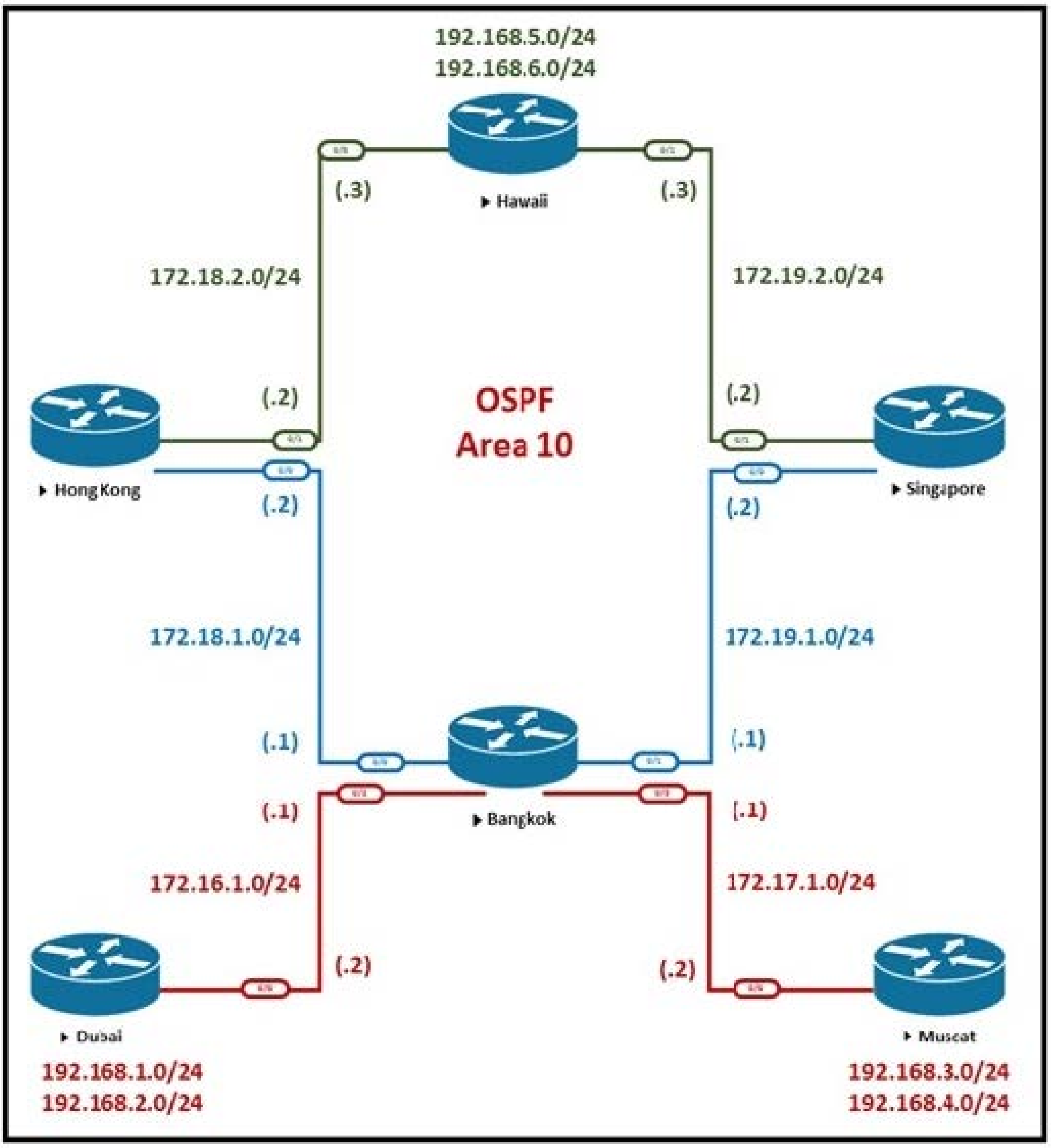
300-410$^{\text{Q\&As}}$

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

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

QUESTION 1

Refer to the exhibit. Bangkok is using ECMP to reach to the 192.168.5.0/24 network. The administrator must configure Bangkok in such a way that Telnet traffic from 192.168.3.0/24 and 192.168.4.0/24 networks uses the HongKong router as the preferred router. Which set of configurations accomplishes this task?



A. access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 ! route-map PBR1 permit 10 match ip address 101 set ip next-hop 172.18.1.2 interface Ethernet0/3 ip policy route-map PBR1

B. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 route-map PBR1 permit 10 match ip address 101 set ip next-hop 172.18.1.2 interface Ethernet0/1 ip policy route-map PBR1

C. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 route-map PBR1 permit 10 match ip address 101 set ip next-hop 172.18.1.2

interface Ethernet0/3 ip policy route-map PBR1

D. access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 route-map PBR1 permit 10 match ip address 101 set ip next-hop 172.18.1.2 interface Ethernet0/1 ip policy route-map PBR1

Correct Answer: C

We need to use Policy Based Routing (PBR) here on Bangkok router to match the traffic from 192.168.3.0/24 and 192.168.4.0/24 and "set ip next-hop" to HongKong router(172.18.1.2 in this case). Note: Please notice that we have to apply the PBR on incoming interface e0/3 to receive traffic from 192.168.3.0/24 and 192.168.4.0/24.

QUESTION 2

First-Hop Security (FHS) is a set of features to optimize IPv6 link operation, and help with scale in large L2 domains. Which of the following are valid First-Hop Security features supported by Cisco? (Choose three.)

