Exam Questions 300-135

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

https://www.2passeasy.com/dumps/300-135/

NEW QUESTION 1
Which two features are supported with GRE-based tunnels? (Choose two)

A. on-demand tunnels
B. any-to-any connectivity
C. data encapsulation
D. encryption
E. multicast traffic forwarding

Answer: CE

NEW QUESTION 2
Which command displays the RSA public keys of a Cisco router?

A. show crypto key rsa
B. show crypto session local
C. show crypto key mypubkey rsa
D. show crypto map

Answer: A

NEW QUESTION 3
Reset/down - This is usually a transient state when the tunnel is reset by software. This usually happens when the tunnel is misconfigured with a Next Hop Server (NHS) that is it's own IP address.
When a tunnel interface is first created and no other configuration is applied to it, the interface is not shut by default:

```
Router#show run interface tunnel 1
Building configuration...

Current configuration : 40 bytes
!
interface Tunnel1
 no ip address
end
```

In this state, the interface is always up/down:

```
Router(config-if)#do show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         172.16.52.1     YES NVRAM  administratively down down
GigabitEthernet0/1         14.36.128.49    YES NVRAM  down                  down
GigabitEthernet0/2         unassigned      YES NVRAM  down                  down
GigabitEthernet0/3         unassigned      YES NVRAM  down                  down
Loopback1                  192.168.2.1     YES NVRAM  up                    up
Tunnel1          unassigned    YES unset  up          down
```

This is because the interface is administratively enabled, but since it does not have a tunnel source or a tunnel destination, the line protocol is down.

In order to make this interface up/up, a valid tunnel source and tunnel destination must be configured:

```
Router#show run interface tunnel 1
Building configuration...
```

```
Current configuration : 113 bytes
!
interface Tunnel1
 ip address 1.1.1.1 255.255.255.0
 tunnel source Loopback1
 tunnel destination 10.0.0.1
end
```

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         172.16.52.1     YES NVRAM  up                    up
GigabitEthernet0/1         14.36.128.49    YES NVRAM  down                  down
GigabitEthernet0/2         unassigned      YES NVRAM  down                  down
GigabitEthernet0/3         unassigned      YES NVRAM  down                  down
Loopback0                  unassigned      YES unset  up                    up
Loopback1                  192.168.2.1     YES manual up                    up
Tunnel1                    1.1.1.1         YES manual up                    up
```

The previous sequence shows that:

- A valid tunnel source consists of any interface that is itself in the up/up state and has an IP address configured on it. For example, if the tunnel source was changed to **Loopback0**, the tunnel interface would go down even though **Loopback0** is in the up/up state:

```
Router(config-if)#int tun 1
Router(config-if)#tunnel source loopback 0
Router(config-if)#
*Sep  6 19:51:31.043: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel1, changed state to down
```

- A valid tunnel destination is one which is routable. However, it does not have to be reachable, which can be seen from this ping test:

```
Router#show ip route 10.0.0.1
% Network not in table
Router#show ip route | inc 0.0.0.0
Gateway of last resort is 172.16.52.100 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.16.52.100
Router#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

4.
Which two statements about IPv6 traffic filtering are true? (Choose two.)

A. It performs virtual fragmentation reassembly after checking egress ACLs.
B. It performs virtual fragmentation after checking ingress ACLs.
C. It requires IPv6 neighbor discovery to be enabled on the interface.
D. It requires configuration to be done at the egress interface.
E. It is configured at the interface level.

Answer: BE

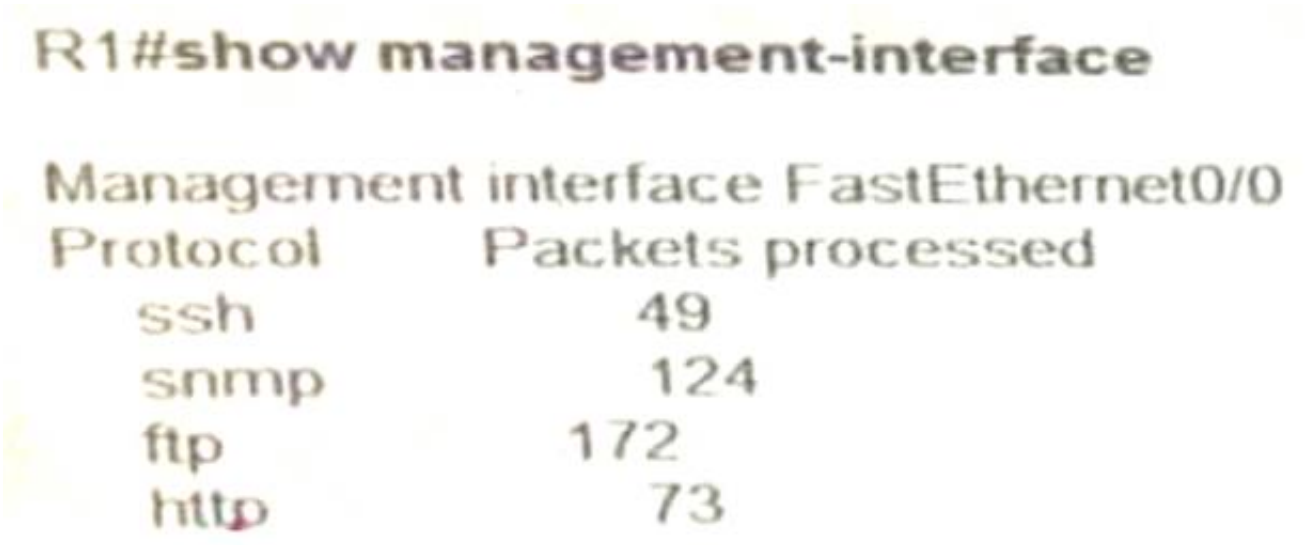
Explanation: When virtual fragmentation reassembly (VFR) is enabled, VFR processing begins after ACL input lists are checked against incoming packets. The incoming packets are tagged with the appropriate VFR information.

NEW QUESTION 4
Which IPsec mode will encrypt a GRE tunnel to provide multiprotocol support and reduced overhead?

A. 3DES
B. multipoint GRE
C. tunnel
D. transport

Answer: D

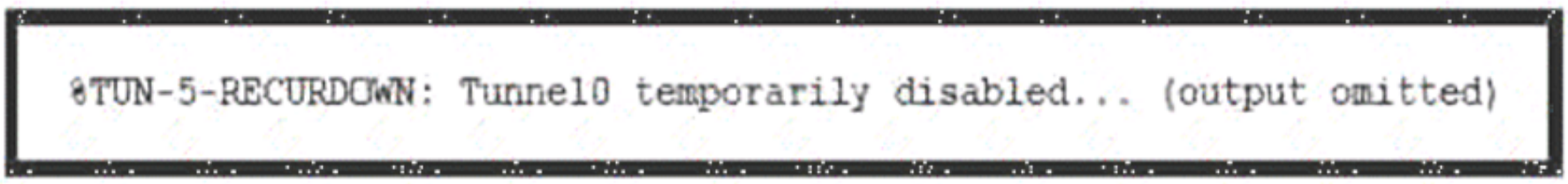
NEW QUESTION 5
Examine the output from R1. Interface FastEthernet0/0 is used for all management of the device. A client is able to connect to R1 on port 22, however, they are unable to connect on port 23. What is the cause of the problem?



A. Management Plane Protection (MPP) is enabled, however telnet is not allowed
B. Telnet and SSH are not allowed at the same time.
C. Management Plane Protection (MPP) is enabled, which only allows SSH
D. Management Plane Protection (MPP) is enabled on the wrong interface

Answer: A

NEW QUESTION 6
Refer to the exhibit.



Which statement indicates a cause for Tunnel0's connection failure?

A. The tunnel destination interface is flapping, which causes the tunnel to go up and down.
B. The tunnel source interface is in an up/down state and the tunnel destination is recursively routing as a result
C. The tunnel is configured with the wrong encapsulation
D. The tunnel destination is intermittently reachable via multiple routing protocols

Answer: D

Explanation: Reference:
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/22327-gre-fla

NEW QUESTION 7
What are two primary components of a GRE tunnel? (Choose two.)

A. IP header
B. payload packet
C. GRE header
D. LLC header
E. Ethernet header

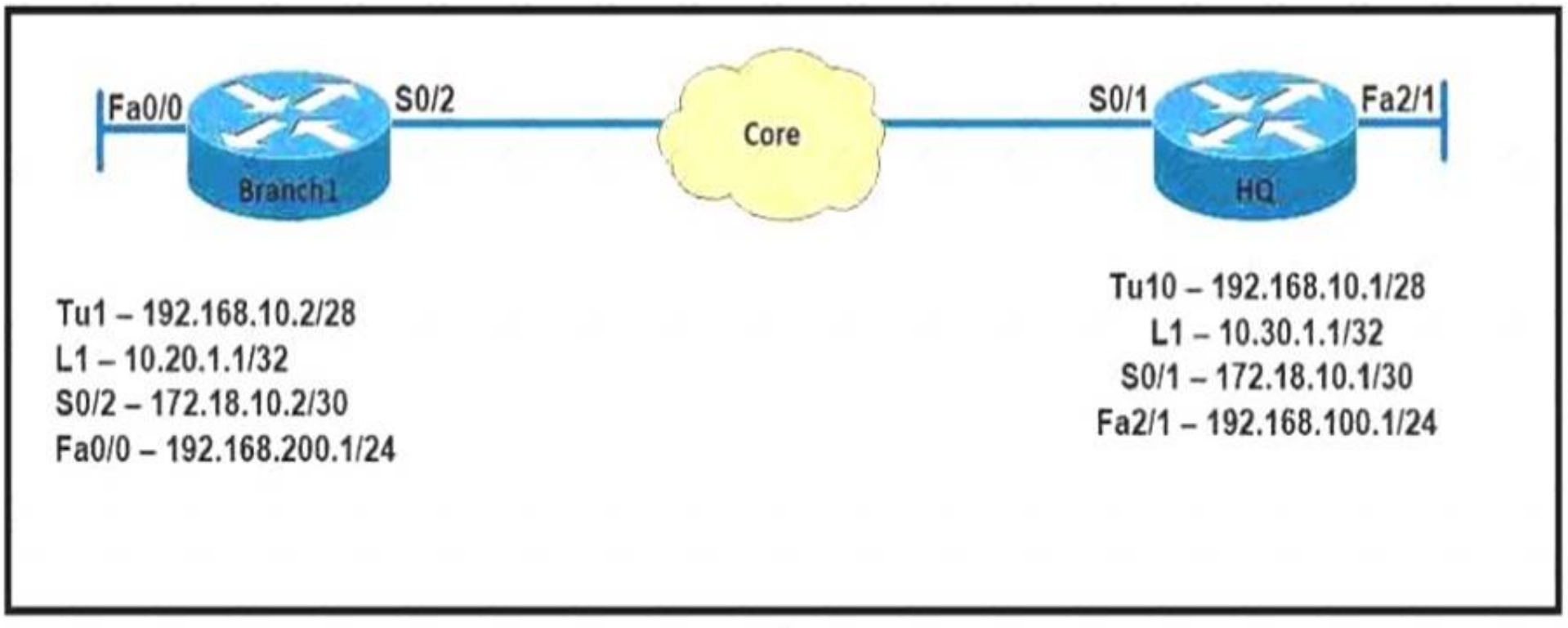
Answer: BC

NEW QUESTION 8
Which two statements about GRE are true?

A. It supports the OSPF and EIGRP routing protocols only.
B. It provides a tunnelless VPN technology.
C. It supports multicast and broadcast transmissions.
D. It supports encryption and authentication
E. It can carry broadcast traffic in the tunnel.

Answer: CE

NEW QUESTION 9
Refer to the exhibit.

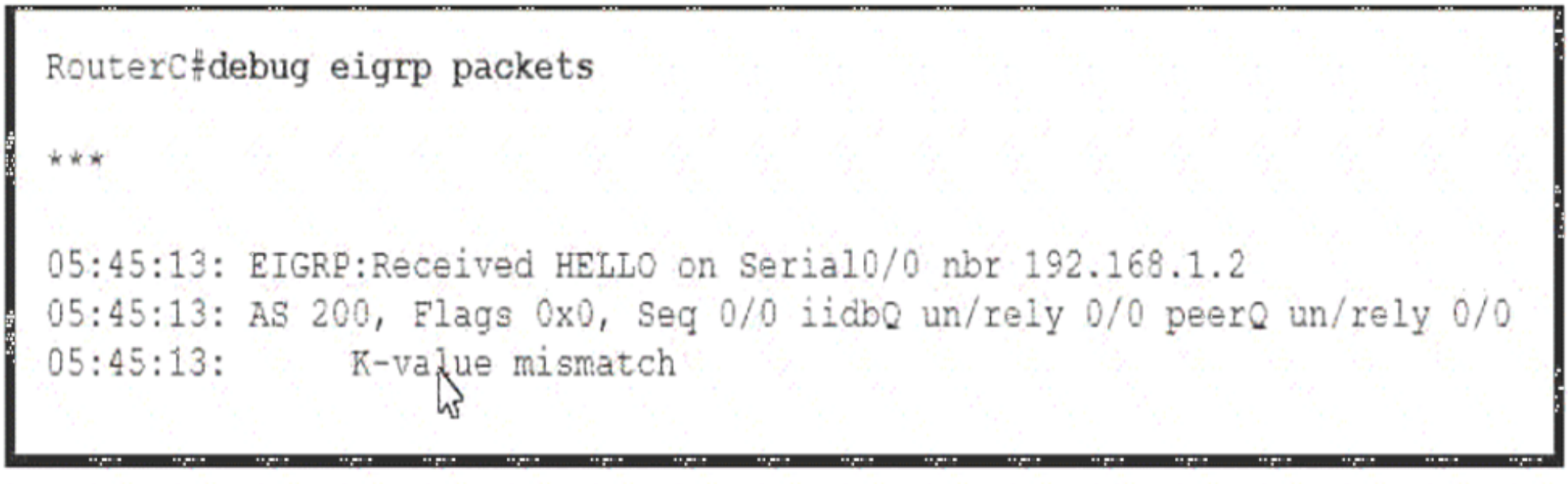


Which IP address should be configured as the tunnel source on the HQ router for maximum resiliency?

