300-410Q&As

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) (Include 2023 Newest Simulation Labs)

Pass Cisco 300-410 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

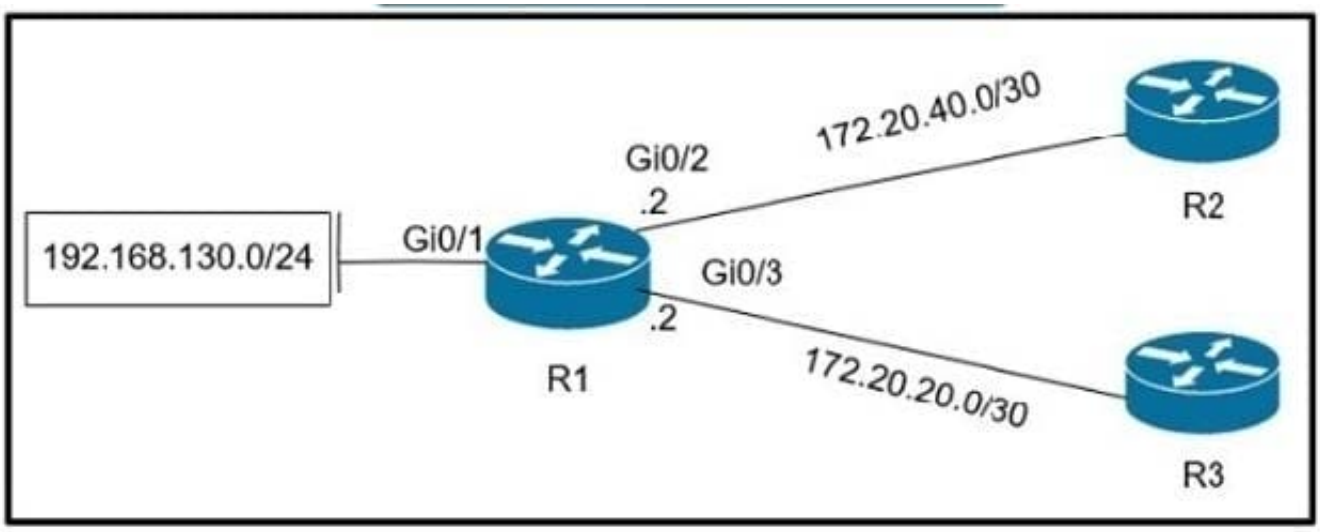
https://www.passapply.com/300-410.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit.



Which policy configuration on R1 forwards any traffic that is sourced from the 192 168 130 0\\'24 network to R2?

A.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.2
```

B.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.1
```