A. IPv6 RA Guard

B. IPv6 Source Guard

C. DHCPv6 Guard

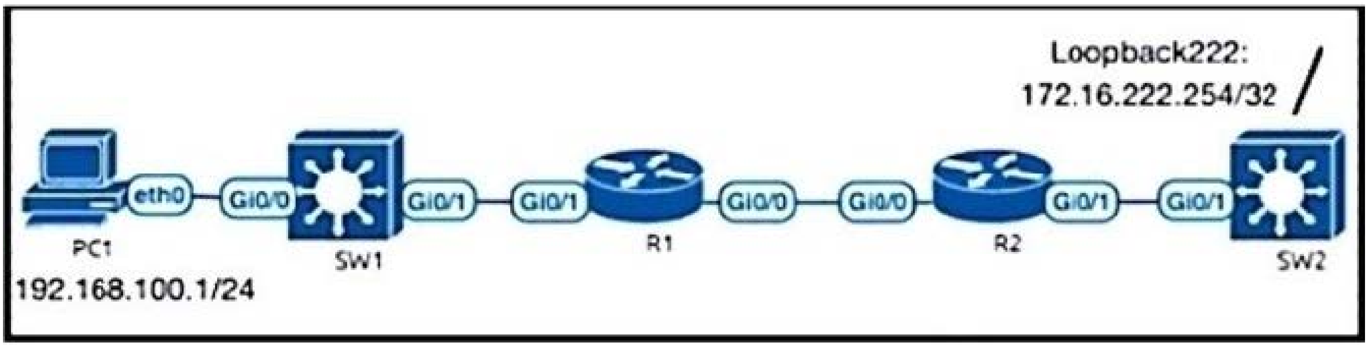
D. IPv6 Snooping

E. DHCPv6 Snooping

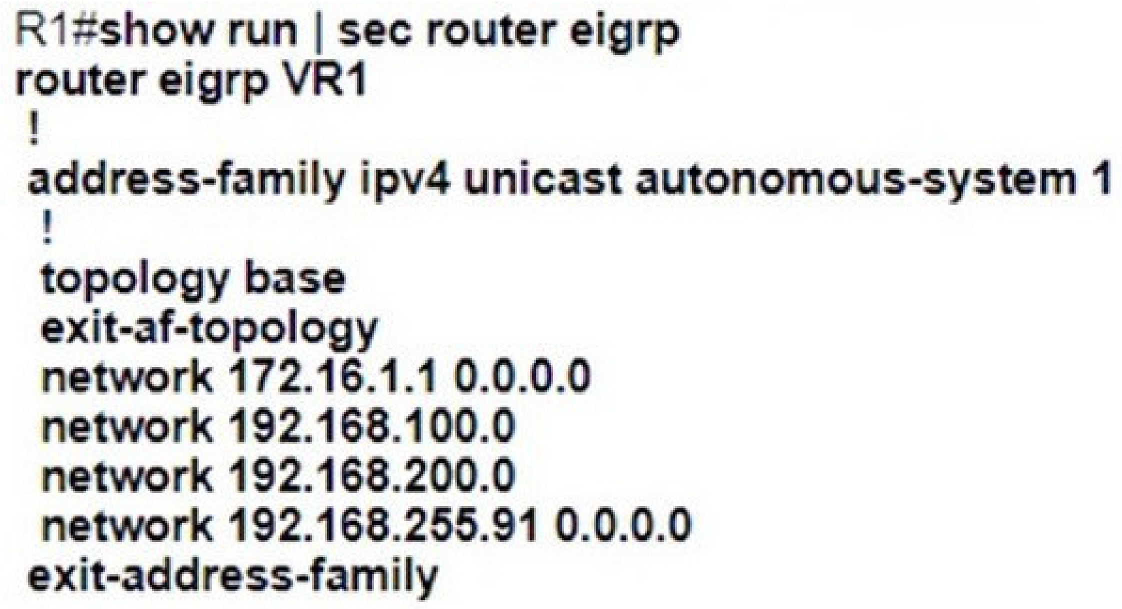
Correct Answer: ACD

QUESTION 3

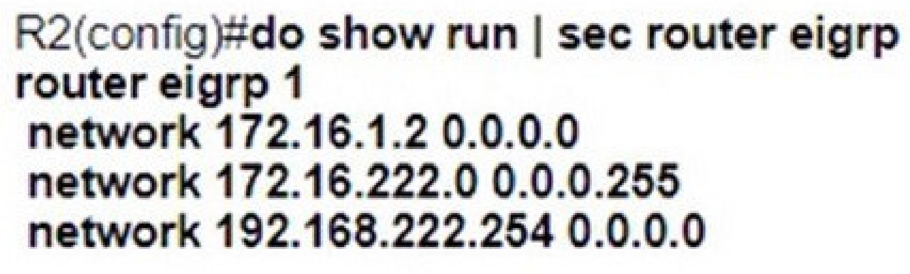
Refer to the exhibit.



R2 can reach Loopback222, but R1, SW1, and PC1 cannot communicate with 172.16.222.254. R1 and R2 configurations are shown here:



```
R1#show run | sec router eigrp
router eigrp VR1
 !
 address-family ipv4 unicast autonomous-system 1
  !
  topology base
  exit-af-topology
  network 172.16.1.1 0.0.0.0
  network 192.168.100.0
  network 192.168.200.0
  network 192.168.255.91 0.0.0.0
 exit-address-family
```



```
R2(config)#do show run | sec router eigrp
router eigrp 1
 network 172.16.1.2 0.0.0.0
 network 172.16.222.0 0.0.0.255
 network 192.168.222.254 0.0.0.0
```

Which EIGRP configuration command resolves the issue?