A. 10.20.1.1.0
B. 10.30.1.1
C. 172.18.10.2
D. 192.168.10.1

Answer: D

NEW QUESTION 10
Refer to the exhibit.



A NOC technician is troubleshooting an EIGRP connection between RouterC IP address 192 168.1 1. and RouterD. IP address 192.168.1 2 Given the debug output on RouterC which outcome is valid?

A. RouterC received a hello packet with mismatched authentication parameters.
B. RouterC received a hello packet with mismatched hello timers
C. RouterC will form an adjacency with RouterD
D. RouterC will not form an adjacency with RouterD

Answer: D

NEW QUESTION 10
Which command securely encrypts the enable password on an IOS device?

A. service password-encryption
B. enable secret
C. enable secure
D. enable password

Answer: A

NEW QUESTION 14

```
R1# debug migrp packet
     (UPDATE, REQUEST, QUERY, REPLY, HELOO, UNKNOWN, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)

R1#
EIGRP: Lost Peer: Total 1 (0/0/0/0/0)
EIGRP: Received HELLO on Gi1.146 - paklen 20 nbr 10.1.146.6
   AS 100, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0
EIGRP: Add Peer: Total 1 (1/0/0/0/0)
       K-value mismatch
EIGRP: Sending TIDLIST on GigabitEthernet1.146 - 1 items
EIGRP: Sending HELLO on Gi1.146 - paklen 30
   AS 100, Flags 0x0 : (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely /0
%DUAL-5-NBRCHANGE: EIGRP_IPv4 100: Neighbor 10.1.146.6 (GigabitEthernet1.146) is down: K-value mismatch
R1#
EIGRP: Lost Peer: Total 1 (0/0/0/0/0)
EIGRP: Sending HELLO on Gi1.13 - paklen 20
   AS 100, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1#
EIGRP: Gi1.13: ignored packet from 10.1.13.3, opcode = 5 (authentication off or key-chain missing)
R1#
EIGRP: Received HELLO on Gi1.146 - paklen 20 nbr 10.1.146.4
   AS 100, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0
```

Refer to the exhibit. When troubleshooting an adjacency issue on router R1, you generated the given debug output. Which two values are mismatched between R1 and its neighbor? (Choose two.)

A. hello timer settings
B. metric calculation mechanisms
C. authentication parameters
D. autonomous system numbers
E. hold timer settings

Answer: BD

NEW QUESTION 19
For which two reasons might a GRE Tunnel interface enter an up/down state? (Choose two)

A. The tunnel source is using a loopback interface.
B. The tunnel mode is defined as transport.
C. Keepalives are disabled on the interfaces
D. The route to the destination is through the tunnel itself.
E. The tunnel source interface is down.

Answer: DE

NEW QUESTION 20
You are performing a peer review on this implementation script, which is intended to enable AAA on a device.

```
username nmops privilege 15 secret Cisco 123
username nmeng privillege 15 secret 123Cisco
enable secret Str0ng34156732
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+
aaa authorization config-commands
aaa authourization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 5 default stop-only group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
```

If the script is deployed which two effects does it have on the device? (Choose two.)

A. Part of the script is rejected.
B. The device authenticates users against the local database first.

C. The device fails to perform AAA because session-id common command is missing.
D. The device authenticates all users except nmops and nmeng against the TACACS+ database.
E. The device fails to perform AAA because the aaa new-model command is missing.

Answer: AE

Explanation: R1#sh run | sec aaa
R1(config)#aaa authentication ?
R1(config)#aaa authentication login default local
^
% Invalid input detected at '^' marker. Also when enabling AAA:
R1#sh run | sec aaa aaa new-model
aaa authentication login default local aaa session-id common

NEW QUESTION 21
You must connect two remote sites over the public internet. Multicast support, security, and simplicity are required. Which tunneling technology sould you consider?

A. MPLS
B. GRE over IPsec
C. GET VPN
D. IPsec

Answer: B

NEW QUESTION 24
Which command can you enter to block SSH traffic from hosts on network 10.10.15.0/24?

A. access-list 142 deny tcp any 10.10.15.0 0.0.0.0 any eq 22
B. access-list 142 deny tcp any 10.10.15.0 0.0.0.255 eq 21
C. access-list 142 deny tcp 10.10.15.0 0.0.0.255 any eq 23
D. access-list 142 deny tcp 10.10.15.0 0.0.0.255 any eq 22

Answer: D

NEW QUESTION 26
Which protocol is used by traceroute and ping operations?

A. IGMP
B. CIP
C. CPIM
D. ICMP

Answer: D

NEW QUESTION 28
If you execute a traceroute and it returns only an asterisk (*), what does the result mean?

A. The protocol is unreachable.
B. The probe timed out.
C. The destination port is unreachable.
D. The destination server reported it is too busy.

Answer: B

NEW QUESTION 30
Refer to the exhibit.

```
MASS-RTR#show running-config
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 02362448181l5F3348
username cisco privilege 15 password 7 0607072C494A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

MASS-RTR#show archive log config all
 idx   sess           user@line      Logged command
    1      1       console@console  |interface GigabitEthernet0/0
    2      1       console@console  | no shutdown
    3      1       console@console  | ip address dhcp
    4      2         admin@vty0     |username cisco privilege 15 password cisco
    5      2         admin@vty0     |!config: USER TABLE MODIFIED
```

A client reports that all the password information appears in plain text when the show archive log config all command has been issued Which command fixes the issue?

A. MASS-RTR(config)#aaa authentication arap
B. MASS-RTR(config-archive-log-cfg)#password encryption aes
C. MASS-RTR(config)#service password-encryption
D. MASS-RTR(config-archive-log-cfg)#hidekeys

Answer: D

NEW QUESTION 35
Refer to the exhibit.

```
GW-RTR#show running-config
!
service password-encryption
!
hostname GW-RTR
!
line con 0
 exec-timeout 0 0
 password 7 0822455D0A16
 logging synchronous
line aux 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password 7 094F471A1A0A
 login
 transport input telnet
!
end
```

Which outcome regarding a telnet connection to the router is valid?

A. Telnet fails because of the missing AAA on the router
B. Telnet fails because of the missing username / password on the router.
C. Telnet fails because of the missing enable secret on the router
D. Telnet completes successfully

Answer: D

NEW QUESTION 38
Refer to the exhibit.

```
Internal#traceroute
Protocol [ip]:
Target IP address: cisco.com
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]: 2
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]: Verbose
Loose, Strict, Record, Timestamp, Verbose[V]:
Type escape sequence to abort.
Tracing the route to cisco.com (72.163.4.162)
VRF info: (vrf in name/id, vrf out name/id)
  1 46.16.251.157 [AS 5713] 1 msec
    46.16.251.158 [AS 5713] 2 msec
  2 46.16.251.169 [AS 5713] 1 msec
    134.222.97.8 [AS 5713] 2 msec
  3 134.222.97.8 [AS 5713] 1 msec
    71.185.45.21 [AS 5713] 1 msec
  4 71.185.45.21 [AS 5713] 2 msec !H
```

Which two statements are correct? (Choose Two)

A. The source device has name resolution configured.
B. The source device is using two routes for the destination, learned from different protocols.
C. A device on the path is introducing considerable delay.
D. The source device is loading balancing traffic.

Answer: AD

Explanation: Router traces domain name (cisco.com) and it gets ICMP answers, so name resolution has happened. Per hop output shows 2 lines, hence 2 active paths exist.

NEW QUESTION 43
Refer to the exhibit.

```
R1#show 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 212.50.185.126 to network 0.0.0.0

D    212.50.167.0/24 [90/160000] via 212.50.185.82, 00:05:55, Ethernet1/0
     212.50.166.0/24 is variably subnetted, 4 subnets, 2 masks
D       212.50.166.0/24 is a summary, 00:05:55, Null0
C       212.50.166.1/32 is directly connected, Loopback1
C       212.50.166.2/32 is directly connected, Loopback2
C       212.50.166.20/32 is directly connected, Loopback20
     212.50.185.0/27 is subnetted, 3 subnets
C       212.50.185.64 is directly connected, Ethernet1/0
C       212.50.185.96 is directly connected, Ethernet0/0
C       212.50.185.32 is directly connected, Ethernet2/0
D*EX 0.0.0.0/0 [170/2174976] via 212.50.185.126, 00:05:55, Ethernet0/0
               [170/2174976] via 212.50.185.125, 00:05:55, Ethernet0/0
```

How would you confirm on R1 that load balancing is actually occurring on the default-network (0.0.0.0)?

A. Use ping and the show ip route command to confirm the timers for each default network resets to 0.
B. Load balancing does not occur over default networks; the second route will only be used for failover.
C. Use an extended ping along with repeated show ip route commands to confirm the gateway of last resort address toggles back and forth.
D. Use the traceroute command to an address that is not explicitly in the routing table.

Answer: D

NEW QUESTION 48
Exhibit:

```
RouterA# debug eigrp packets
...
01:39:13:  EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:39:13:           K-value mismatch
```

A network administrator is troubleshooting an EIGRP connection between RouterA, IP address 10.1.2.1, and RouterB, IP address 10.1.2.2. Given the debug output on RouterA, which two statements are true? (Choose two.)

A. RouterA received a hello packet with mismatched autonomous system numbers.
B. RouterA received a hello packet with mismatched hello timers.
C. RouterA received a hello packet with mismatched authentication parameters.
D. RouterA received a hello packet with mismatched metric-calculation mechanisms.
E. RouterA will form an adjacency with RouterB.
F. RouterA will not form an adjacency with RouterB.

Answer: DF

NEW QUESTION 52
You want to troubleshoot an OSPF adjacency issue. Which two tasks must you perform? (Choose two.)

A. Issue the debug ip ospf nsf command to identity the cause.
B. Issue the debug ip ospf adj command to identify the cause.
C. Verify that the router IDs on the two routers match.
D. Verify that the subnet masks on the two routers match.
E. Verify that the process IDs on the two routers match.

Answer: BD

NEW QUESTION 54
Refer to the exhibit.

```
Gateway-Router(config-cp)#service-policy input DOS_Stop
'Weighted Fair Queueing' not supported on control-plane
error: failed to install policy map DOS_Stop
```

A large number of TCP sessions attempting to connect to a router cause memory leakage and the router to hang. During troubleshooting the client configures a service policy and applies it to the control plane resulting in the error shown What is the root cause of this error message?

A. The router license is missing in order to configure the policy map
B. The bandwidth command is not supported for policy maps configured for CoPP
C. Cisco routers lack the support for protecting the control plane.
D. The service policy should be configured for the output direction

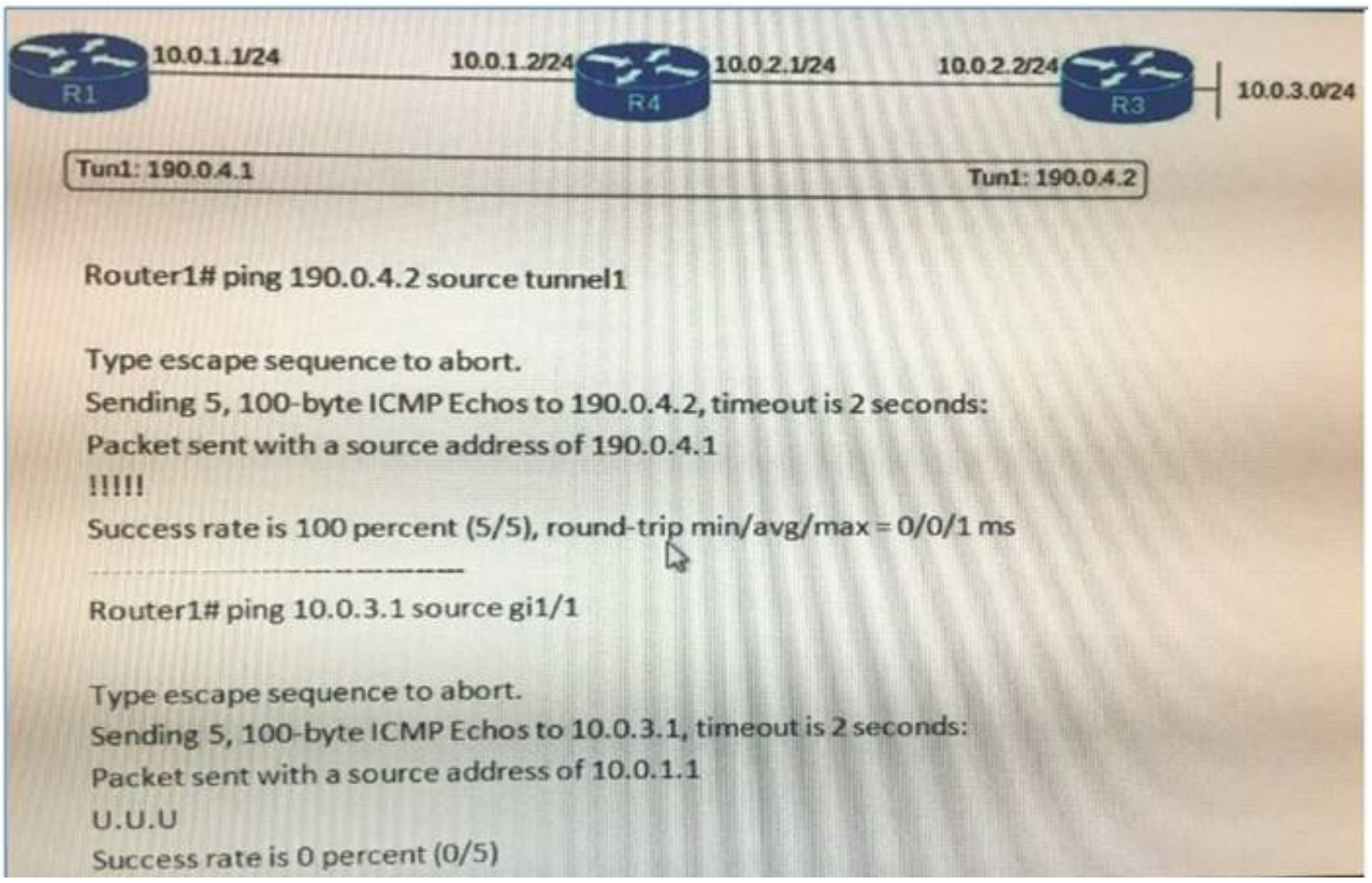
Answer: A

NEW QUESTION 56
When troubleshooting an EIGRP connectivity problem, you notice that two connected EIGRP routers are not becoming EIGRP neighbors. A ping between the two routers was successful. What is the next thing that should be checked?