C.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.1
```

D.
```
access-list 1 permit 192.168.130.0 0.0.0.255
!
interface Gi0/1
ip policy route map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2
```

A. Option A

B. Option B

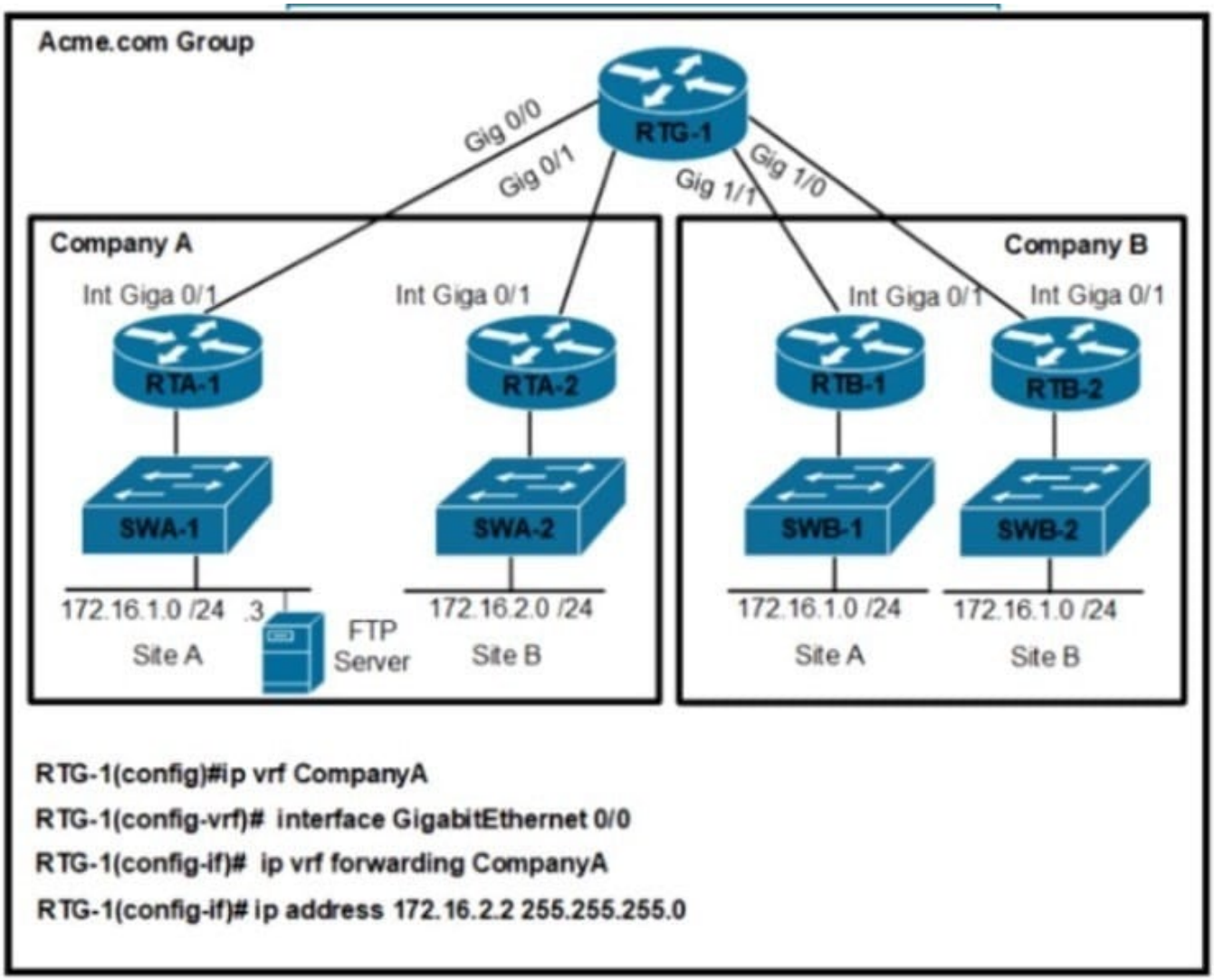
C. Option C

D. Option D

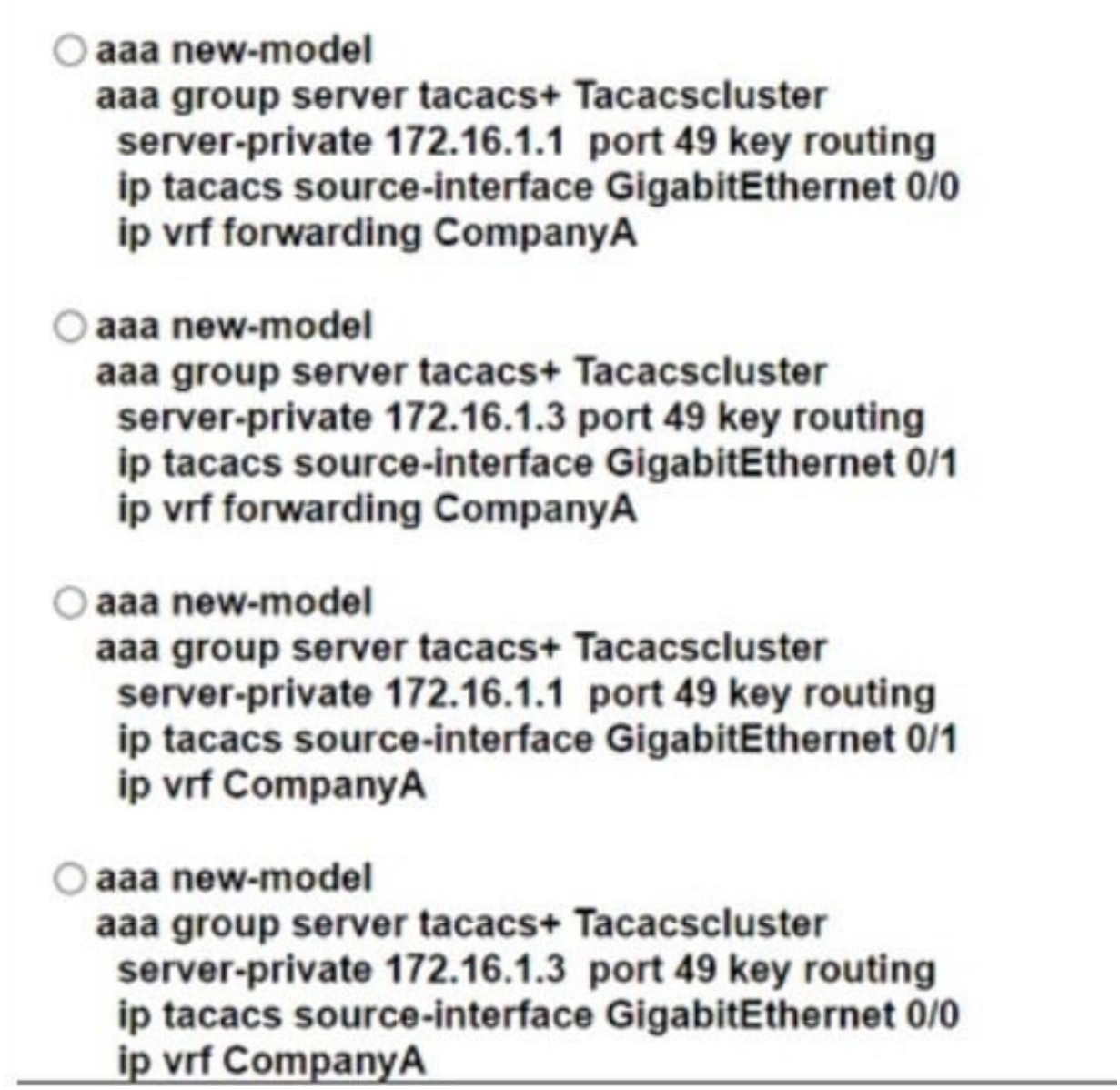
Correct Answer: C

QUESTION 2

Refer to the exhibit.



An engineer must configure a per VRF for TACACS+ for company A. Which configuration on RTG-1 accomplishes the task?



A. Option A

B. Option B