A. R1(config-router)# redistribute static

B. R2(config-router)# redistribute static

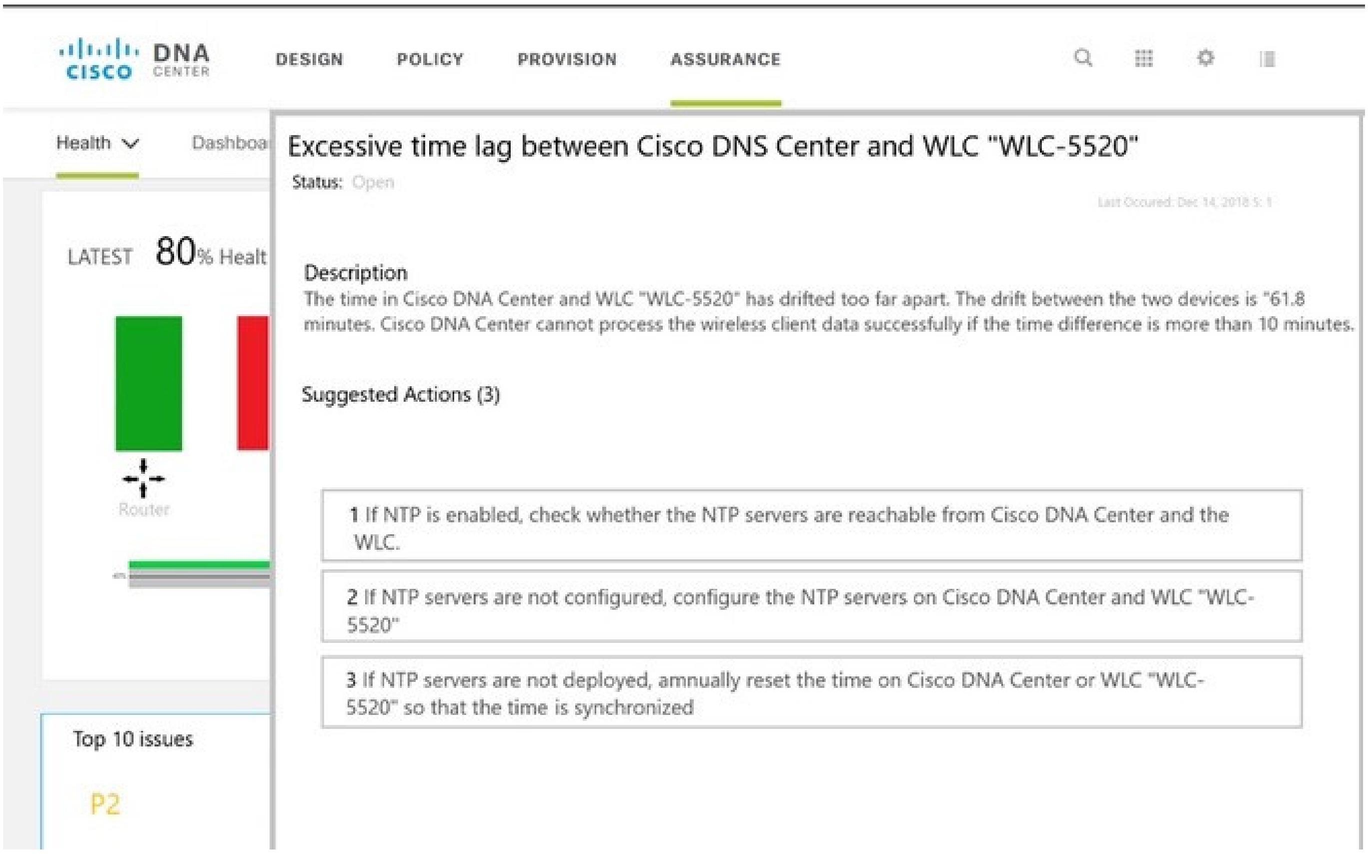
C. R1(config-router)# network 172.16.222.254 0.0.0.0

D. R1(config-router)# network 172.16.222.254 255.255.255.255

Correct Answer: B

QUESTION 4

Refer to the exhibit. NTP is configured across the network infrastructure and Cisco DNA Center. An NTP issue was reported on the Cisco DNA Center at 17:15.



Excessive time lag between Cisco DNS Center and WLC "WLC-5520"

Status: Open

Last Occured: Dec 14, 2018 5: 1

Description

The time in Cisco DNA Center and WLC "WLC-5520" has drifted too far apart. The drift between the two devices is "61.8 minutes. Cisco DNA Center cannot process the wireless client data successfully if the time difference is more than 10 minutes.

Suggested Actions (3)

1 If NTP is enabled, check whether the NTP servers are reachable from Cisco DNA Center and the WLC.

2 If NTP servers are not configured, configure the NTP servers on Cisco DNA Center and WLC "WLC-5520"

3 If NTP servers are not deployed, amnually reset the time on Cisco DNA Center or WLC "WLC-5520" so that the time is synchronized

Which action resolves the issue?

A. Check and resolve reachability between the WLC and the NTP server

B. Reset the NTP server to resolve any synchronization issues tor all devices

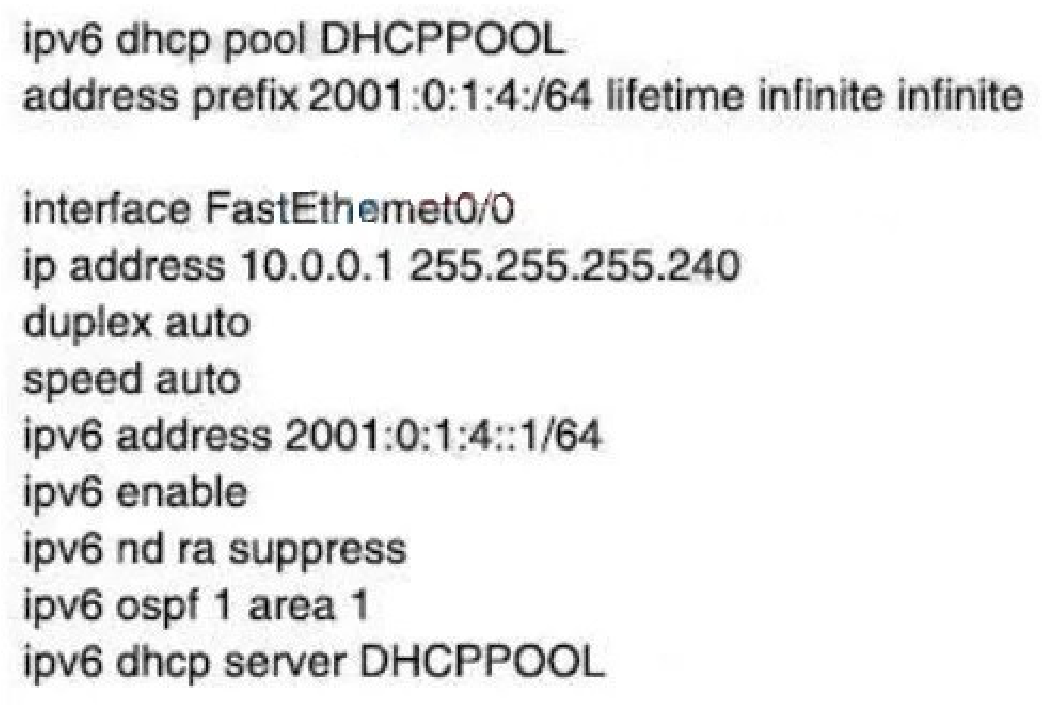
C. Check and resolve reachability between Cisco DNA Center and the NTP server