A. Verify that the EIGRP hello and hold timers match exactly.
B. Verify that EIGRP broadcast packets are not being dropped between the two routers with the show ip EIGRP peer command.
C. Verify that EIGRP broadcast packets are not being dropped between the two routers with the show ip EIGRP traffic command.
D. Verify that EIGRP is enabled for the appropriate networks on the local and neighboring router.

Answer: D

NEW QUESTION 61
Refer to exhibit:



After a junior technician configures a new branch office GRE tunnel, which step is missing from the configuration to pass traffic through tunnel on Router 1?

A. static route to 10.0.3.0/24 via 10.0.1.1
B. static route to 10.0.3.0/24 via 10.0.2.1
C. static route to 10.0.3.0/24 via 190.0.4.1
D. static route to 10.0.3.0/24 via 190.0.4.2

Answer: D

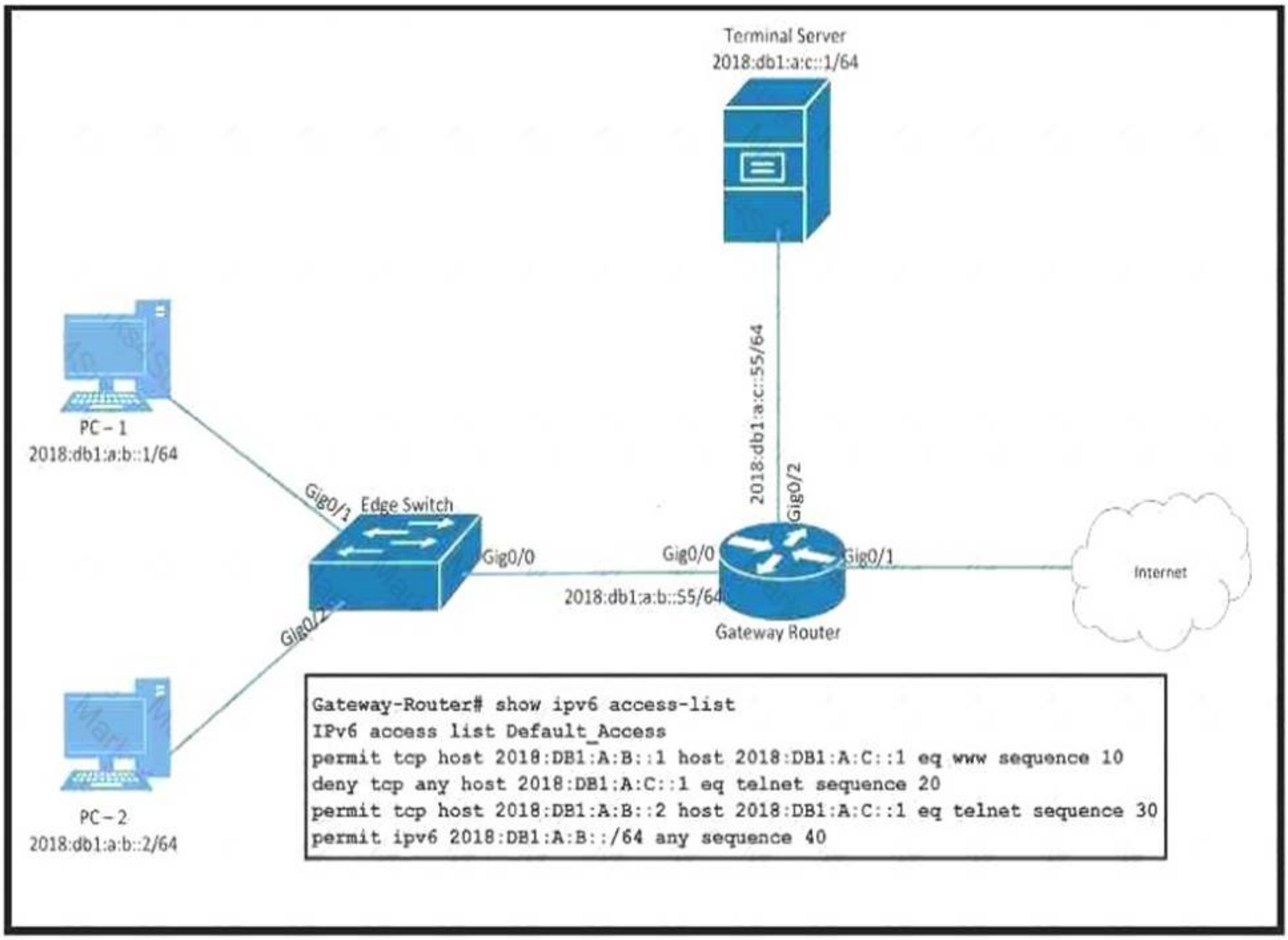
NEW QUESTION 63
In which standard troubleshooting methodology do you start in the middle of the OSI model stack, then move up or down the stack based on your findings?

A. follow the path
B. bottom up
C. divide and conquer
D. move the problem

Answer: C

NEW QUESTION 65

Refer to the exhibit.



PC-2 failed to establish a Telnet connection to the Terminal Server Which solution allows PC-2 to establish the Telnet connection?

A)
```
Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#no sequence 20
Gateway-Router(config-ipv6-acl)#sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
```

B)
```
Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
```

C)
```
Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
```

D)
```
Gateway-Router(config)#ipv6 access-list Default_Access
Gateway-Router(config-ipv6-acl)#sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet
```

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

Answer: A

NEW QUESTION 67
R1 and R2 are directly connected using interface Ethernet0/0 on both sides. R1 and R2 were not becoming adjacent, so you have just configured R2 interface Ethernet0/0 as network type broadcast. Which two statements are true?

A. Three OSPF routers are in the network segment connected to 192.168.1.0/24
B. R1 installs a route to 2.2.2.2/32 as O.
C. R2 is not an OSPF ABR.
D. R1 interface Ethernet0/0 is configured as OSPF type point to point.

E. R1 installs a route to 2.2.2.2/32 as O IA.
F. both routers R1 and R2 are neighbors and R2 IS BDR.

Answer: EF

Explanation: -For the Answer 5 "R1 installs a route to 2.2.2.2/32 as O IA":
That because the route 2.2.2.2/32 belong to another area (area1).
-for the Answer 6 "both routers R1 and R2 are neighbors, and R2 IS BDR":
Here clearly the question, say that R1 and R2 are not adjacent, but that not mean they are not neighbors, from the output of "show ip ospf neighbor" command we can see clearly that routers R1 and R2 are neighbors, and actually the R2 is BDR.
There different between adjacent and neighbor, neighbors" and "adjacent". Two terminologies that doesn't mean the same thing, but can often be misused in a discussion. Neighbors in this case means "show up as neighbors while using the show ip ospf neighbors command". While "adjacent" means they are fully exchanging topology information.
For further information check the links below: https://learningnetwork.cisco.com/message/564573#564573 http://blog.ine.com/2008/01/08/understanding-ospf-network-types/

NEW QUESTION 72
When troubleshooting recursive routing issues with GRE tunnels, which three actions resolve the issue? (Choose 3)

A. Remove the configuration on the tunnel interface and reconfigure
B. Perform shut and no shut commands on the tunnel interface.
C. Add static routes for the tunnel source and destination
D. Remove the network advertisements from the routing protocols.
E. Change the tunnel source or destination interface.
F. If using OSPF to peer across the tunnel use EIGRP instead

Answer: CDE

NEW QUESTION 74
Which two statements about GRE tunnel keepalives are true? (Choose two)

A. They are supported in point-to-point GRE tunnels.
B. They are supported in multipoint GRE tunnels.
C. They are supported in VRFs only if the fVRF and iVRF match.
D. They are supported with IPsec tunnel protection.
E. They are enabled by default.

Answer: AD

NEW QUESTION 77
Which protocol does mGRE use to determine where packets are sent?

A. CEF
B. EIGRP
C. NHRP
D. DMVPN

Answer: A

Explanation: Reference:
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html

NEW QUESTION 82

```
SW3#sho run | sec vty
line vty 0 4
access-class 100 in
login
transport input ssh

SW3sho access-list
Extended IP access list 100
10 deny tcp any any eq 22
20 permit ip any any
Extended IP access list 150
10 permit tcp any any eq telnet
20 deny tcp any any eq 22
30 permit ip any any
Extended IP access list 175
10 permit tcp any any eq 22
20 permit tcp any any eq telnet
```

Refer to the exhibit. Your company security policy states you must use SSH on your network devices. Your attempt to SSH into SW3 is unsuccessful. What action must you take to correct the issue?

A. Change access-class 100 in to access-class 175 in.
B. Change access-class 100 in to access-class 150 in.
C. Change access-class 100 in to access-class 100 out.
D. Change transport inut ssh to transport input telnet

Answer: A

NEW QUESTION 86
Which statement is true about an IPsec/GRE tunnel?

A. The GRE tunnel source and destination addresses are specified within the IPsec transform set.
B. An IPsec/GRE tunnel must use IPsec tunnel mode.
C. GRE encapsulation occurs before the IPsec encryption process.
D. Crypto map ACL is not needed to match which traffic will be protected.

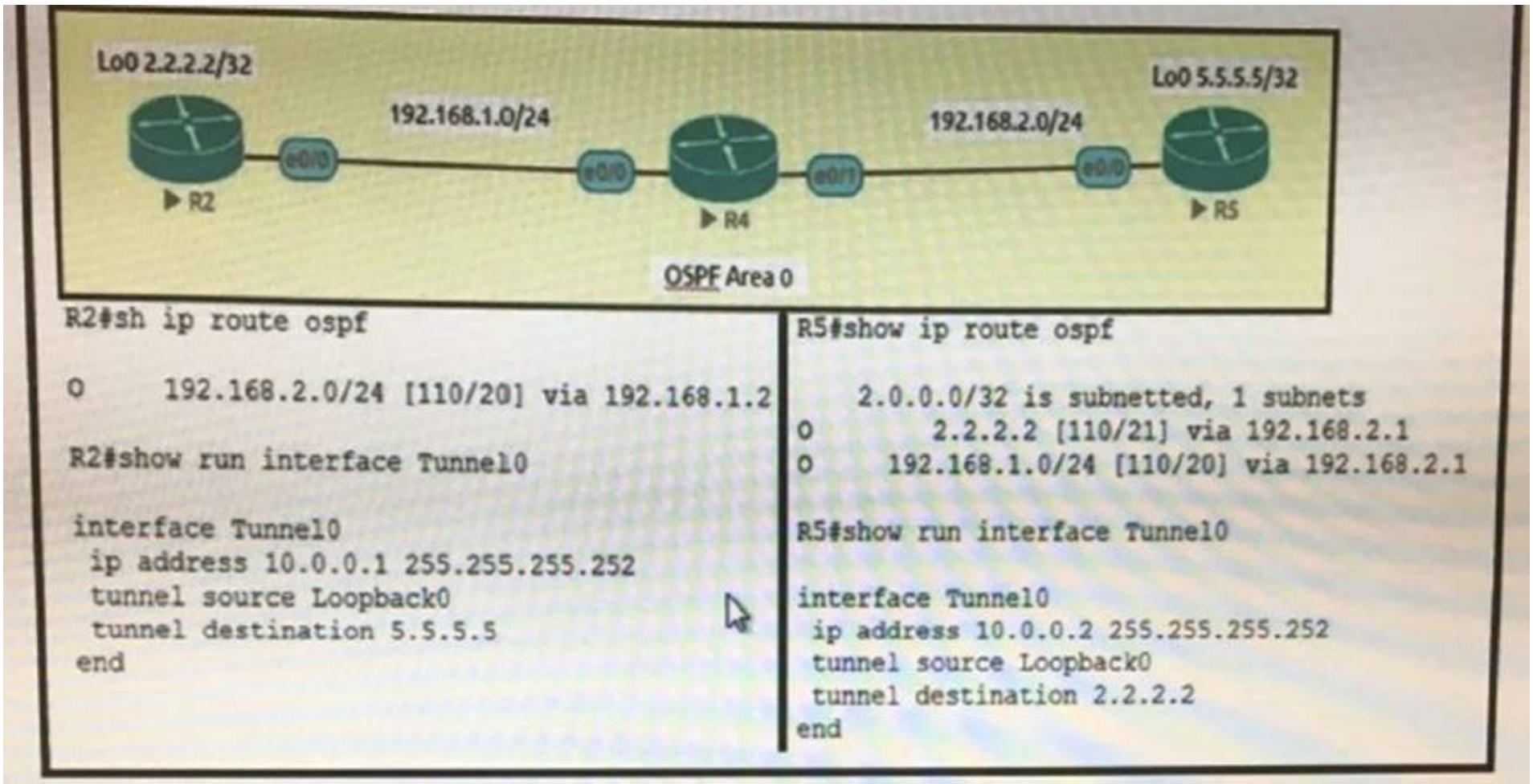
Answer: C

NEW QUESTION 87
Which three features are benefits of using GRE tunnels in conjunction with IPsec for building site-to-site VPNs? (Choose three.)

A. allows dynamic routing over the tunnel
B. supports multi-protocol (non-IP) traffic over the tunnel
C. reduces IPsec headers overhead since tunnel mode is used
D. simplifies the ACL used in the crypto map
E. uses Virtual Tunnel Interface (VTI) to simplify the IPsec VPN configuration

Answer: ABD

NEW QUESTION 90
Refer to exhibit.



