
P 10.1.1.0/30, 1 successors, FD is 28160 via Connected, FastEthernet1/0
P 10.55.13.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.37.100.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.55.72.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.55.144.0/24, 1 successors, FD is 409600 via 10.1.2.2 (409600/128256), FastEthernet0/0
P 10.123.187.0/24, 0 successors, FD is Inaccessible via 10.1.2.2 (409600/128256), FastEthernet0/0
```

- A. Use distribute-list to modify the route as an internal EIGRP route
- B. Redistribute the route in EIGRP with metric, delay, and reliability
- C. Use distribute-list to filter the external router in OSPF
- D. Remove route redistribution in R2 for this route in OSPF

Answer: C

QUESTION 311

An engineer configured a router with this configuration:

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

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

The router console starts receiving log message:

```
%SEC-6-IPACCESSLOGP: list DENY_TELNET denied tcp 192.168.1.10(1022)(FastEthernet1/0 D508.89gb.003f)
->192.168.2.20(23), 1 packet"
```

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

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

Answer: B

QUESTION 312

Refer to the exhibit. 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)

```
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
```

- 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

QUESTION 313

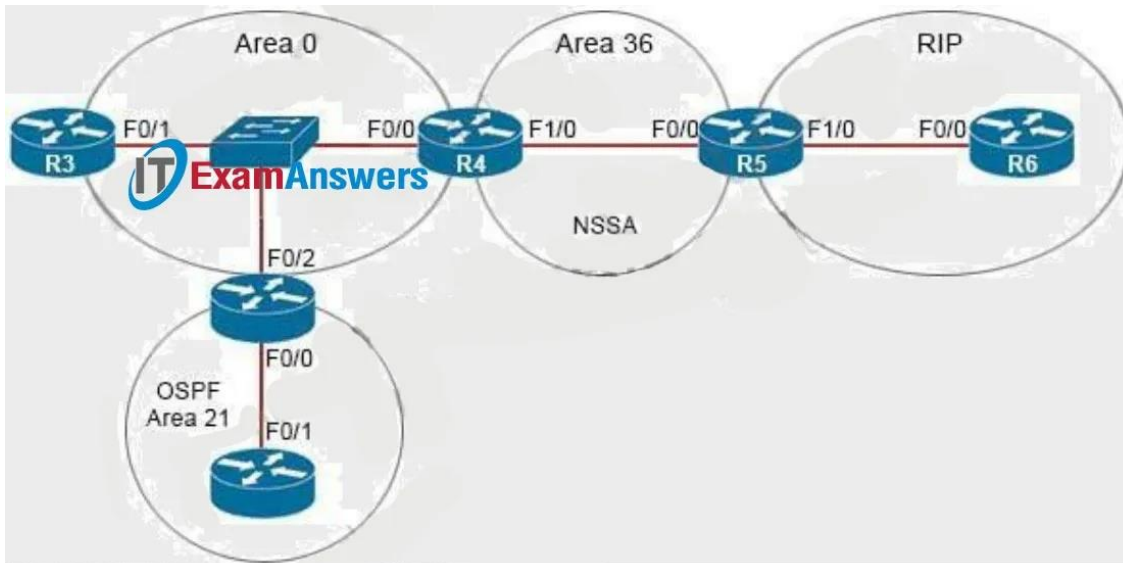
Which IPv6 first hop security feature controls the traffic necessary for proper discovery of neighbor device operation and performance?

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

Answer: D

QUESTION 314

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



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

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

Answer: A

Explanation:

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

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

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

QUESTION 315

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

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

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

Answer: C

QUESTION 316

A customer requested a GRE tunnel through the provider network between two customer sites using loopback to hide internal networks.

Which configuration on R2 establishes the tunnel with R1?

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

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

Answer: D

QUESTION 317

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

QUESTION 318

Which IPv6 feature enables a device to reject traffic when it is originated from an address that is not stored in the device binding table?

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

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xr-3s/ip6f-xr-3s-book/ip6-src-guard.html

QUESTION 319

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