D. Check and configure NTP on the WLC and synchronize with Cisco DNA Center

Correct Answer: A

QUESTION 5

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 FastEthemet0/0
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 address 2001:0:1:4::1/64

B. ipv6 dhcp server DHCPPOOL

C. ipv6 nd ra suppress

D. address prefix 2001:0:1:4::/64 lifetime infinite infinite

Correct Answer: C

QUESTION 6

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

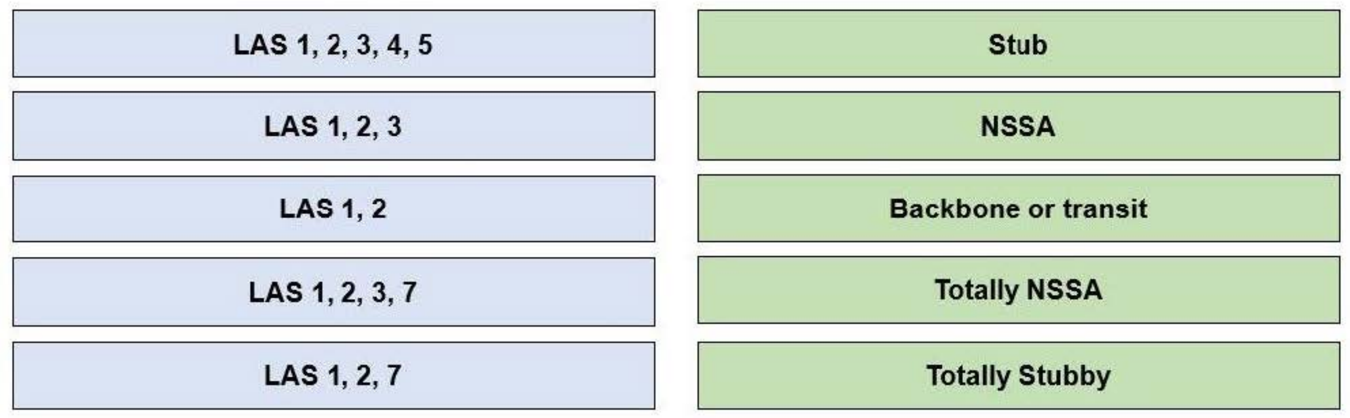
Correct Answer: A

QUESTION 7

DRAG DROP

Click and drag the associated set of OSPF LEAs on the left to the corresponding area type on the right where this set of LEAs may be seen.

Select and Place:



LAS 1, 2, 3, 4, 5

LAS 1, 2, 3

LAS 1, 2

LAS 1, 2, 3, 7

LAS 1, 2, 7

Stub

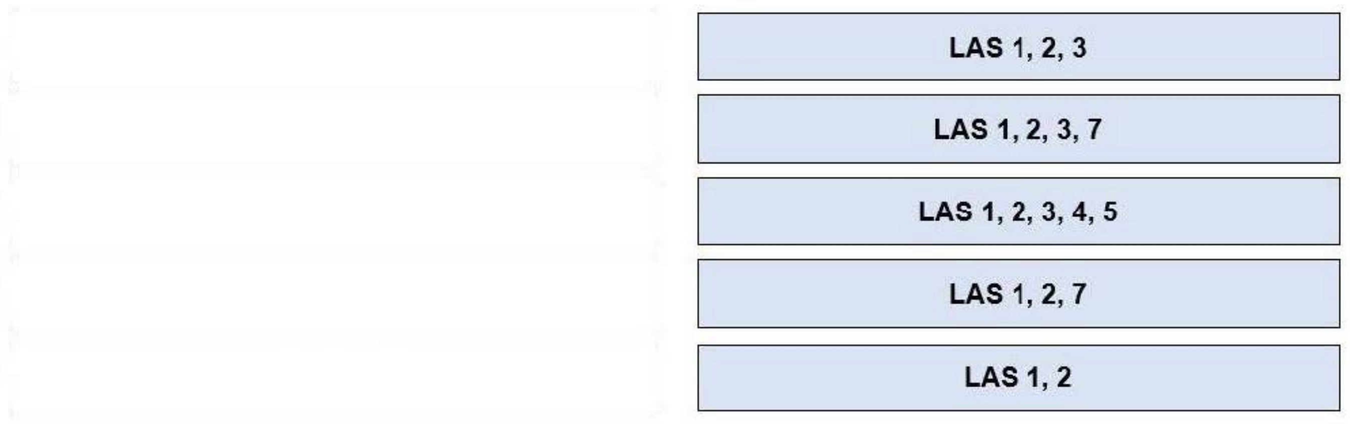
NSSA

Backbone or transit

Totally NSSA

Totally Stubby

Correct Answer:



LAS 1, 2, 3

LAS 1, 2, 3, 7

LAS 1, 2, 3, 4, 5

LAS 1, 2, 7

LAS 1, 2

QUESTION 8

With respect to modifying an OSPF router ID to a loopback address, which of the following statements are true?

A. OSPF is not as reliable if a loopback interface is configured.

B. Using a loopback address avoids wasting an additional IP address.

C. A loopback interface is not always active, and it can go "down" like a real interface.

D. The loopback address does not automatically appear in the routing table of neighboring OSPF routers, so it cannot be pinged from other routers unless you include it with a network statement on the router local to the loopback interface.

Correct Answer: D

A loopback address does not automatically appear in neighboring routers\\' routing tables, so it cannot be pinged for network troubleshooting.