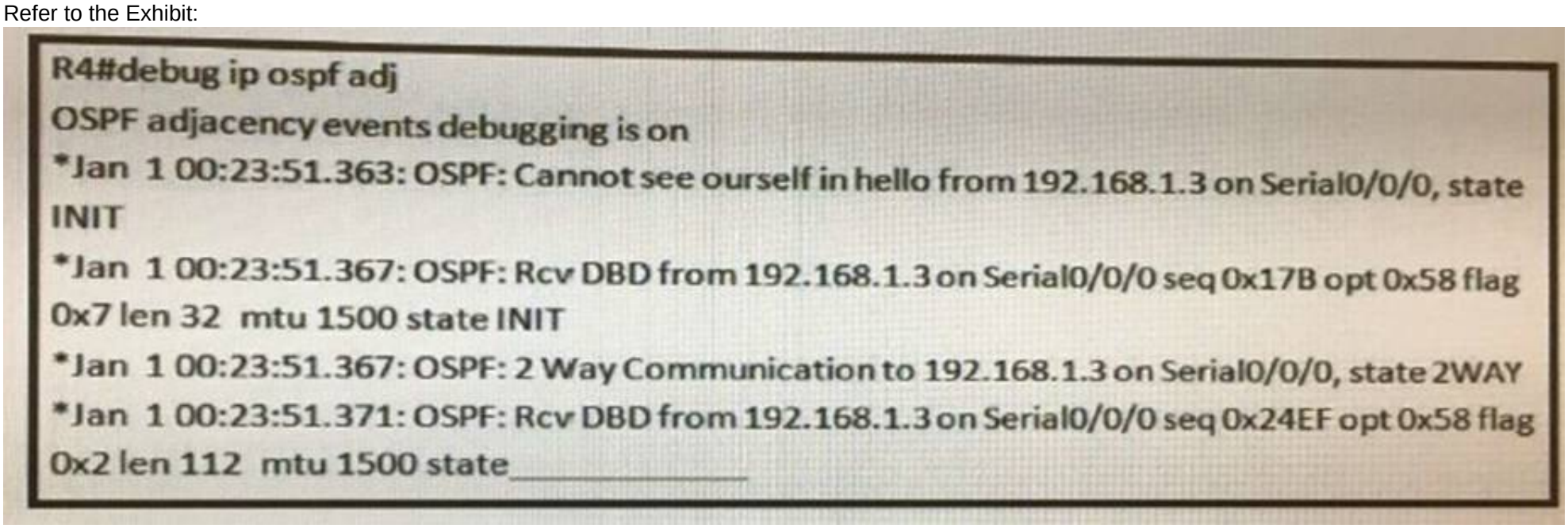
The tunnel between R2 and R5 is not coming up. R2, R4 and R5 do not have any routing information sources other than OSPF and no route filtering is implemented anywhere in the network. Which two actions fix the issue? (Choose Two)

A. Redistribute connected routes to OSPF on R5.
B. Change the tunnel destination on R2 to 192.168.2.1
C. Advertise interface Lo0 to OSPF on R5.
D. Configure a static route on R5 to 2.2.2.2 via 192.168.2.1
E. Fix the OSPF adjacency issue between R2 and r5.

Answer: AC

Explanation: In order for the tunnel to be established between R2-R5 ,the R2 should have a path for the 5.5.5.5/32 route in its own routing table , and because the ospf is the only routing protocol here , so R5 has to advertise the route 5.5.5.5/32, and that is possible through these option:
1- redistribute connected route to ospf on R5 2-Advertise interface lo0 to OSPF on R5
For knowing more about the rules for the gre channel to be established, check the link below:
http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html

NEW QUESTION 91
Refer to the Exhibit:

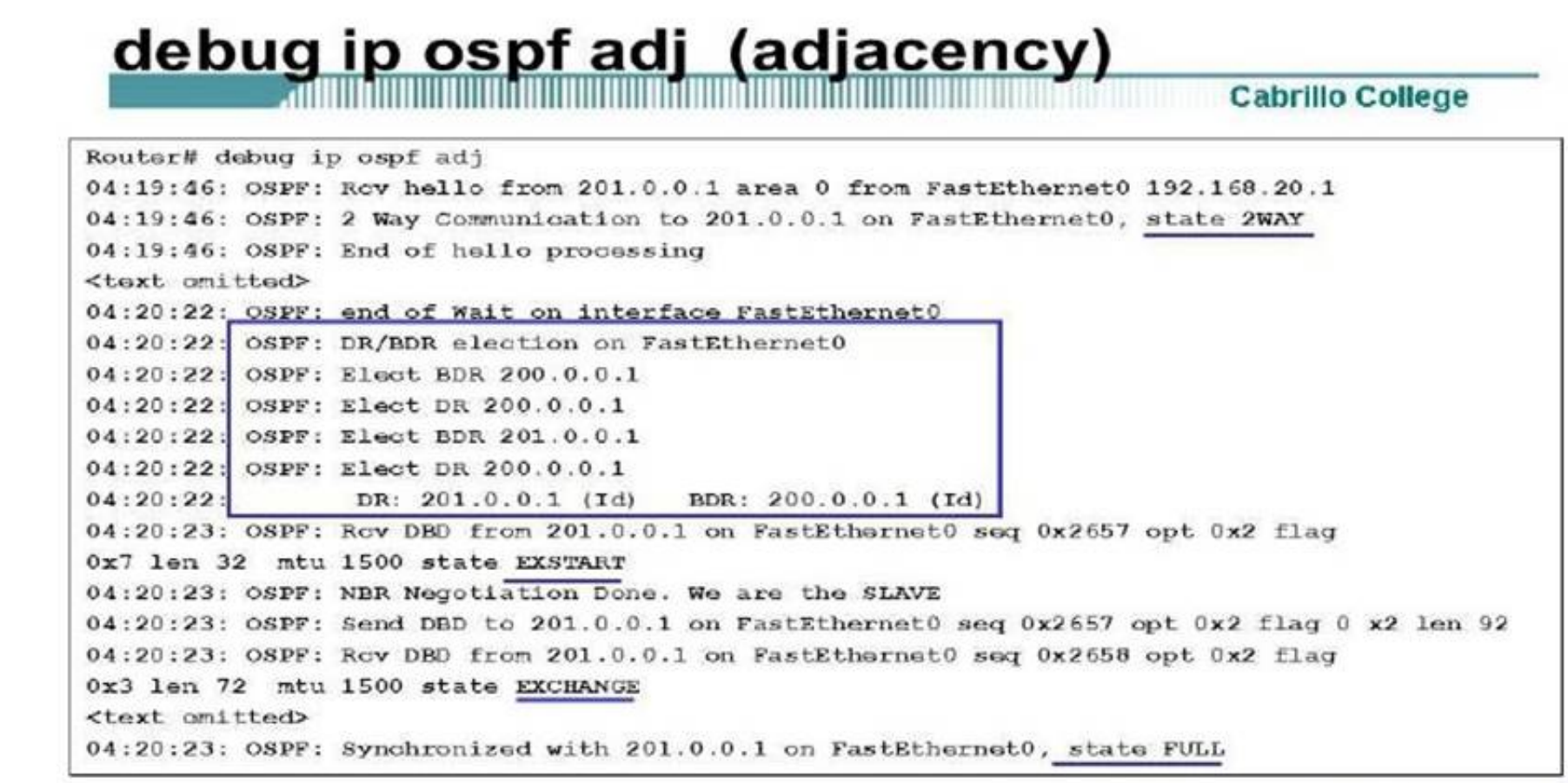


Which output is expected in the blank line for the OSPF adjacency process?

A. DOWN
B. EXSTART
C. EXCHANGE
D. LOADING

Answer: B

Explanation: You can check the output of "debug ip ospf adj" here:



NEW QUESTION 93
Refer to exhibit.

If all routers are sharing routes via OSPF area 0, which two configuration can you apply to R2 and R3 so that they can enable a GRE tunnel between them? (Choose two)

A. R2#interface tunnel 0 Description To HQ-A316:56369Ip address 10.10.23.2.255.255.255.0Tunnel source GigabitEthernet0/0 Tunnel destination 192.168.13.3
B. R3#interface tunnel 0 Description To HQ-B652:4289Ip address 10.10.23.2.255.255.255.0Tunnel source GigabitEthernet0/0 Tunnel destination 192.168.21.2
C. R2#interface tunnel 0 Description To HQ-A316:56369Ip address 10.10.23.2.255.255.255.0Tunnel source GigabitEthernet0/1 Tunnel destination 192.168.131
D. R2#interface tunnel 0 Description To HQ-A316:56369Ip address 10.10.23.2.255.255.255.0Tunnel source 192.168.21.2Tunnel destination 192.168.13.3
E. R3#interface tunnel 0 Description To HQ-B652:4289Ip address 10.10.23.3.255.255.255.0Tunnel source GigabitEthernet0/0 Tunnel destination 192.168.13.3

Answer: BD

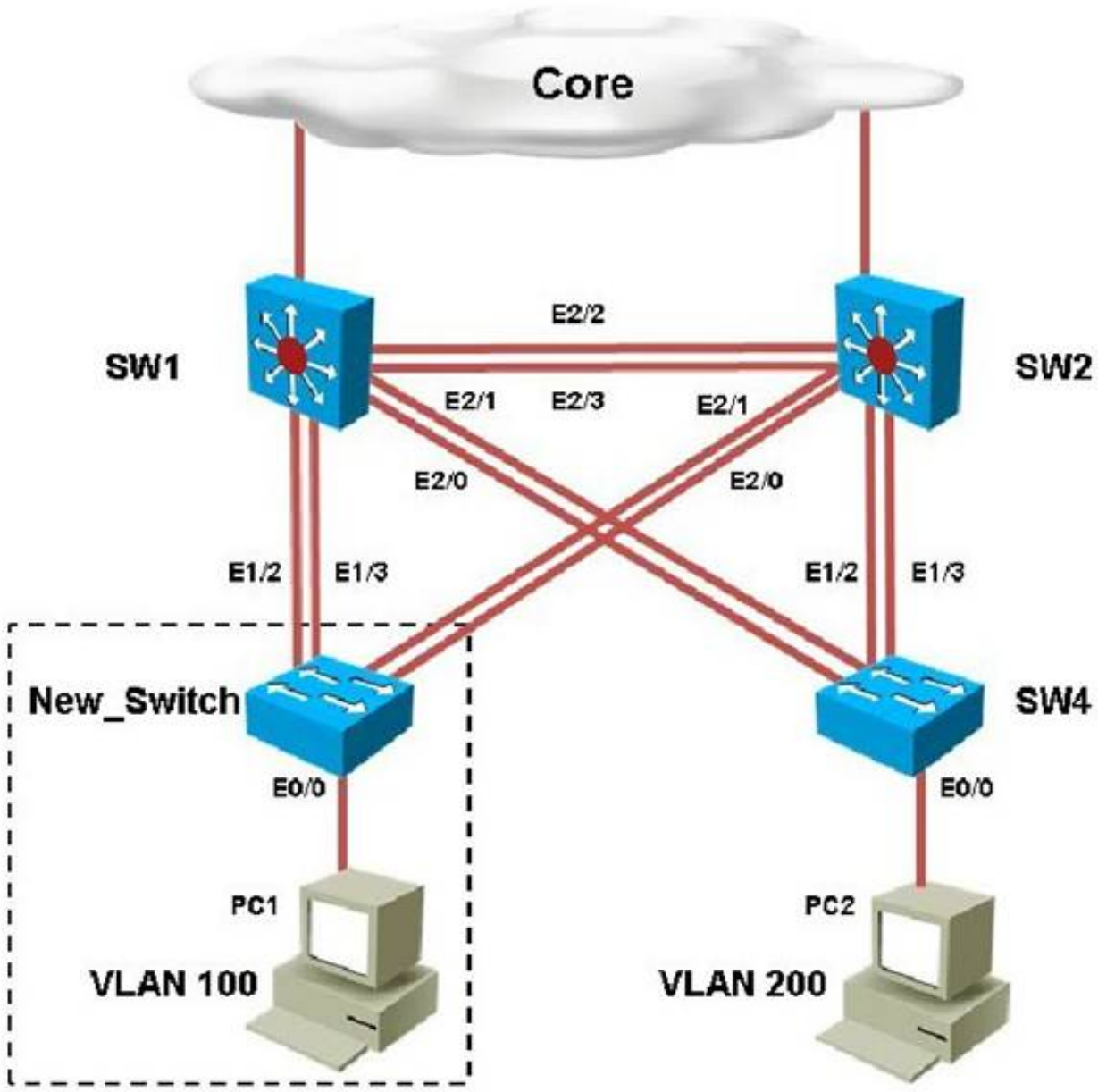
NEW QUESTION 94
You want to troubleshoot a GRE tunnel that is configured with an ACL. Which two tasks must you perform? (Choose two)

A. Verify that the ACL permits TCP port 8080
B. A Verify that the ACL permits IP protocol 47.
C. Verity that the remote device is reachable across the network
D. Verify that the IP addresses of the physical interfaces are on the same subnet
E. Verify that the ACL permits TCP port 1723.