```
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#
```

- 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 1
R1(config-router)# distance eigrp 130 120
- D. R1(config)# router eigrp 1
R1(config-router)# distance eigrp 120 120

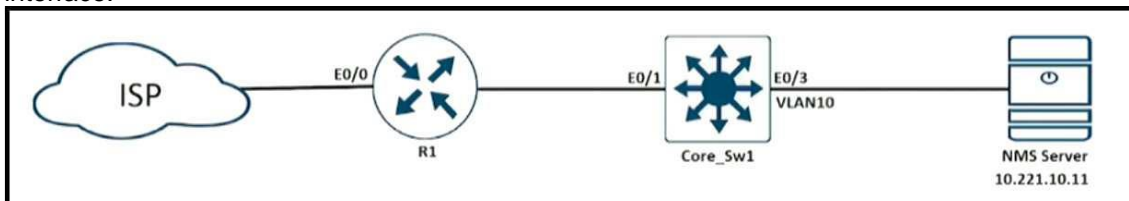
Answer: C

Explanation:

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

QUESTION 320

Refer to the exhibit. During ISP router maintenance, the network produced many alerts because of the flapping interface.



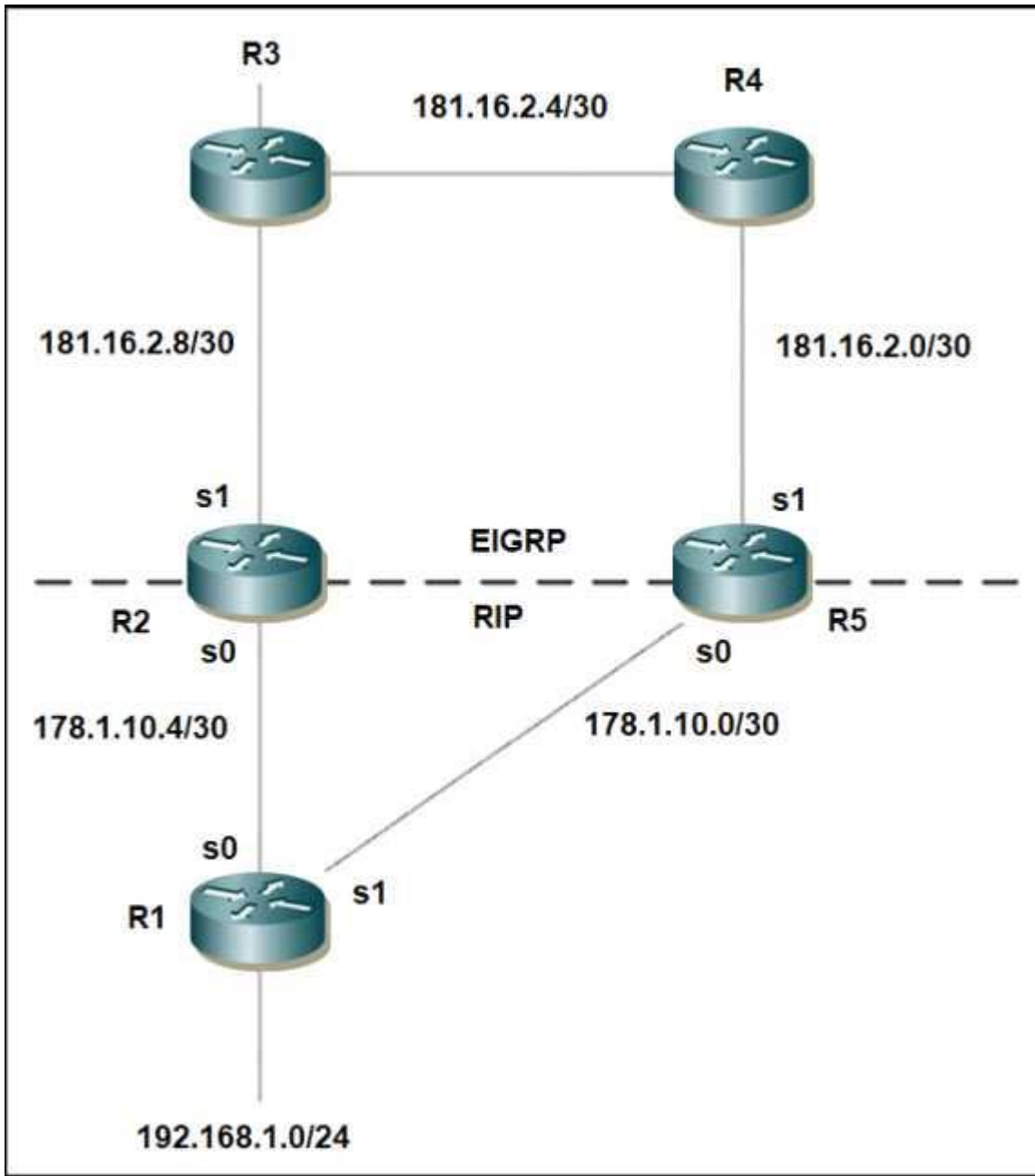
Which configuration on R1 resolves the issue?

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

Answer: A

QUESTION 321

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



A. R2:

```

router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

```

R5:

```

router eigrp 10
network 181.16.0.0

```


redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0

!

router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

B. R2:

router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0

!

router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

R5:

router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0

!

router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

C. R2:

router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s0

!

router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

R5:

router eigrp 10
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1

!

router rip
network 178.1.0.0
redistribute eigrp 10 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

D. R2:

```

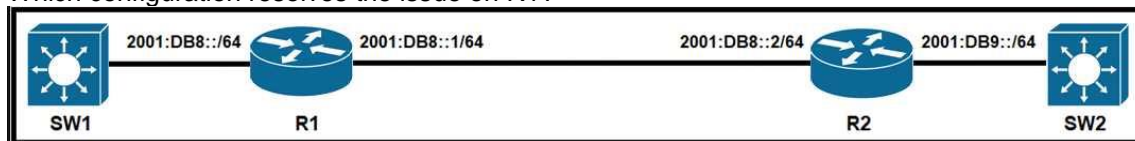
router eigrp 7
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 7 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any
R5:
router eigrp 7
network 181.16.0.0
redistribute rip metric 1 1 1 1 1
distribute-list 1 in s1
!
router rip
network 178.1.0.0
redistribute eigrp 7 metric 2
!
access-list 1 deny 192.168.1.0
access-list 1 permit any

```

Answer: C

QUESTION 322

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



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

Answer: B

QUESTION 323

An engineer failed to run diagnostic commands on devices using Cisco DNA Center. Which action in Cisco DNA Center resolves the issue?

- A. Enable Command Runner
- B. Enable APIs
- C. Enable CDP
- D. Enable Secure Shell

Answer: A

QUESTION 324

Which two solutions are used to overcome a flapping link that causes a frequent label binding exchange between MPLS routers? (Choose two)

- A. Create link dampening on links to protect the session.
- B. Increase input queue on links to protect the session.
- C. Create targeted hellos to protect the session.
- D. Increase a hold-timer to protect the session.
- E. Increase a session delay to protect the session.

Answer: AC

Explanation:

To avoid having to rebuild the LDP session altogether, you can protect it. When the LDP session between two directly connected LSRs is protected, a targeted LDP session is built between the two LSRs. When the directly connected link does go down between the two LSRs, the targeted LDP session is kept up as long as an alternative path exists between the two LSRs. For the protection to work, you need to enable it on both the LSRs. If this is not possible, you can enable it on one LSR, and the other LSR can accept the targeted LDP Hellos by configuring the command `mpls ldp discovery targeted-hello accept`.

Reference:

<https://www.ccexpert.us/mppls-network/mppls-ldp-session-protection.html>

<https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/5eU6DfQV/TECMPL-3201.pdf>

Troubleshooting LDP Issues

Problem:

I. When a link flaps (for a short time),

...

Solution:

+ When LDP session supported by link hello is setup, create a targeted hello to protect the session.

QUESTION 325

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



- A. `crypto isakmp policy 5`
`authentication pre-share`
`encryption 3des`
`hash sha`
`group 2`
`!`
`crypto isakmp key cisco123 address 200.1.1.3`
- B. `crypto isakmp policy 5`
`authentication pre-share`
`encryption 3des`
`hash md5`
`group 2`

[2V0-71.21 Exam Dumps](#) [2V0-71.21 Exam Questions](#) [2V0-71.21 PDF Dumps](#) [2V0-71.21 VCE Dumps](#)

<https://www.braindump2go.com/2v0-71-21.html>

- !
- crypto isakmp key cisco123 address 200.1.1.3
- C. crypto isakmp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
- crypto isakmp key cisco123 address 199.1.1.1
- D. crypto isakmp policy 5
authentication pre-share
encryption 3des
hash md5
group 2
!
- crypto isakmp key cisco123! address 199.1.1.1

Answer: A

Explanation:

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

QUESTION 326

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.

QUESTION 327

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

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

Answer: CD

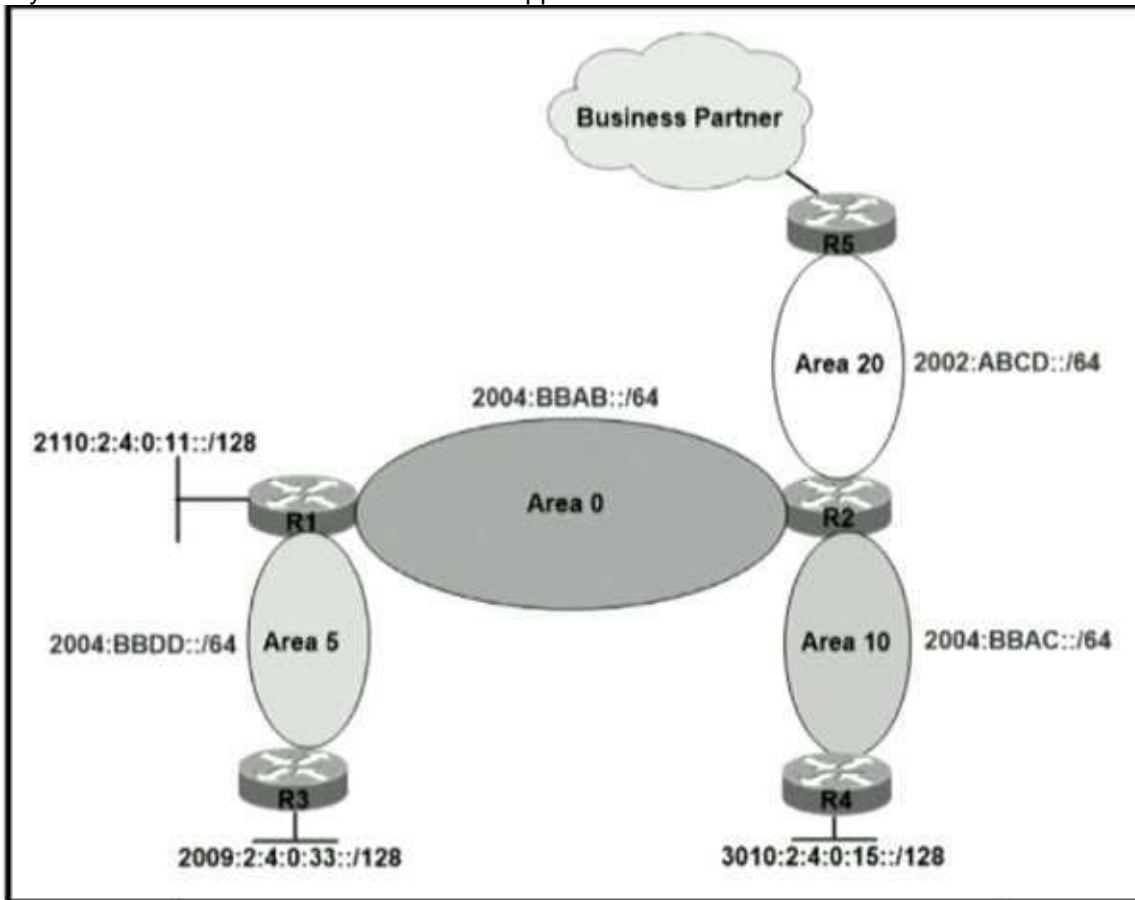
QUESTION 328

Refer to the exhibit. A network engineer applied a filter for LSA traffic on OSPFv3 interarea routes on the area 5 ABR to

[2V0-71.21 Exam Dumps](#) [2V0-71.21 Exam Questions](#) [2V0-71.21 PDF Dumps](#) [2V0-71.21 VCE Dumps](#)

<https://www.braindump2go.com/2v0-71-21.html>

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?