A work-around for this problem is to add a network statement under OSPF that advertises the loopback address network so that other routers will know how to reach your loopback.

A loopback address is an IP address assigned to a loopback interface, which is a logical interface on a router that behaves like a physical interface. Their advantage is that, unlike physical interfaces, logical interfaces do not go down.

For example:

```
Router(config)# interface loopback 0

Router(config-if)# ip address 172.17.1.1 255.255.255.0
```

In the example, a loopback IP address is used by OSPF to provide its router ID. This type of address is preferred because it is assumed to be more stable than a router ID tied to a physical interface. The traditional problem with a router ID

tied to a physical interface is that if the physical interface were to go down, the router would have to change its router ID to some other value. That would cause the OSPF neighbor relationships to reset and change values in the link-state

advertisements (LSAs), causing a disruption to the OSPF area.

With this consideration in mind, OSPF is more reliable when using a loopback interface than using a physical interface.

Using a loopback address does not avoid wasting an additional IP address. The address must still be unique.

A loopback interface is always active, and it cannot go "down" as a physical interface can.

Objective:

Layer 3 Technologies

Sub-Objective:

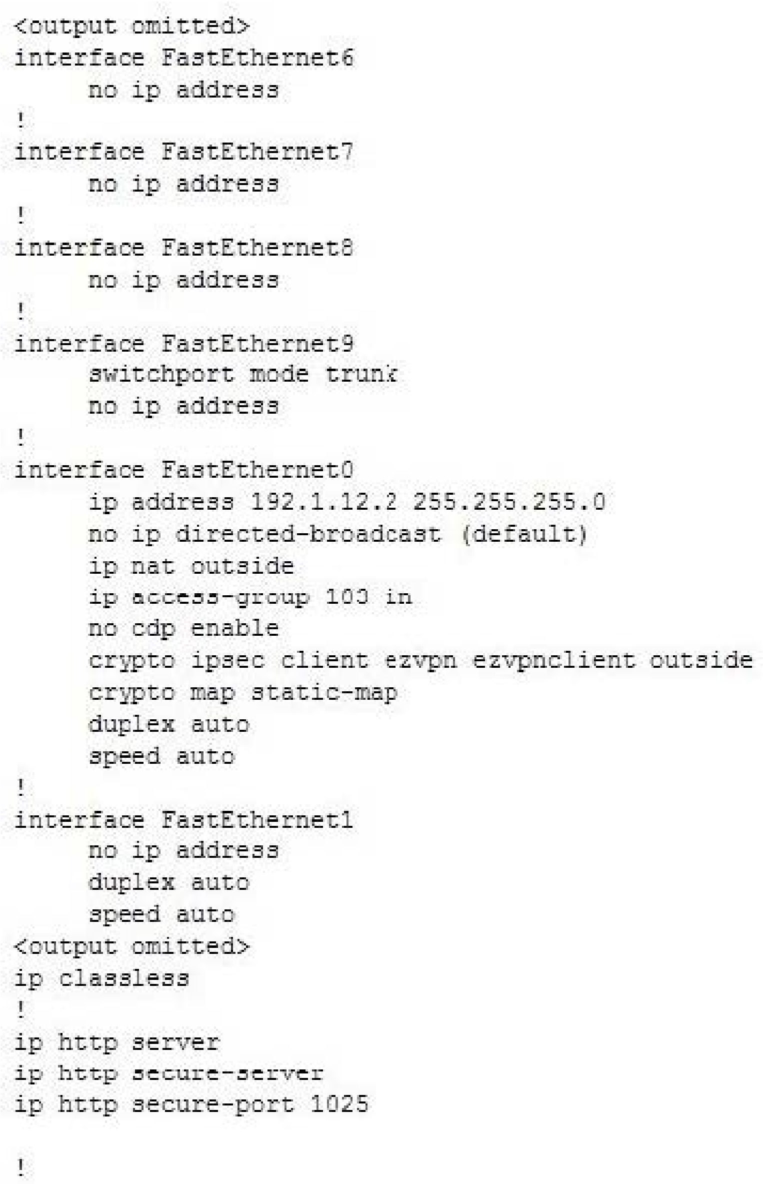
Configure and verify OSPF operations

References:

Cisco > IP Routing: OSPF Configuration Guide > Configuring OSPF > Forcing the Router ID Choice with a Loopback Interface

QUESTION 9

Some of the technicians in your organization use the secure web interface to make some of the configurations changes on the router R68. Today it was reported that a technician could not make a connection to the secure web server. You execute a show run command on R68 and receive the following output:



```
<output omitted>
interface FastEthernet6
     no ip address
!
interface FastEthernet7
     no ip address
!
interface FastEthernet8
     no ip address
!
interface FastEthernet9
     switchport mode trunk
     no ip address
!
interface FastEthernet0
     ip address 192.1.12.2 255.255.255.0
     no ip directed-broadcast (default)
     ip nat outside
     ip access-group 103 in
     no cdp enable
     crypto ipsec client ezvpn ezvpnclient outside
     crypto map static-map
     duplex auto
     speed auto
!
interface FastEthernet1
     no ip address
     duplex auto
     speed auto
<output omitted>
ip classless
!
ip http server
ip http secure-server
ip http secure-port 1025

!
```

What must the technician do to make the connection to the secure web interface?

A. specify port 443 in the command

B. specify port 1025 in the command

C. disable the HTTP server first

D. enable the secure server

Correct Answer: B

The partial output of the show run command indicates that the port number of the HTTPS interface has been changed to 1025. This is indicted by the presence of this command in the configuration:

ip http secure-port 1025

That is not the default port configuration of 443. Therefore, anyone wishing to connect to the secure server will need to reference the new port number in the command. If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:

https://device:port_number

In this syntax, port_number is the HTTPS port number.

It will not help for the technician to reference port 443 in the command, because that is no longer the port number of the secure server. It is now 1025.

It is not required to disable the HTTP server to use the HTTPS server, although it is a best practice to do so.