Answer: BC

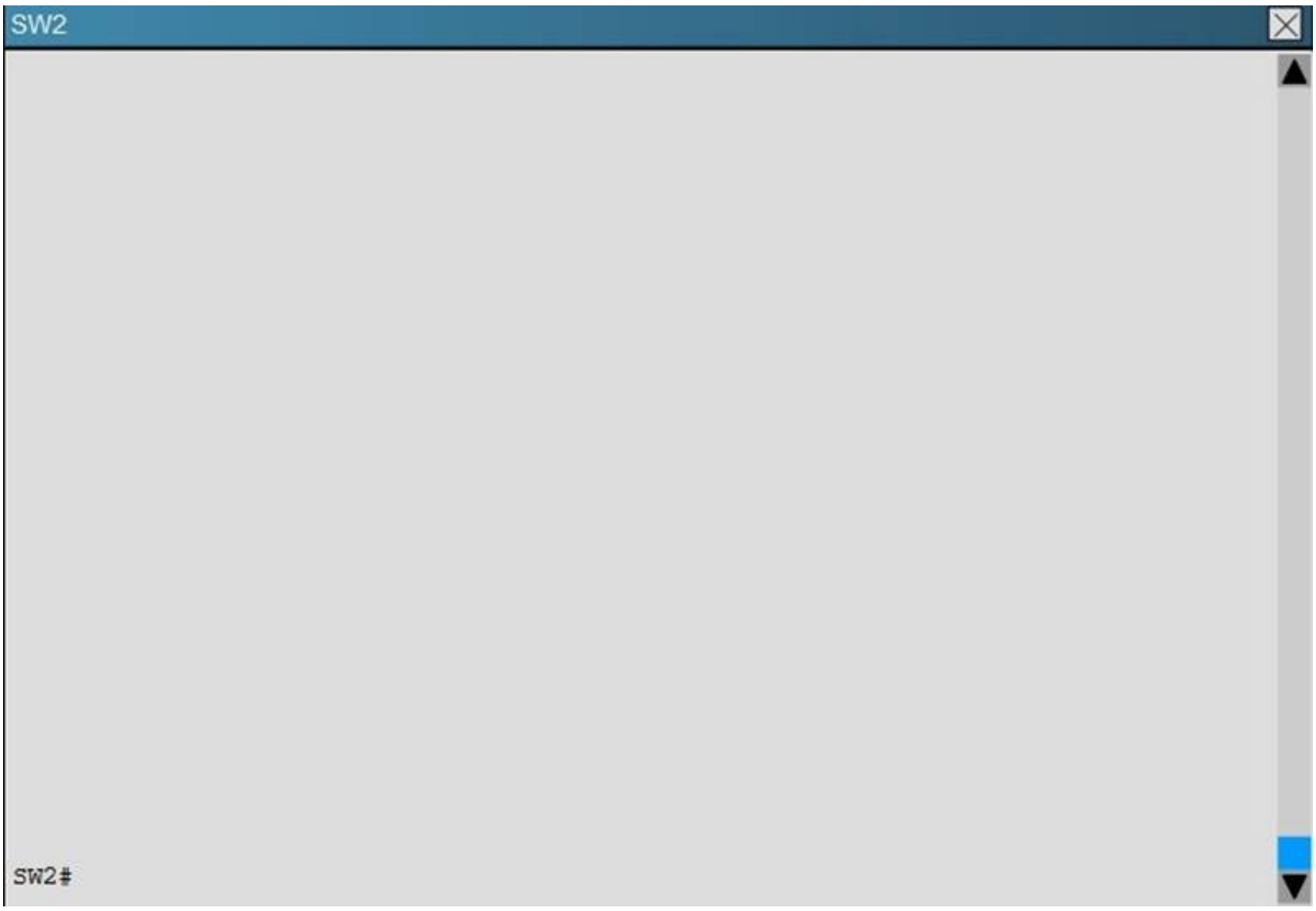
Explanation: Topic 2, Troubleshooting VTP

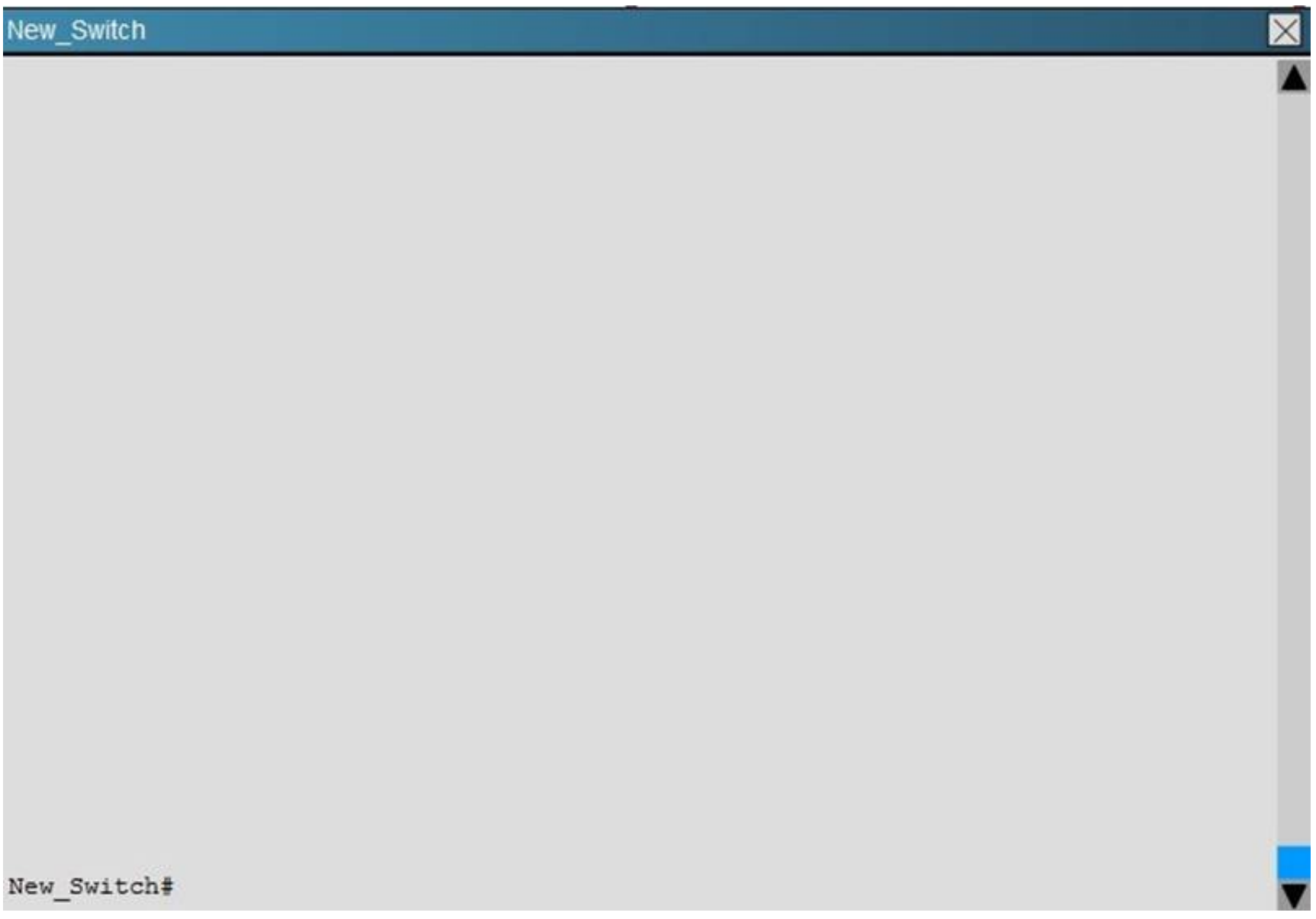
NEW QUESTION 98
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.

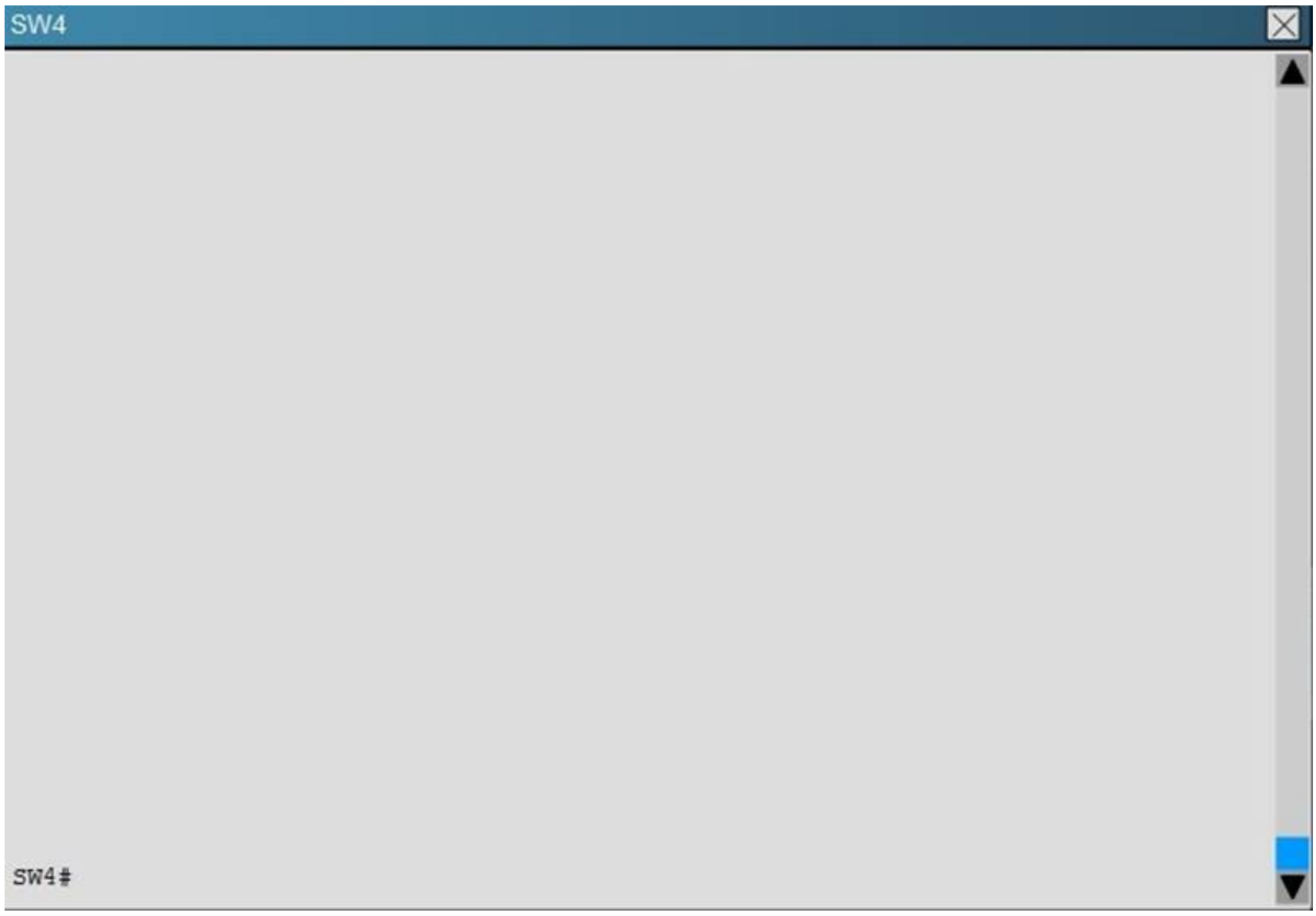

Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
VLAN 100
PC2
VLAN 200

SW1

SW1#


SW2
SW2#


New_Switch
New_Switch#

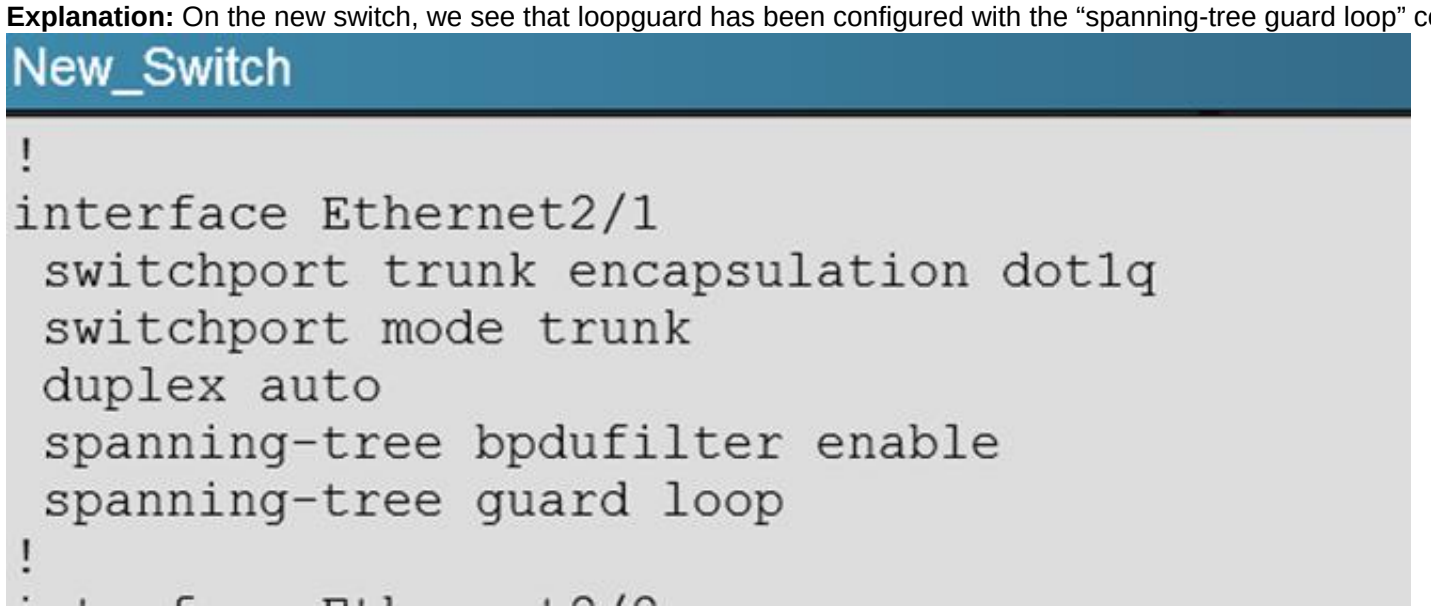


Which of statement is true regarding STP issue identified with switches in the given topology?