```

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. 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

QUESTION 329

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


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

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

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

Answer: C

QUESTION 330

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

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

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

Answer: D

QUESTION 331

Refer to the exhibit. The control plane is heavily impacted after the CoPP configuration is applied to the router. Which

[2V0-71.21 Exam Dumps](#) [2V0-71.21 Exam Questions](#) [2V0-71.21 PDF Dumps](#) [2V0-71.21 VCE Dumps](#)

<https://www.braindump2go.com/2v0-71-21.html>

command removal lessens the impact on the control plane?

```
!-- ACL for CoPP Routing class-map  
!
```

```
access-list 120 permit tcp any gt 1024 eq bgp log  
access-list 120 permit tcp any bgp gt 1024 established  
access-list 120 permit tcp any gt 1024 eq 639  
access-list 120 permit tcp any eq 639 gt 1024 established  
access-list 120 permit tcp any eq 646  
access-list 120 permit udp any eq 646  
access-list 120 permit ospf any  
access-list 120 permit ospf any host 224.0.0.5  
access-list 120 permit ospf any host 224.0.0.6  
access-list 120 permit eigrp any  
access-list 120 permit eigrp any host 224.0.0.10  
access-list 120 permit udp any any eq pim-auto-rp
```

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

Answer: A

QUESTION 332

Refer to the exhibit. 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?

```
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
```

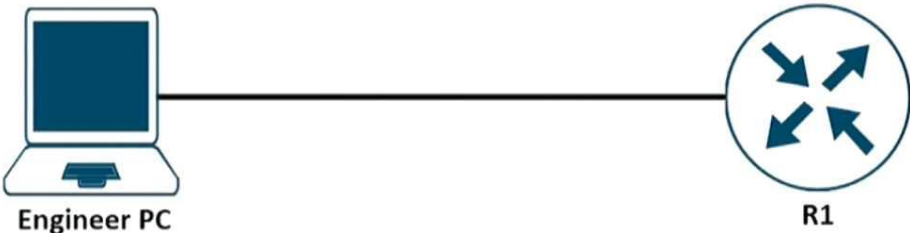
- A. Configure IOS control plane protection using ACL 90 on interface E1/0
- B. Configure IOS management plane protection using ACL 90 on interface E1/0
- C. Create an inbound ACL on interface E1/0 to deny SNMP from host 10.11.110.12
- D. Add a permit statement including the host 10.11.110.12 into ACL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

Answer: C

QUESTION 333

Refer to the exhibit. An engineer is trying to add an encrypted user password that should not be visible in the router configuration.

Which two configuration commands resolve the issue? (Choose two)



```
R1(config)#username Admin password 7 Cisco@123
Invalid encrypted password: Cisco@123
```

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

Answer: DF

QUESTION 334

Refer to the exhibit. Which action restores OSPF adjacency between R1 and R2?

```
R2#show running-config | section ospf
ip ospf 1 area 1
ip ospf 1 area 1
router ospf 1
 log-adjacency-changes
 area 1 stub no-summary
R2#show ip ospf interface brief
Interface  PID  Area  IP Address/Mask  Cost  State  Nbrs  F/C
Lo0        1    1    10.0.0.2/32      1     Loop  0/0
Fa0/0      1    1    10.10.10.1/30    1     DR    0/1

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

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

R2#show ip ospf neighbor
```

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

```
R1#show running-config | section ospf
ip ospf 1 area 0
ip ospf 1 area 1
router ospf 1
 log-adjacency-changes
 area 1 stub no-summary
R1#show ip ospf interface brief
Interface  PID  Area  IP Address/Mask  Cost  State  Nbrs  F/C
Lo0        1    0    10.0.0.1/32      1     LOOP  0/0
Lo0        1    1    10.10.10.2/30    1     BDR    0/1

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

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

R1#show ip ospf neighbor
```