There is no need to enable the secure server. We can see it has been enabled by the presence of this command in the configuration:

ip http secure-server

Objective:

Infrastructure Services

Sub-Objective:

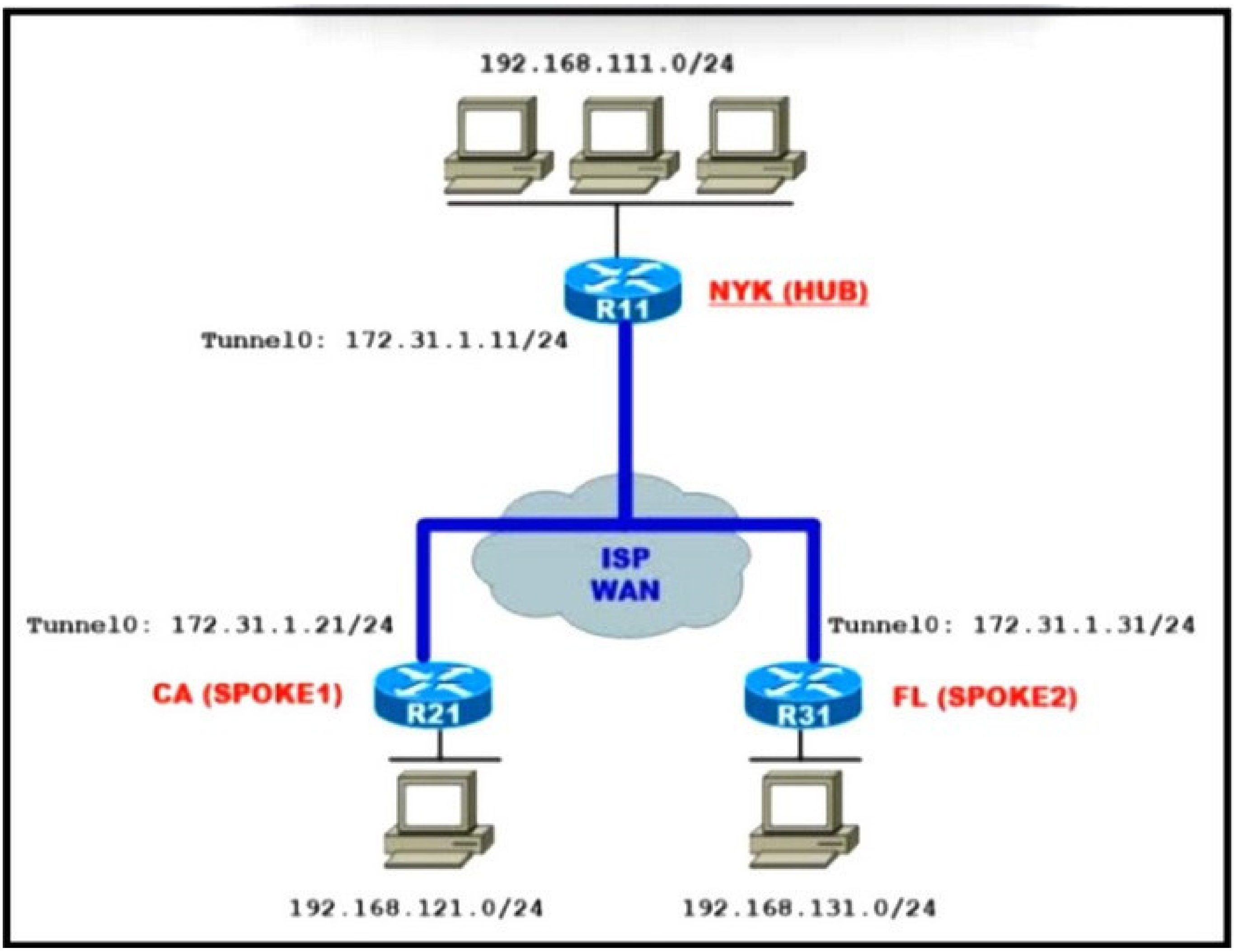
Configure and verify device management

References:

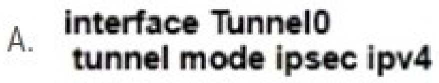
Cisco IOS HTTP Services Command Reference > clear ip http client cookie through show ip http server secure status > ip http secure-port

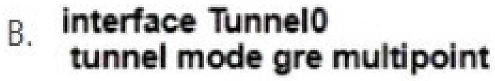
QUESTION 10

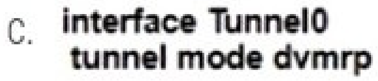
Refer to the exhibit.

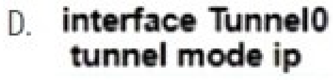


An engineer must configure the hub router to add new offices in the same infrastructure without performing any further configurations at the hub router. Which tunnel mode configuration on the hub router meets this requirement?