A. Loopguard configured on the New_Switch places the ports in loop inconsistent state
B. Rootguard configured on SW1 places the ports in root inconsistent state
C. Bpduguard configured on the New_Switch places the access ports in error-disable
D. Rootguard configured on SW2 places the ports in root inconsistent state

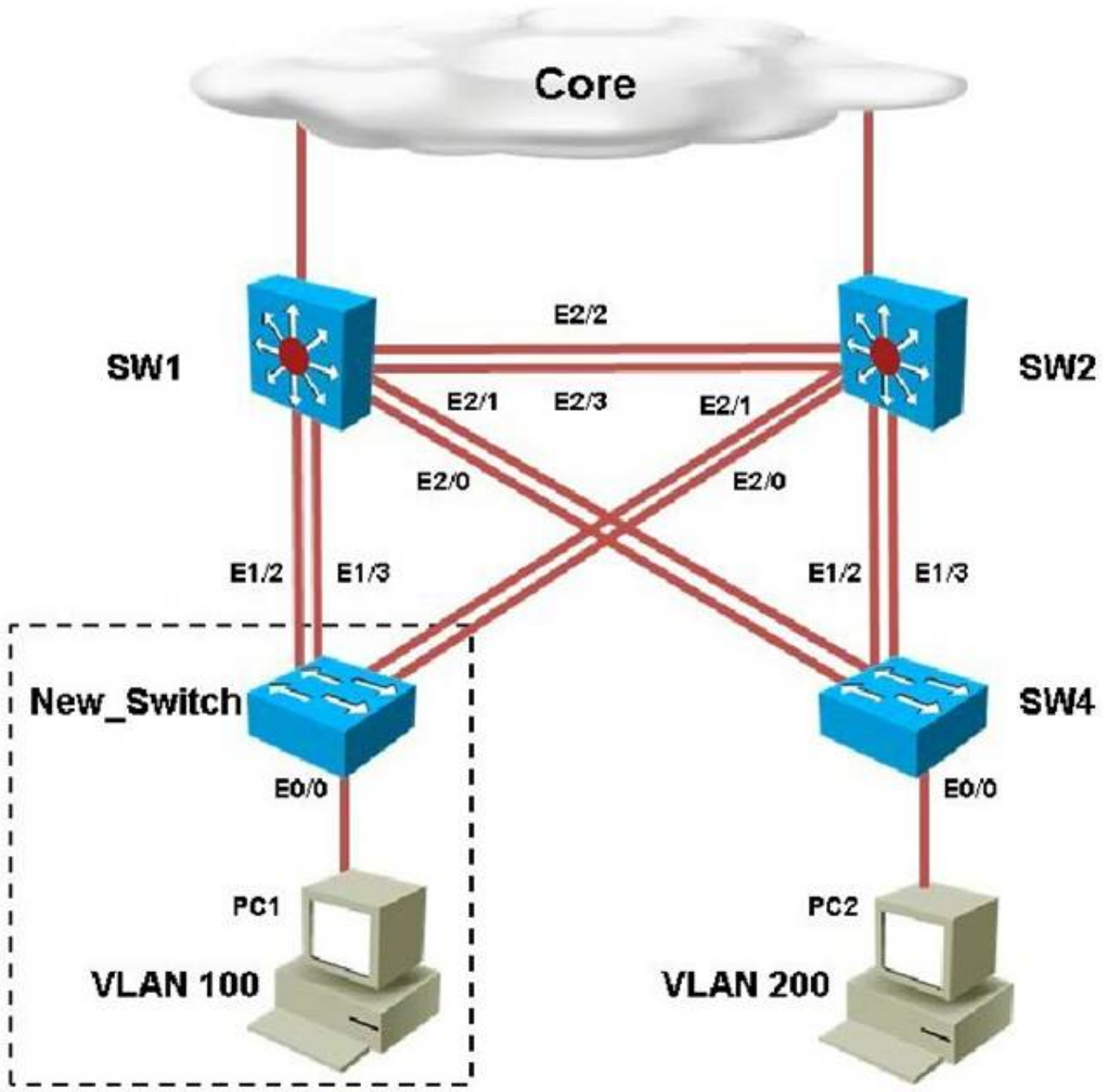
Answer: A

Explanation: On the new switch, we see that loopguard has been configured with the “spanning-tree guard loop” command.

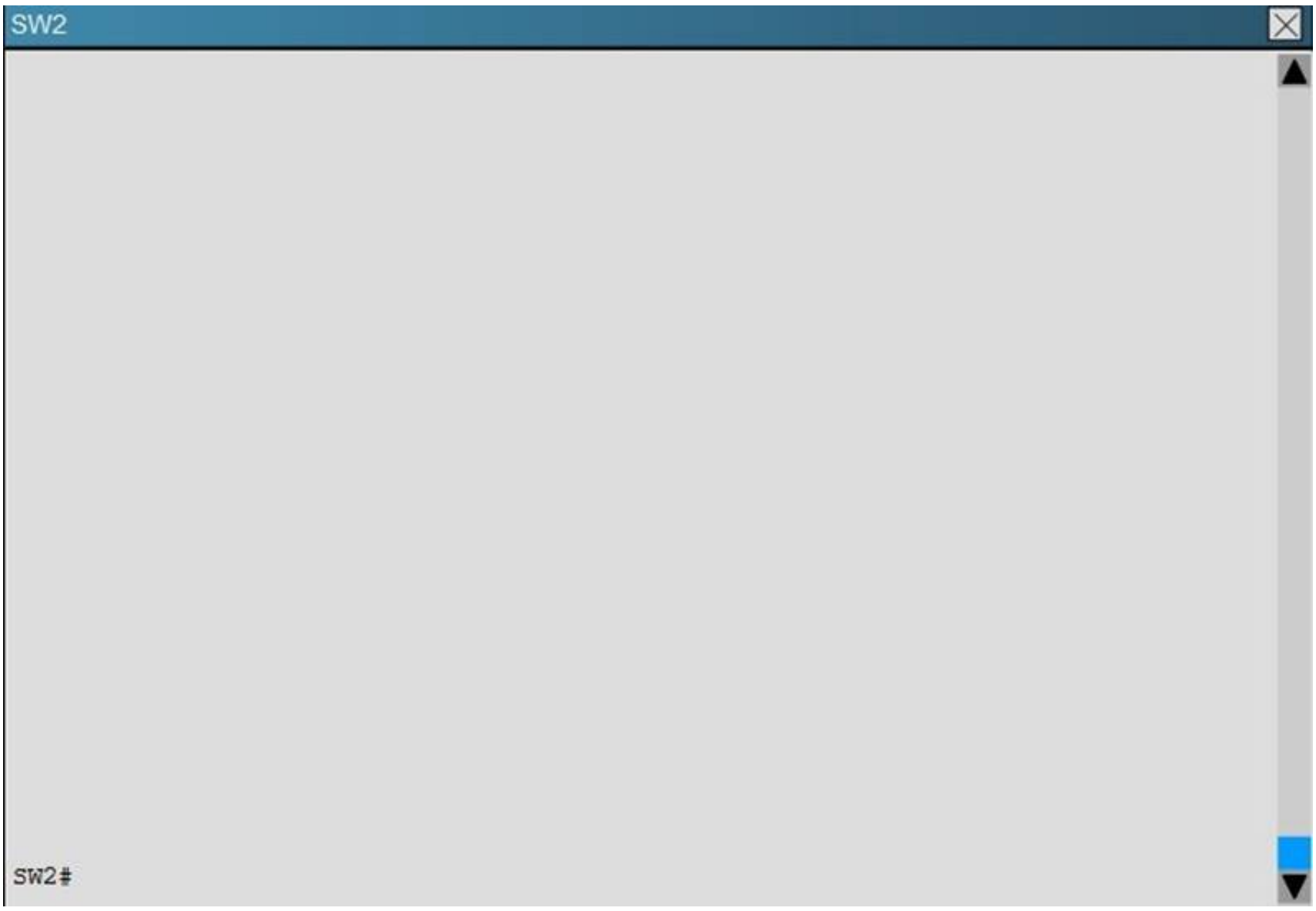


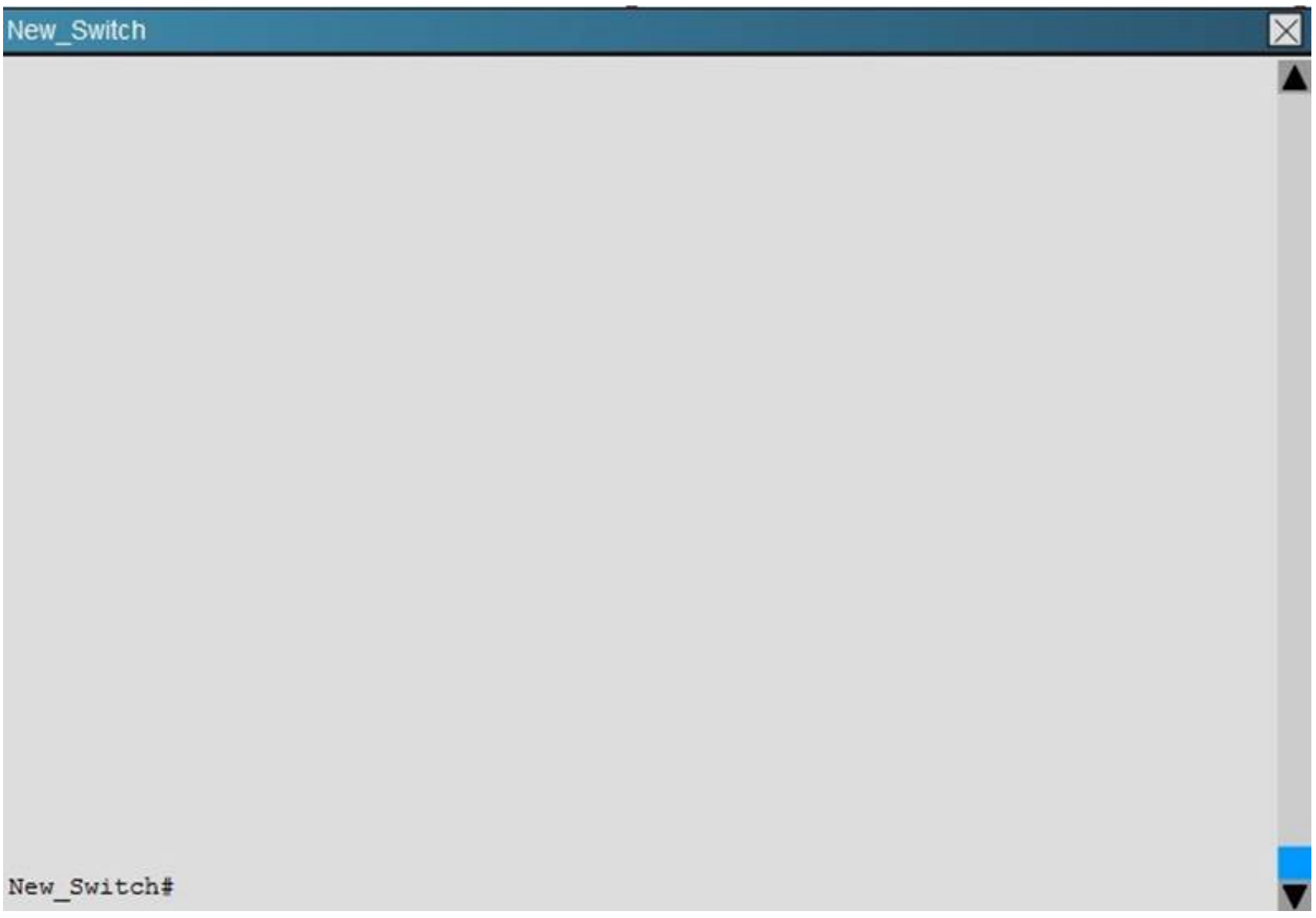
The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.

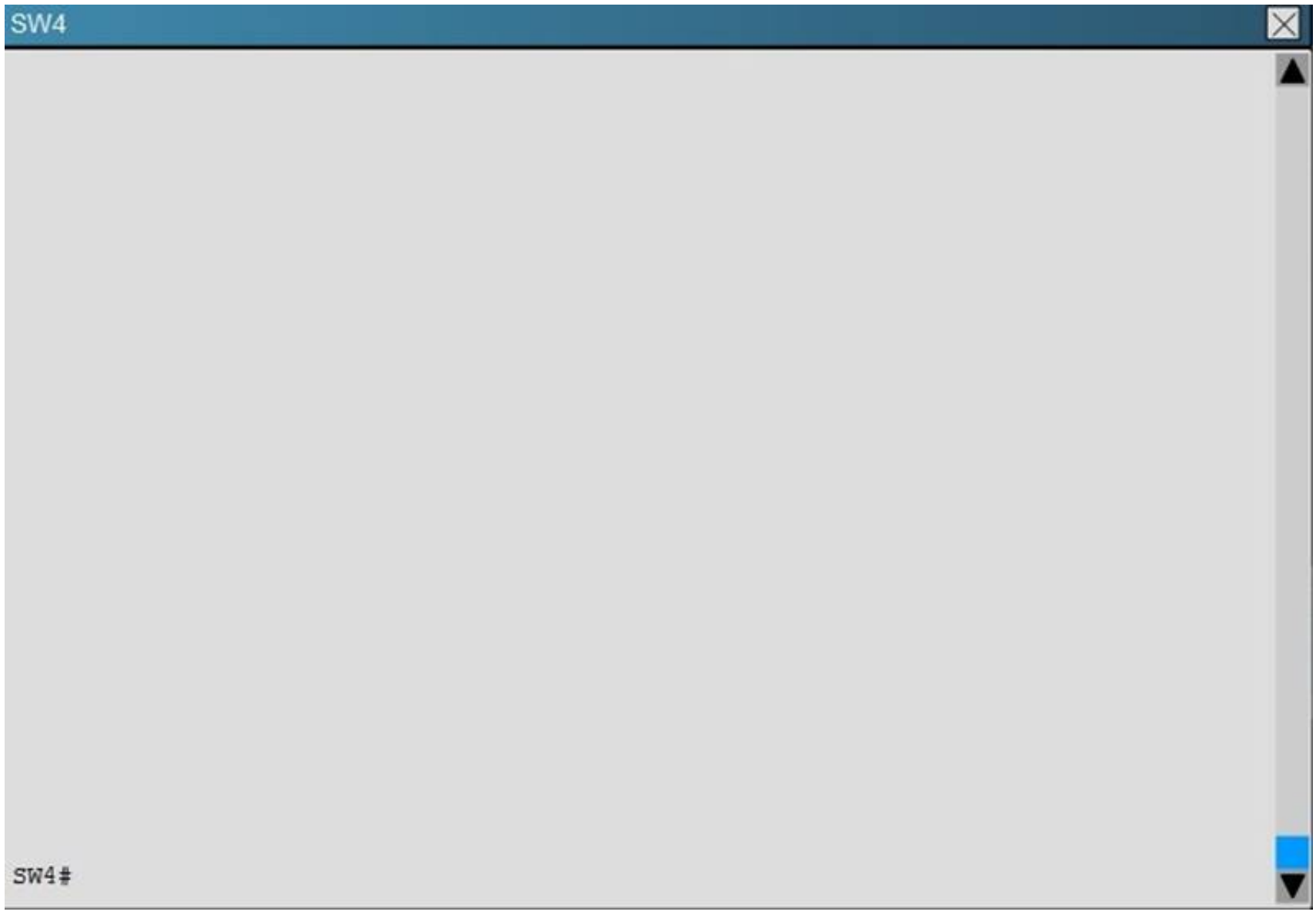
NEW QUESTION 101
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.


Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200


SW1
SW1#


SW2
SW2#


New_Switch
New_Switch#



Refer to the topology.
SW1 Switch Management IP address is not pingable from SW4. What could be the issue?