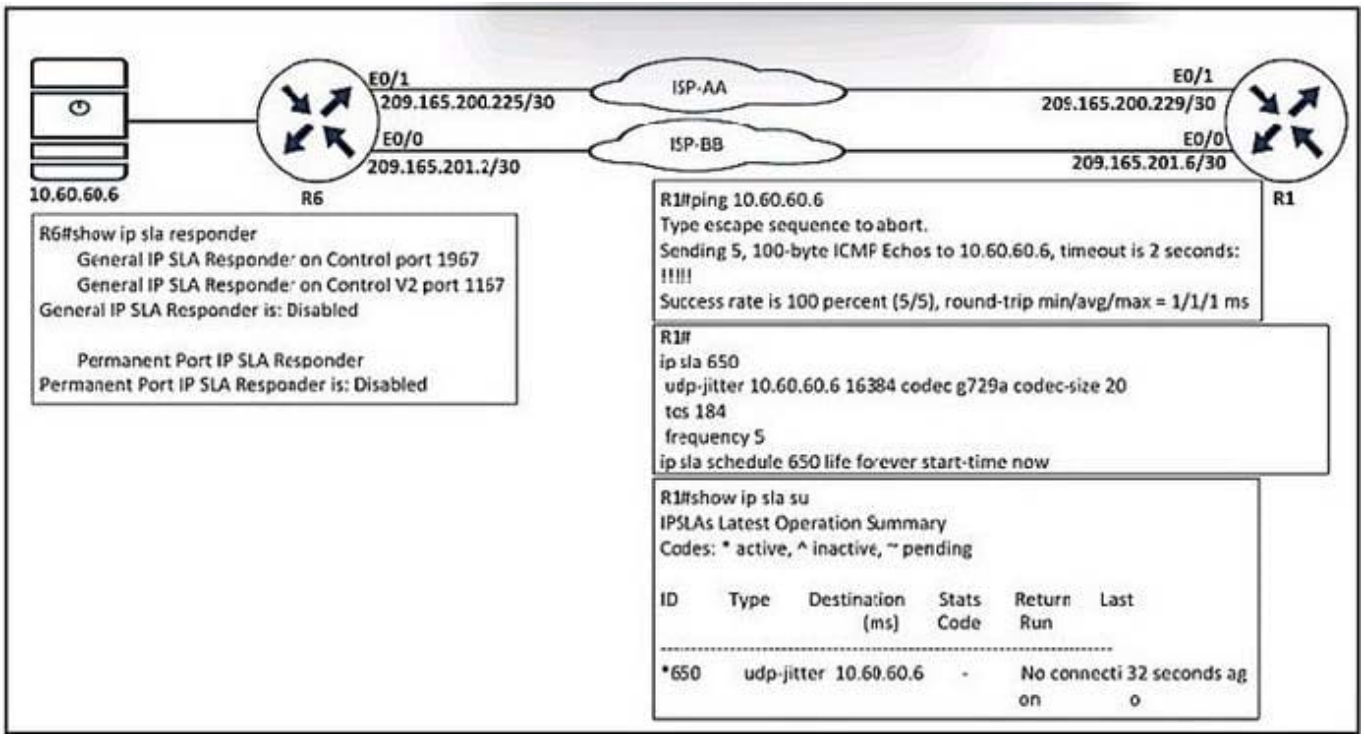
C. Option C

D. Option D

Correct Answer: D

QUESTION 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

Correct Answer: A

QUESTION 4

Which command can you use to display information about OSPF virtual links?

A. debug ip ospf adj

B. show ip ospf [process-id]

C. show ip ospf virtual-links

D. show ip ospf border-routers

Correct Answer: C

The correct answer is show ip ospf virtual-links. The show ip ospf virtual-links command displays the current state of OSPF virtual links, as shown below.