A.
```
interface Tunnel0
 tunnel mode ipsec ipv4
```


B.
```
interface Tunnel0
 tunnel mode gre multipoint
```


C.
```
interface Tunnel0
 tunnel mode dvmrp
```


D.
```
interface Tunnel0
 tunnel mode ip
```

A. Option A

B. Option B

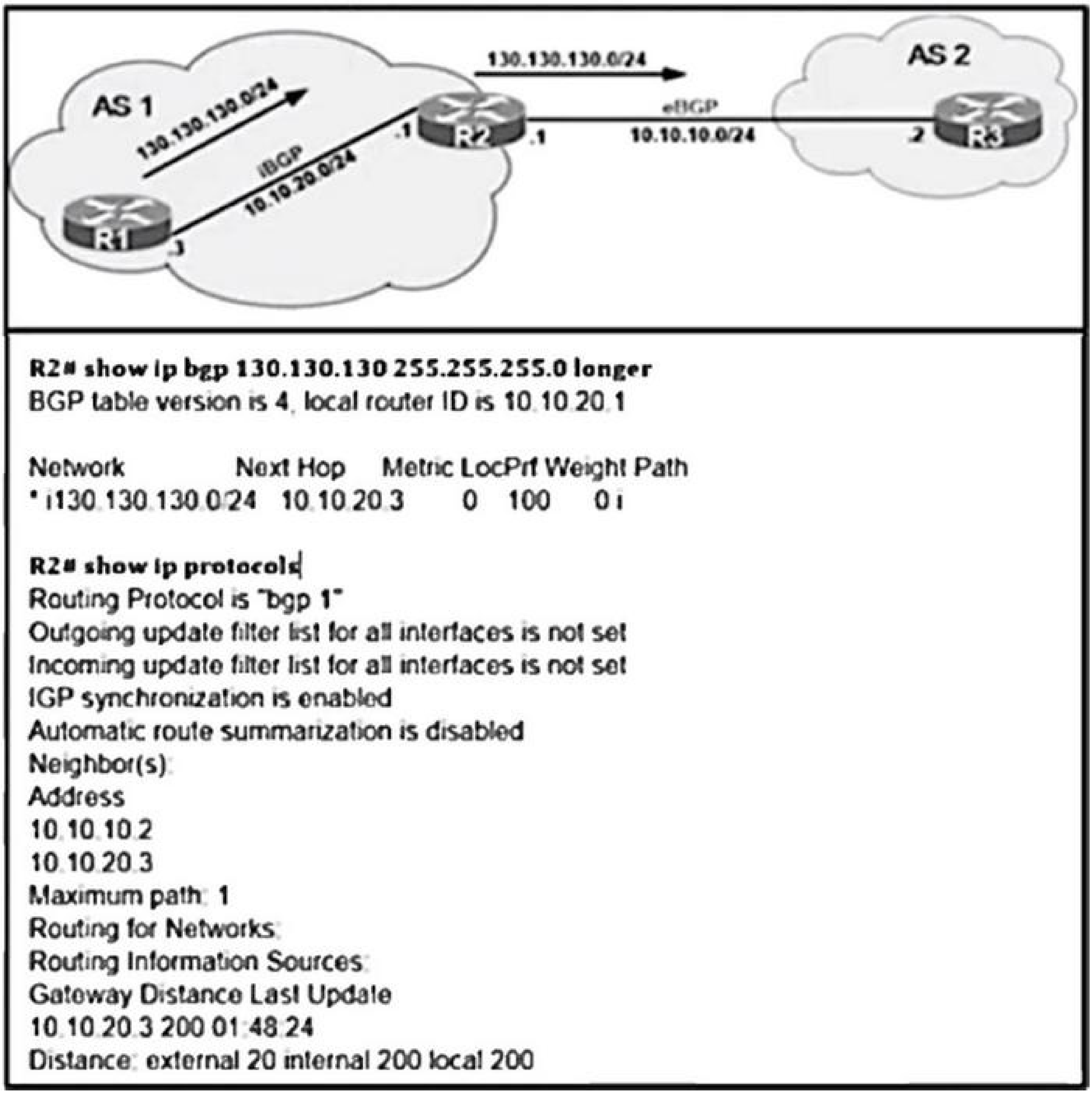
C. Option C

D. Option D

Correct Answer: B

QUESTION 11

Refer to the exhibit.



```
R2# show ip bgp 130.130.130 255.255.255.0 longer
BGP table version is 4, local router ID is 10.10.20.1

Network            Next Hop     Metric LocPrf Weight Path
* i130.130.130.0/24   10.10.20.3      0    100     0 i

R2# show ip protocols
Routing Protocol is "bgp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
IGP synchronization is enabled
Automatic route summarization is disabled
Neighbor(s):
Address
10.10.10.2
10.10.20.3
Maximum path: 1
Routing for Networks:
Routing Information Sources:
Gateway Distance Last Update
10.10.20.3 200 01:48:24
Distance: external 20 internal 200 local 200
```

The 130.130.130.0/24 route shows in the R2 routing table but is getting filtering toward R3. Which action resolves the issue?

A. Automatic route summarization must be enabled on R2.

B. The outgoing filter list for all interfaces must be set on R2.

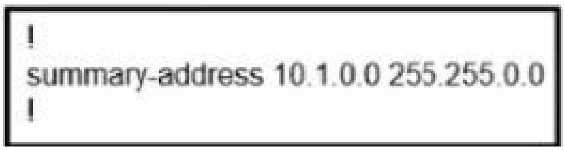
C. The incoming filter list for all interfaces must be set on R2.

D. IGP synchronization must be disabled on R2.

Correct Answer: D

QUESTION 12

Refer to the exhibit.



```
!
summary-address 10.1.0.0 255.255.0.0
!
```

The none area 0 routers in OSPF still receive more specific routes of 10.1.1.0.10.1.2.0.10.1.3.0 from area 0. Which action resolves the issue?

A. Configure route summarization on OSPF-enabled interfaces.

B. Summarize by using the summary-address 10.1.0.0 255.255.252.0 command.

C. Summarize by using the area range command on ABRs

D. Configure the summary-address 10.1.0.0 255.255.252.0 command under OSPF process.

Correct Answer: C

QUESTION 13

A customer reports that traffic is not passing on an EIGRP enabled multipoint interface on a router configured as below:

interface Serial0/0/0 no ip address interface Serial0/0/0.9 multipoint ip address 10.1.1.1 255.255.255.248 ip split-horizon eigrp 1

Which action resolves the issue?

A. Enable split horizon.

B. Disable poison reverse.

C. Disable split horizon.

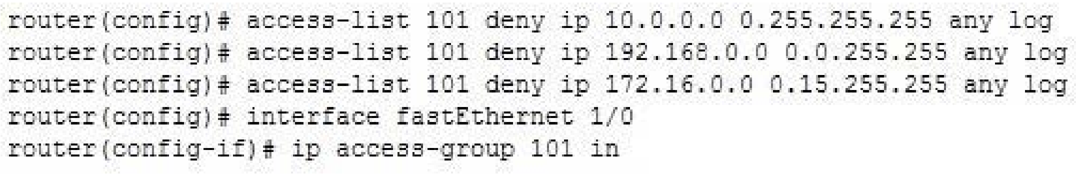
D. Enable poison reverse.