A. Management VLAN not allowed in the trunk links between SW1 and SW4
B. Management VLAN not allowed in the trunk links between SW1 and SW2
C. Management VLAN not allowed in the trunk link between SW2 and SW4
D. Management VLAN ip address on SW4 is configured in wrong subnet
E. Management VLAN interface is shutdown on SW4

Answer: D

Explanation: In the network, VLAN 300 is called the Management VLAN. Based on the configurations shown below, SW1 has VLAN 300 configured with the IP address of 192.168.10.1/24, while on SW4 VLAN 300 has an IP address of 192.168.100.4/24, which is not in the same subnet.

SW1

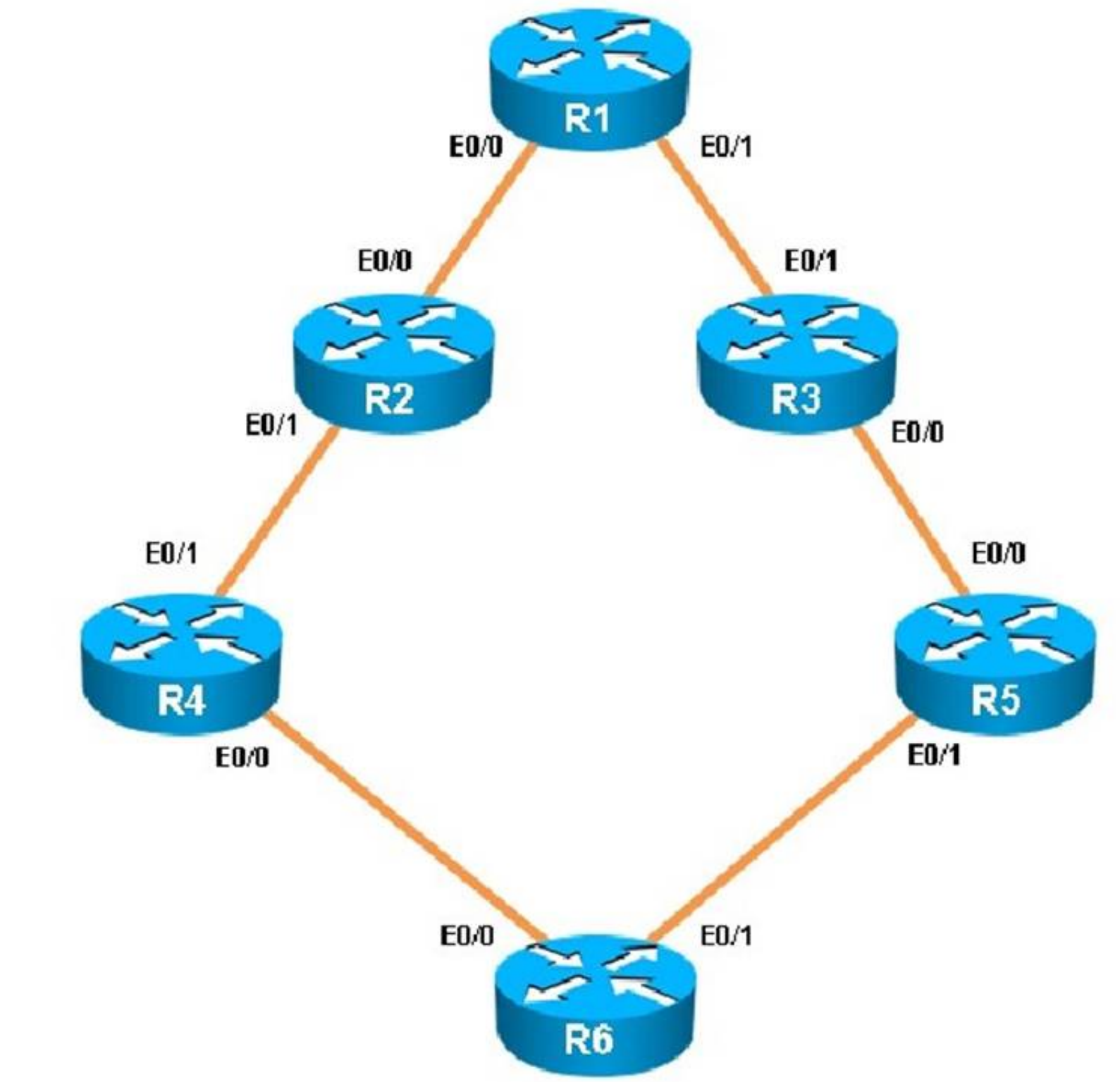
```
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 172.16.100.1 255.255.255.0
!
interface Vlan200
 ip address 172.16.200.1 255.255.255.0
!
interface Vlan300
 ip address 192.168.10.1 255.255.255.0
!
```

SW4

```
 switchport mode trunk
 duplex auto
!
interface Ethernet2/2
 shutdown
 duplex auto
!
interface Ethernet2/3
 shutdown
 duplex auto
!
interface Vlan1
 no ip address
!
interface Vlan300
 ip address 192.168.100.4 255.255.255.0
!
!
```

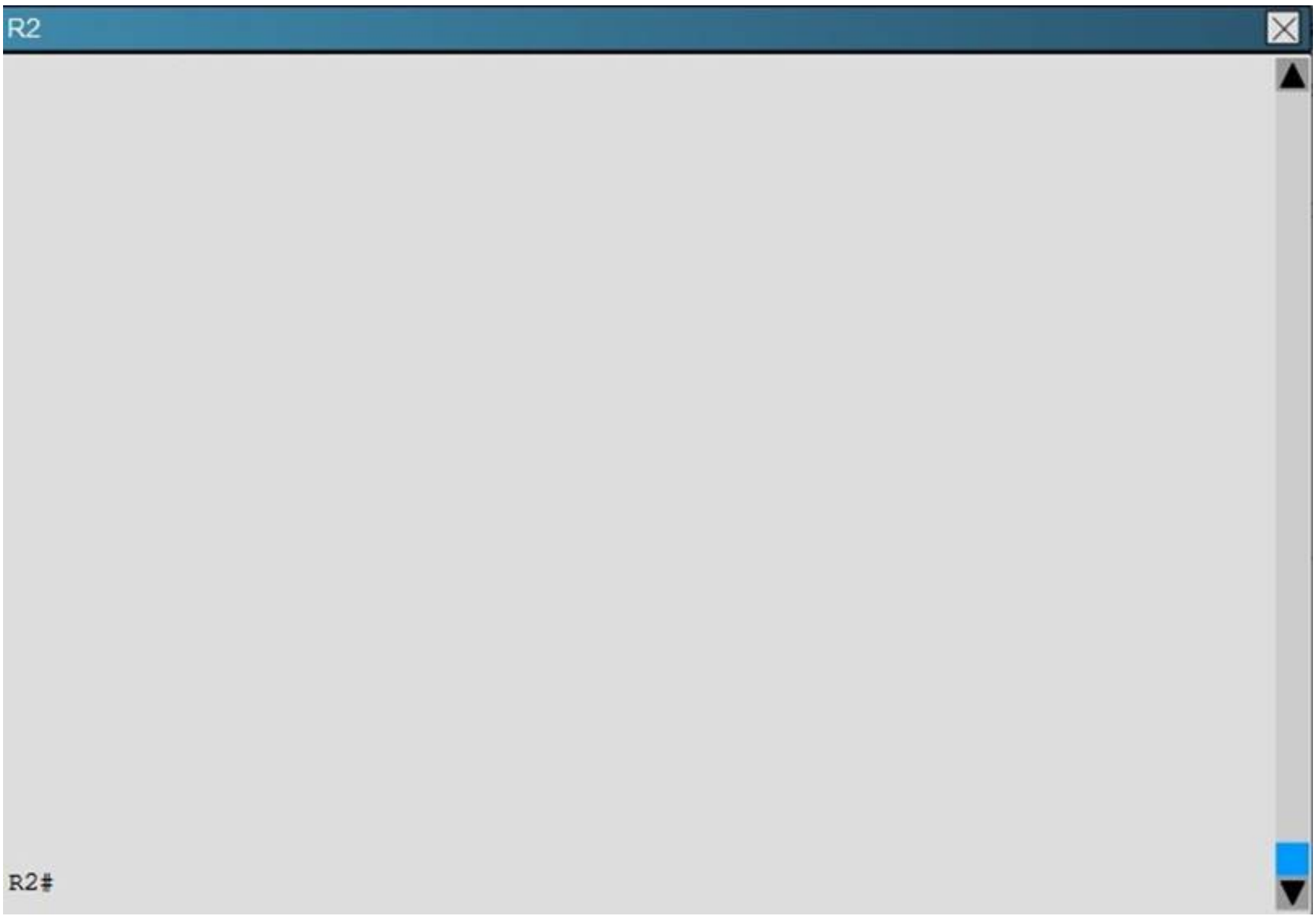
Topic 3, Troubleshooting EIGRP

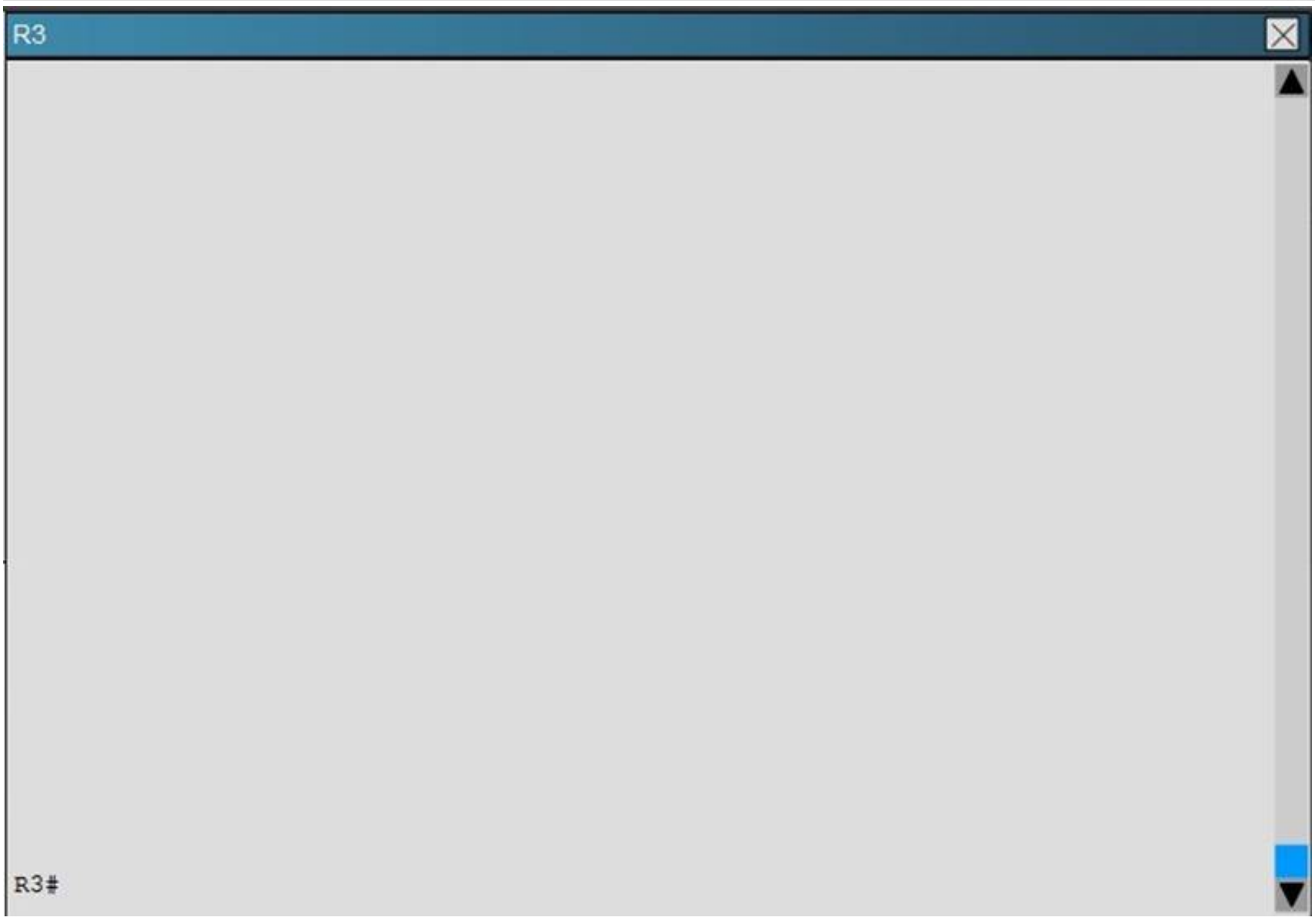
NEW QUESTION 102
Scenario:
You have been brought in to troubleshoot an EIGRP network. You have resolved the initial issue between routers R2 and R4, but another issue remains. You are to locate the problem and suggest solution to resolve the issue.
The customer has disabled access to the show running-config command.