```
Router10# show ip ospf virtual-links
Virtual Link to router 192.168.15.7 is up
Transit area 0.0.0.1, via interface Ethernet1, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

The following additional commands are available to verify OSPF configurations: show ip ospf border-routers, debug ip ospf adj, and show ip ospf.

The show ip ospf border-routers command displays internal OSPF routing table entries for an ABR, as shown below.

router10#show ip ospf border-routers

Codes: i - Intra-area route, I-Inter-area route

Type Dest Address Cost NextHop Interface ABR ASBR Area SPF

i 2.2.2.2 10 192.1.1.199 Ethernet 2 TRUE FALSE 0 3 i 3.2.2.2 10 192.1.1.200 Ethernet 2 TRUE FALSE 0 3 The show ip ospf command displays information about the router\\'s role and each area to which the router is connected, as shown below.

```
router10# show ip ospf
Routing Process "ospf 3" with ID 15.0.0.1 and Domain ID 15.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 100 secs
Interface flood pacing timer 55 msecs
Retransmission pacing timer 100 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 3
Area has message digest authentication
SPF algorithm executed 4 times
Area ranges are
Number of LSA 4. Checksum Sum 0x29BEB
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 3
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
Area 172.16.40.0
Number of interfaces in this area is 0
Area has no authentication
SPF algorithm executed 1 times
Area ranges are
192.168.0.0/16 Passive Advertise
Number of LSA 1. Checksum Sum 0x44FD
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 1
Number of indication LSA 1
Number of DoNotAge LSA 0
Flood list length 0
```

The debug ip ospf adj command displays information about the state of neighbor adjacencies, as shown below.

R3#debug ip ospf adj OSPF adjacency events debugging is on

00:54:04: OSPF: Rcv pkt from 172.12.23.2, Ethernet0, area 0.0.0.1 : src not on the same network

In the above example, either the IP address or the subnet mask is misconfigured on either this router or the neighbor.

Objective:

Layer 3 Technologies

Sub-Objective:

Configure and verify network types, area types, and router types

References:

Cisco > Cisco IOS IP Routing Protocols Command Reference > IP Routing Protocol-Independent Commands:

S through T > show ip ospf virtual-links

QUESTION 5

Refer to the exhibit.


```
CSR103#sh ip ospf interface gigabitEthernet 2
GigabitEthernet2 is up, line protocol is up
  Internet Address 172.16.1.42/30, Interface ID 8, Area 1
  Attached via Network Statement
  Process ID 1, Router ID 172.16.100.7, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1          no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.100.7, Interface address 172.16.1.42
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Youngest key id is 1

CSR103#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.3      1   FULL/DR         00:00:34    172.16.1.25     GigabitEthernet3
172.16.100.5      1   FULL/BDR        00:00:20    172.16.1.41     GigabitEthernet2
CSR103#
CSR103#
*Jan 11 16:43:54.644: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.100.5 on GigabitEthernet2
from FULL to DOWN, Neighbor Down: Dead timer expired
```

Which configuration must the engineer apply on CSR103 to resolve the problem?

A.
```
key chain ospf
 key 1
  key-string 7 4A442D591C17
   cryptographic-algorithm hmac-sha-256
!
interface GigabitEthernet2
 ip ospf authentication key-chain ospf
```

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

C.
```
key chain ospf
 key 1
  key-string 7 02050D480809
   cryptographic-algorithm hmac-sha-1
!
int GigabitEthernet 2
 ip ospf message-digest-key 1 md5 cisco
 ip ospf authentication message-digest
```

D.
```
key chain ospf
 key 1
  key-string 7 02050D480809
   cryptographic-algorithm hmac-sha-256
!
router ospf 1
 area 1 authentication message-digest
!
int GigabitEthernet 2
 ip ospf message-digest-key 1 md5 cisco
```