Correct Answer: C

In this question sub-interface is used so we have to turn off split-horizon for EIGRP.

QUESTION 14

The following commands were executed on the perimeter router. The Fa1/0 interface in the router is the external interface.



```
router(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
router(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
router(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
router(config)# interface fastEthernet 1/0
router(config-if)# ip access-group 101 in
```

What will be the effect of these commands?

A. all traffic will be blocked incoming

B. traffic sourced from private IP addresses will be blocked incoming

C. traffic destined for private IP addresses will be allowed incoming

D. no traffic will be blocked incoming

Correct Answer: A

All traffic will be blocked incoming. While it appears on the surface that this list was designed to block incoming traffic sourced from private IP addresses, it is lacking a single permit statement. Due to the implied deny all at the end of the list,

no traffic will be allowed incoming.

Blocking incoming traffic from private IP addresses is a way to prevent IP spoofing, since there should be no reason for traffic from private IP addresses to be incoming from the Internet. However, you need to include a permit statement at the

end to allow all other traffic types.

Traffic destined for private IP addresses is not all that will be blocked by this command set. In fact, no traffic would be allowed. If there were a permit ip any any at the end of the list, then incoming traffic destined for private IP addresses would

be allowed. This is probably not a great idea either, but if it a permit IP any were added at the end of the command set in the scenario, it would allow incoming traffic destined for private IP addresses.

Objective:

Infrastructure Security

Sub-Objective:

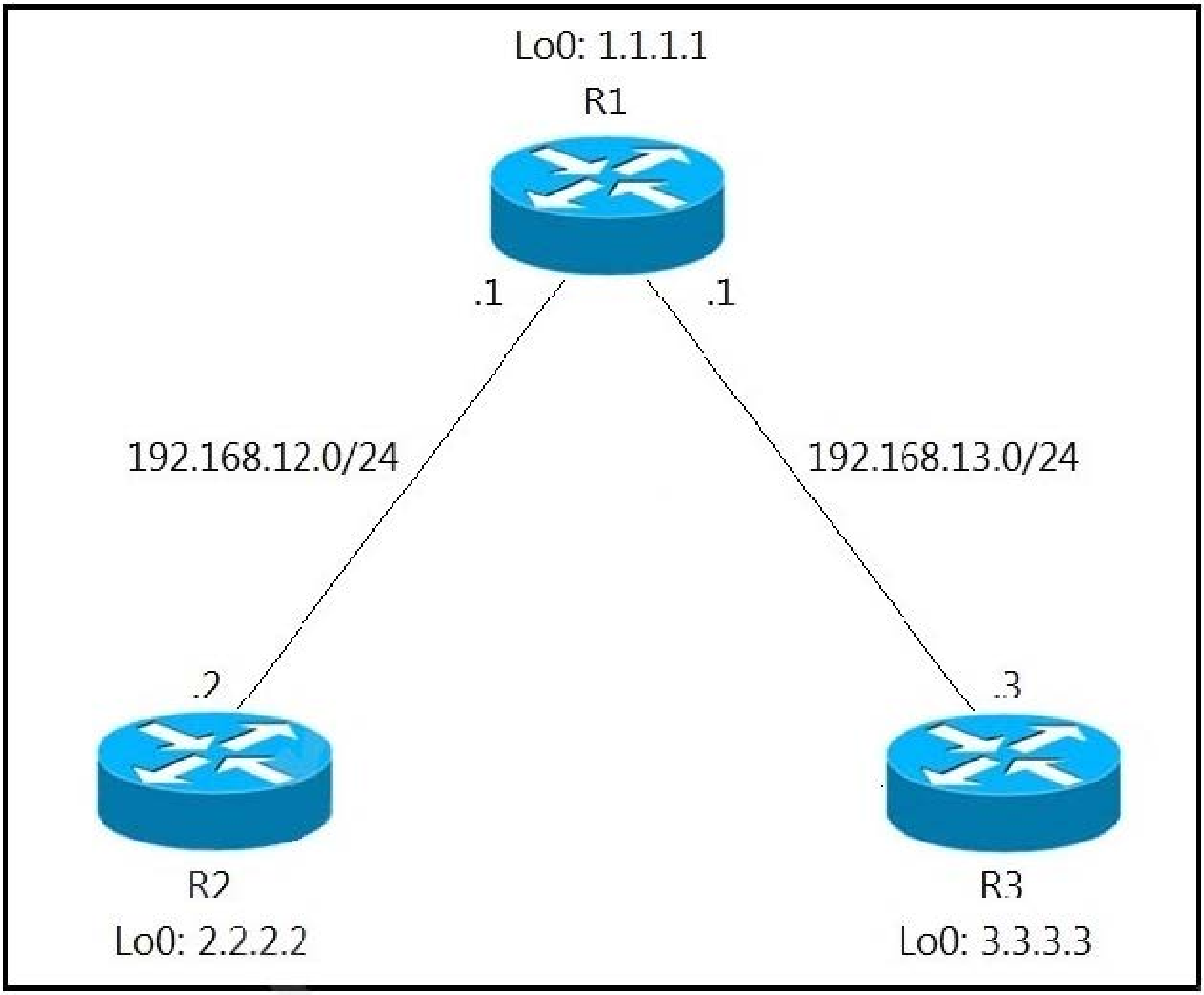
Configure and verify router security features

References:

Cisco > Cisco IOS Security Command Commands A to C > access-list Cisco > Cisco IOS Security Command Commands D to L > ip-group Prevent IP spoofing with the Cisco IOS

QUESTION 15

Refer to the exhibit. An engineer has configured R1 as EIGRP stub router. After the configuration, router R3 failed to reach to R2 loopback address.



Which action advertises R2 loopback back into the R3 routing table?

A. Add a static route for R2 loopback address in R1 and redistribute it to advertise to R3.

B. Use a leak map on R1 that matches the required prefix and apply it with the distribute list command toward R3.

C. Use a leak map on R3 that matches the required prefix and apply it with the EIGRP stub feature.

D. Add a static null route for R2 loopback address in R1 and redistribute it to advertise to R3.

Correct Answer: B

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

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