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

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

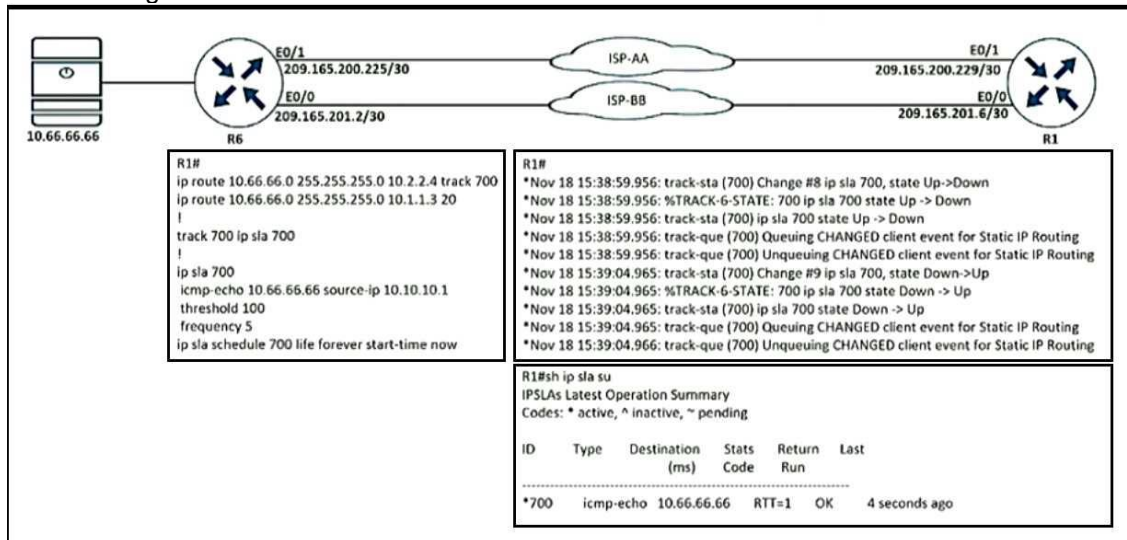
Answer: D

QUESTION 335

[2V0-71.21 Exam Dumps](#)
[2V0-71.21 Exam Questions](#)
[2V0-71.21 PDF Dumps](#)
[2V0-71.21 VCE Dumps](#)

<https://www.braindump2go.com/2v0-71-21.html>

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?

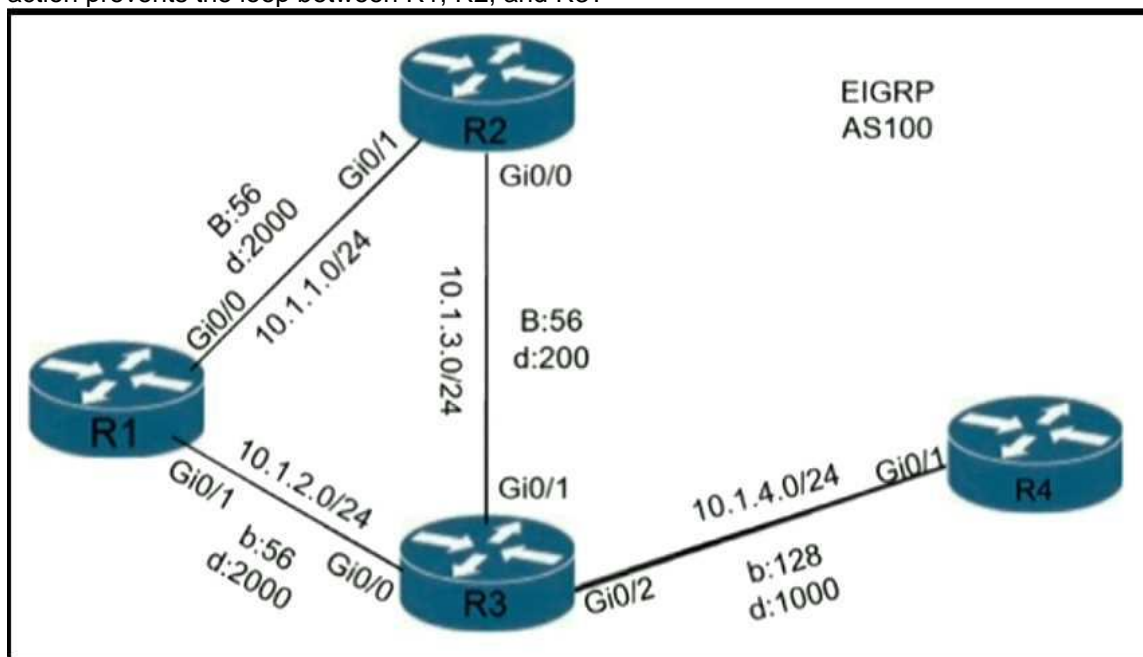


- A. R1(config)# ip sla 700
R1(config-track)# delay down 30 up 20
- B. R1(config)# ip sla 700
R1(config-track)# delay down 20 up 30
- C. R1(config)# track 700 ip sla 700
R1(config-track)# delay down 30 up 20
- D. R1(config)# track 700 ip sla 700
R1(config-track)# delay down 20 up 30

Answer: C

QUESTION 336

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



- A. Configure route tagging

[2V0-71.21 Exam Dumps](#) [2V0-71.21 Exam Questions](#) [2V0-71.21 PDF Dumps](#) [2V0-71.21 VCE Dumps](#)

<https://www.braindump2go.com/2v0-71-21.html>

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

Answer: C