A. Option A

B. Option B

C. Option C

D. Option D

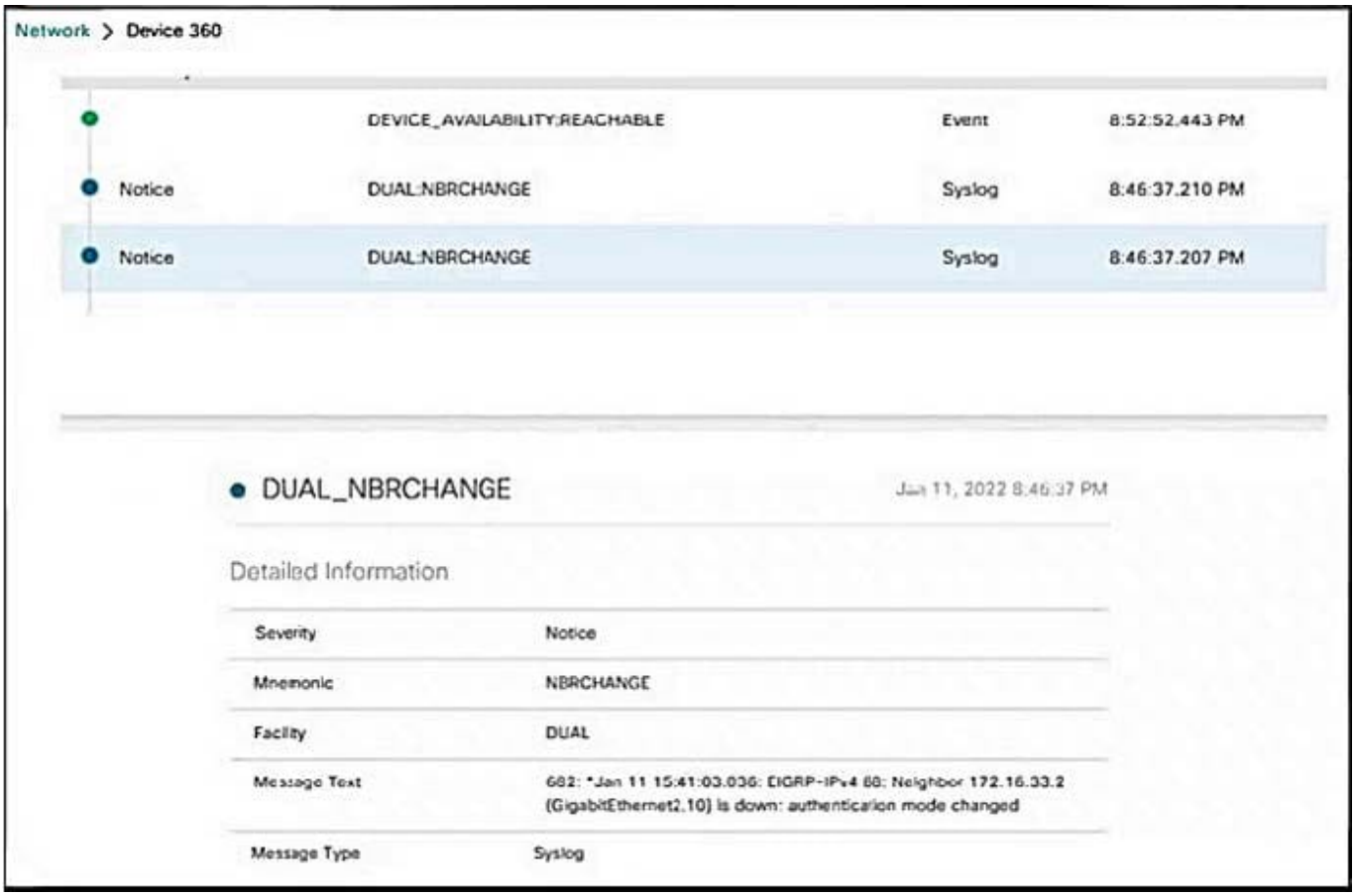
Correct Answer: C

md5 authentication

Message digest authentication enabled Youngest key id is 1 https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13697-25.html

QUESTION 6

Refer to the exhibit.



R1 lost its directly connected EIGRP peer 172.16.33.2 (SW1). Which configuration resolves the issue?

A.
```
key chain EIGRP
  key 1
    key-string Cisco
!
interface GigabitEthernet 2.10
  ip authentication mode eigrp 88 md5
  ip authentication key-chain eigrp 88 EIGRP
```

B.
```
key chain EIGRP
  key 1
    key-string Cisco
!
interface GigabitEthernet 2
  ip authentication mode eigrp 88 md5
  ip authentication key-chain eigrp 88 EIGRP
```

C.
```
key chain EIGRP
  key 1
    key-string Cisco
!
interface GigabitEthernet 2.10
  ip authentication mode eigrp 88 md5
  ip authentication key-chain eigrp 88 Cisco
```

D.
```
key chain EIGRP
  key 1
    key-string Cisco
!
interface GigabitEthernet 2
  ip authentication mode eigrp 88 md5
  ip authentication key-chain eigrp 88 Cisco
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/82110-eigrp-authentication.html

QUESTION 7

Refer to the exhibit.

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

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

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

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

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

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

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

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 8

You have configured DHCP on a router and configured it to assign IP addresses in the range of 192.168.1.10 through 192.168.1.150. You just discovered that one of your print servers is using the address 192.168.1.100 and you cannot change it.

What command can you use on the router to solve this problem?

A. Router(config)# ip dhcp excluded-address

B. Router(config)# access-list

C. Router(dhcp-config)# ip dhcp excluded-address

D. Router(config)# dhcp exclude-address

E. Router(config)# service dhcp excluded-address

Correct Answer: A

The ip dhcp excluded-address command will allow you to specify an address or group of addresses in a pool that the DHCP server will not assign. This is typically used when a host has a permanent address assigned that would conflict with

addresses that the DHCP server would hand out. The proper syntax for this command is as follows:

Router(config)# ip dhcp excluded-address low-address [high-address]

The other options use improper syntax or are executed at an incorrect prompt. The ip dhcp excluded-address command should be executed at global configuration mode.

Objective:

Infrastructure Services

Sub-Objective:

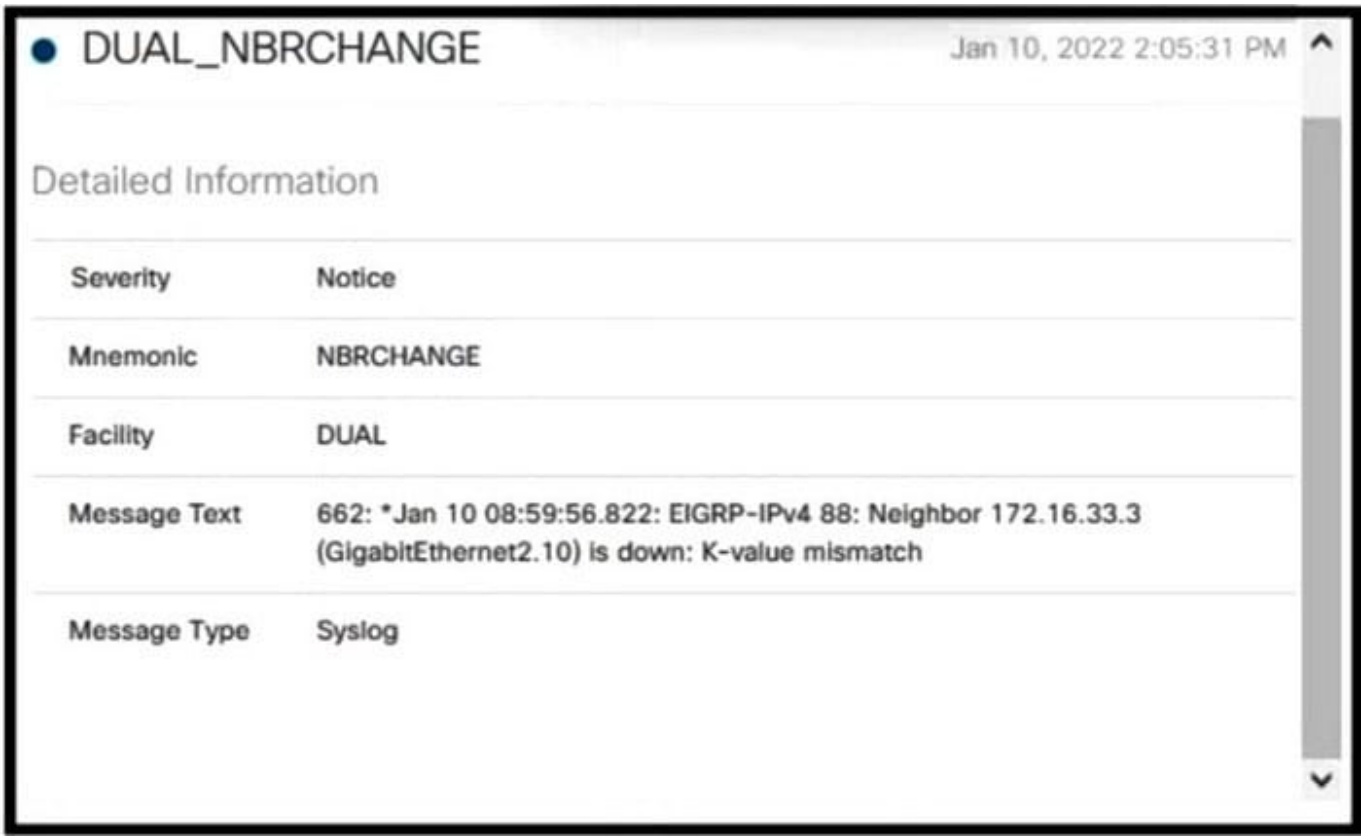
Configure and verify IPv4 and IPv6 DHCP

References:

Cisco > Cisco IOS IP Addressing Services Command Reference > ip dhcp excluded-address

QUESTION 9

Refer to the exhibit.



EIGRP peering was lost.

Which configuration resolves the issue?

A.
```
router EIGRP 88
 metric weights  1 0 1 0 10
```

B.
```
router EIGRP 88
 metric weights 1 1 1 0 0 0
```

C.
```
router EIGRP 88
 metric weights 0 1 1 0 01
```

D.
```
router EIGRP 88
 metric weights 0 1 1 1 0 0
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 10

Which feature minimizes DoS attacks on an IPv6 network?

A. IPv6 Binding Security Table

B. IPv6 Router Advertisement Guard

C. IPv6 Prefix Guard

D. IPv6 Destination Guard

Correct Answer: D

The Destination Guard feature helps in minimizing denial-of-service (DoS) attacks. It performs address resolutions only for those addresses that are active on the link, and requires the FHS binding table to be populated with the help of the IPv6 snooping feature.The feature enables the filtering of IPv6 traffic based on the destination address, and blocks the NDP resolution for destination addresses that are not found in the binding table. By default, the policy drops traffic coming for an unknown destination.

QUESTION 11

Which SNMP verification command shows the encryption and authentication protocols that are used in SNMPV3?

A. show snmp group

B. show snmp user

C. show snmp

D. show snmp view

Correct Answer: B

QUESTION 12

An engineer notices that R1 does not hold enough log messages to Identity the root cause during troubleshooting Which command resolves this issue?

A. #loggin buffered 4096 critical

B. (config)#logging buffered 16000 informational

C. #loggin buffered 16000 critical

D. (config)#logging buffered 4096 informational

Correct Answer: B

QUESTION 13

An engineer configured Reverse Path Forwarding on an interface and noticed that the routes are dropped when a route lookup fails on that interface for a prefix that is available in the routing table Which interface configuration resolves the issue?

A. ip verify unicast source reachable-via rx

B. ip verify unicast source reachable-via any

C. ip verify unicast source reachable-via allow-default

D. ip verify unicast source reachable-via 12-src

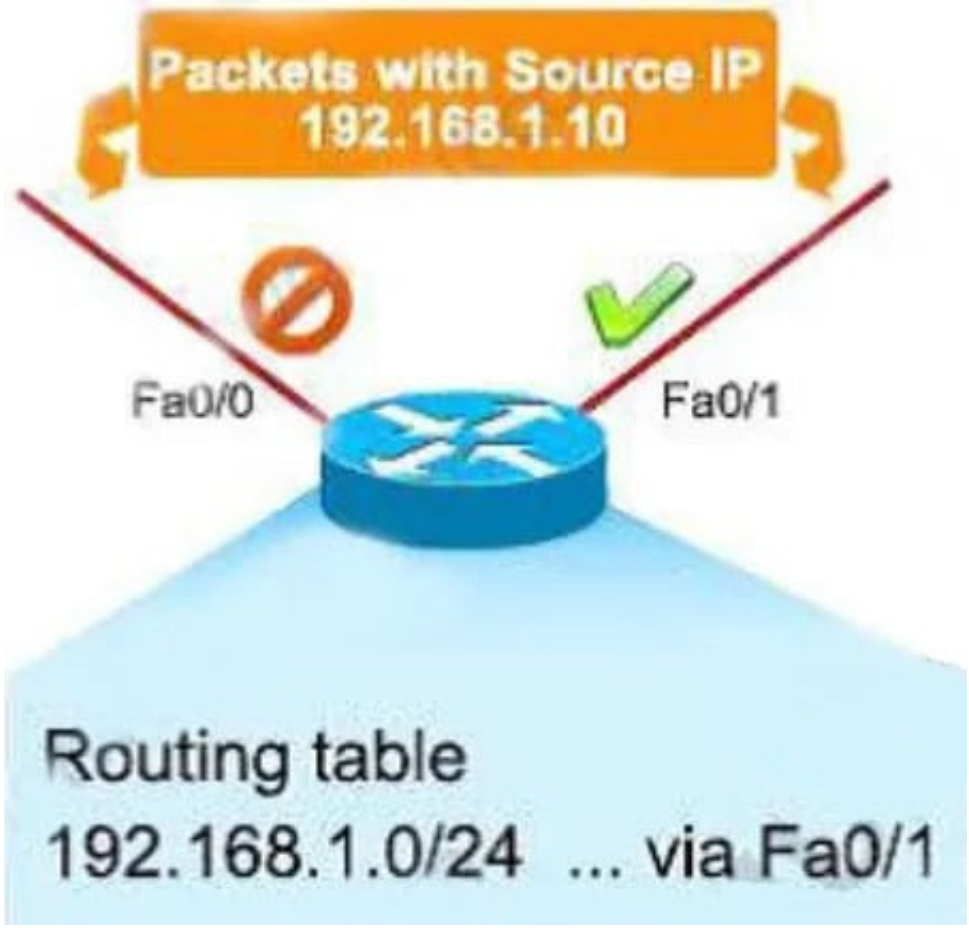
Correct Answer: B

According to this question, uRPF is running in strict mode because packets are dropped even when that route exists in the routing table. Maybe packets are dropped because the receiving interface is different from the interface the local

router uses to send packets to that destination.

The ip verify unicast source reachable-via rx command enables Unicast RPF in strict mode.

To enable loose mode, administrators can use the any option (ip verify unicast source reachable-via any). In loose mode, it doesn\\'t matter if we use this interface to reach the source or not.



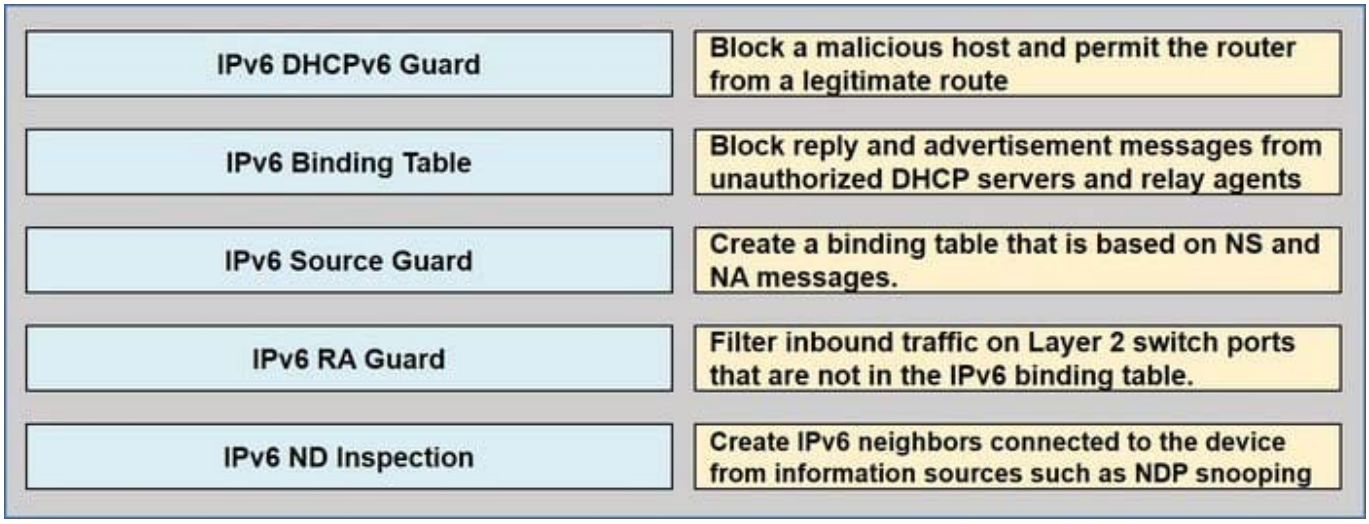
The allow-default option allows the use of the default route in the source verification process.

QUESTION 14

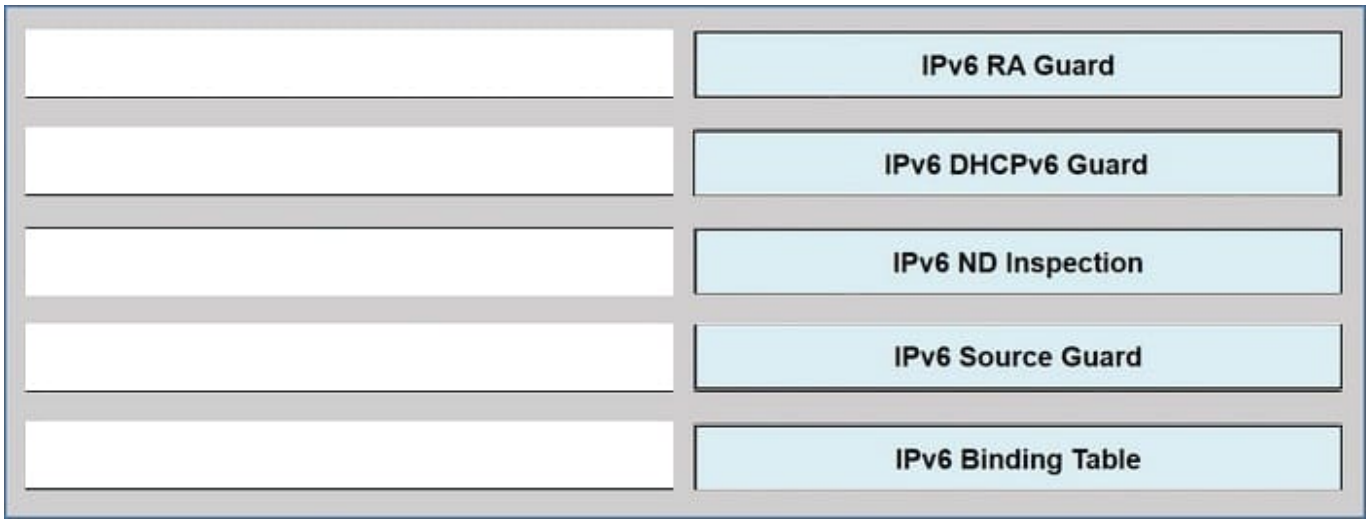
DRAG DROP

Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.

Select and Place:



Correct Answer:



+

Block reply and advertisement messages from unauthorized DHCP servers and relay agents: IPv6 DHCPv6 Guard

+

Create a binding table that is based on NS and NA messages: IPv6 ND Inspection

+

Filter inbound traffic on Layer 2 switch port that are not in the IPv6 binding table: IPv6 Source Guard

+

Block a malicious host and permit the router from a legitimate route: IPv6 RA Guard

+

Create IPv6 neighbors connected to the device from information sources such as NDP snooping: IPv6 Binding Table

QUESTION 15

What is a function of the IPv6 DHCP Guard feature for DHCP messages?

A. If the device is configured as a DHCP server, no message is switched.

B. All client messages are always switched regardless of the device role.

C. It blocks only DHCP request messages.

D. Only access lists are supported for matching traffic.

Correct Answer: B

DHCPv6 Guard Overview 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. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcpv6-guard.pdf