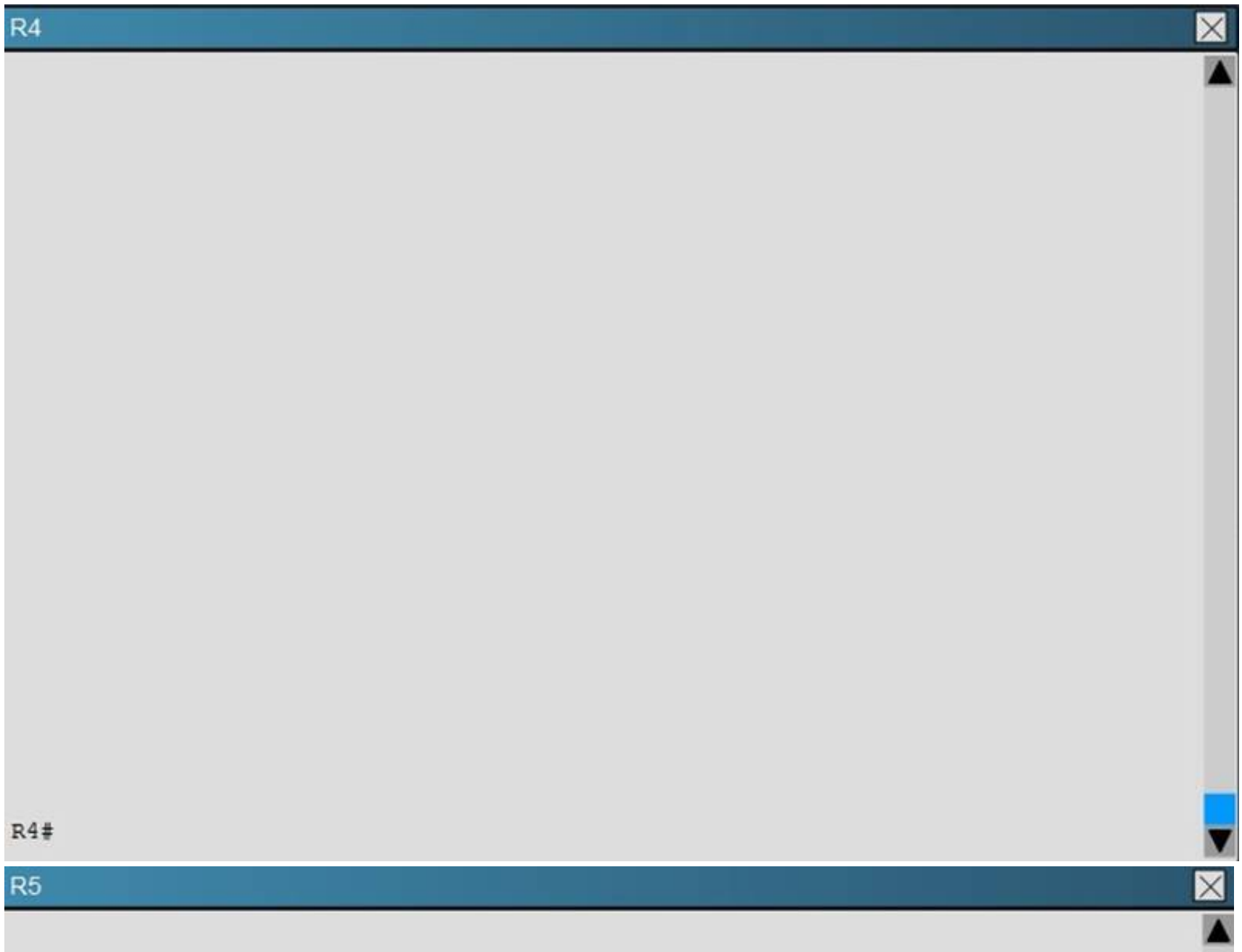


R1

```
R1#
```


R2
R2#


R3
R3#

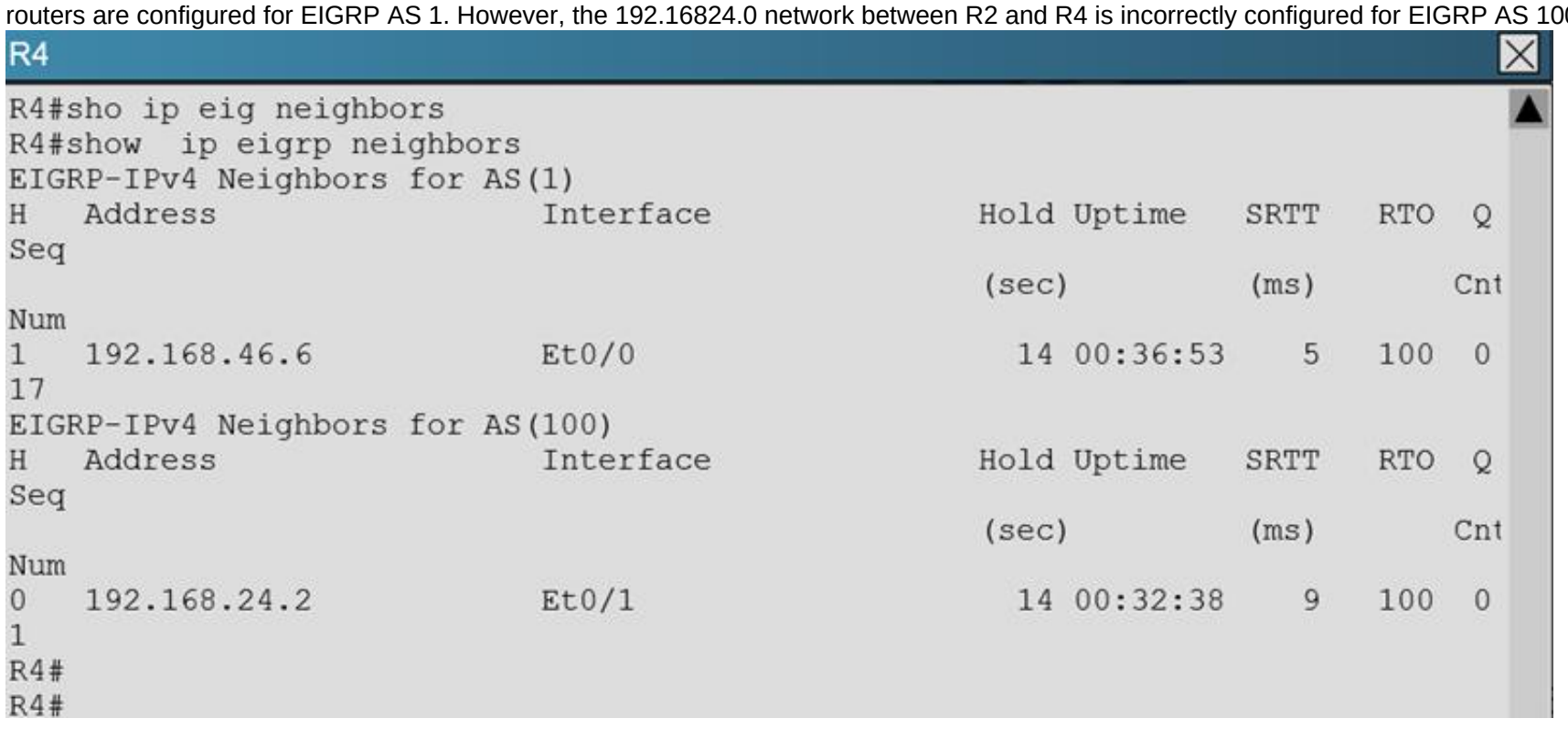

R4
R4#
R5
R5#

The network segment between R2 and R4 has become disconnected from the remainder of the network. How should this issue be resolved?

A. Change the autonomous system number in the remainder of the network to be consistent with R2 and R4.
B. Move the 192.168.24.0 network to the EIGRP 1 routing process in R2 and R4.
C. Enable the R2 and R4 router interfaces connected to the 192.168.24.0 network.
D. Remove the distribute-list command from the EIGRP 200 routing process in R2.
E. Remove the distribute-list command from the EIGRP 100 routing process in R2.

Answer: B

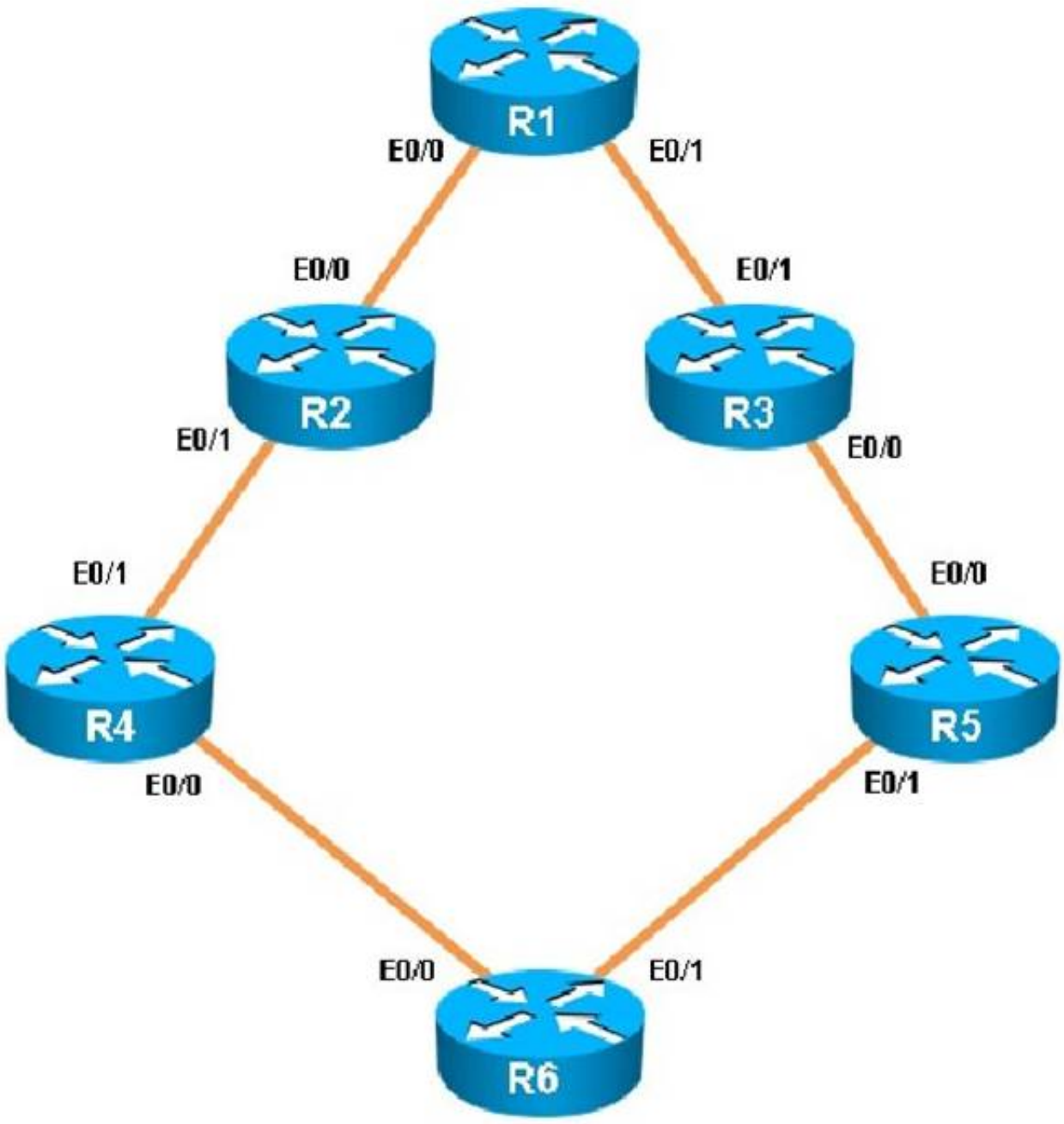
Explanation: When issuing the “show ip eigrp neighbor” command (which is about the only command that it lets you do in this question) you will see that all other routers are configured for EIGRP AS 1. However, the 192.16824.0 network between R2 and R4 is incorrectly configured for EIGRP AS 100:

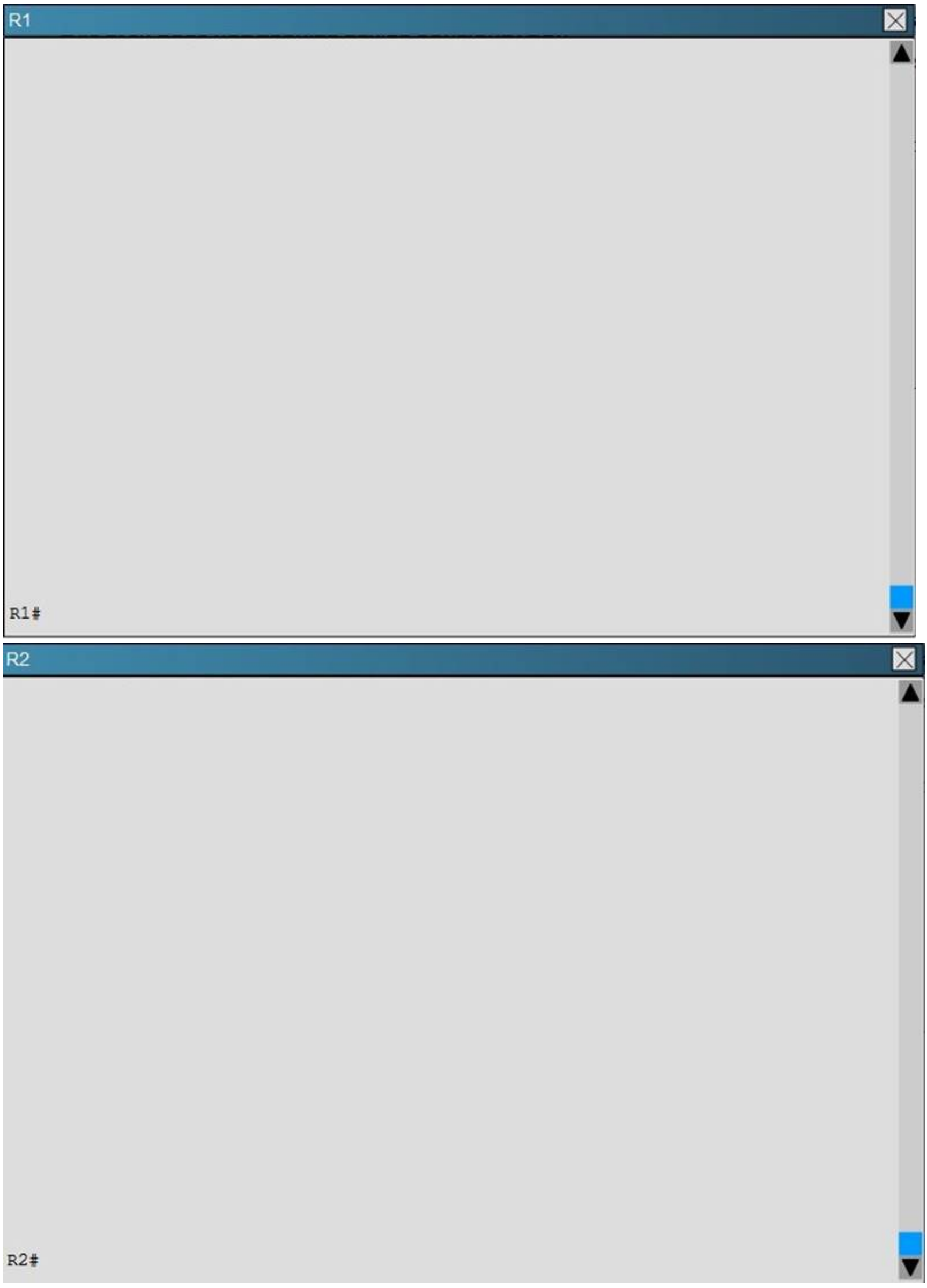


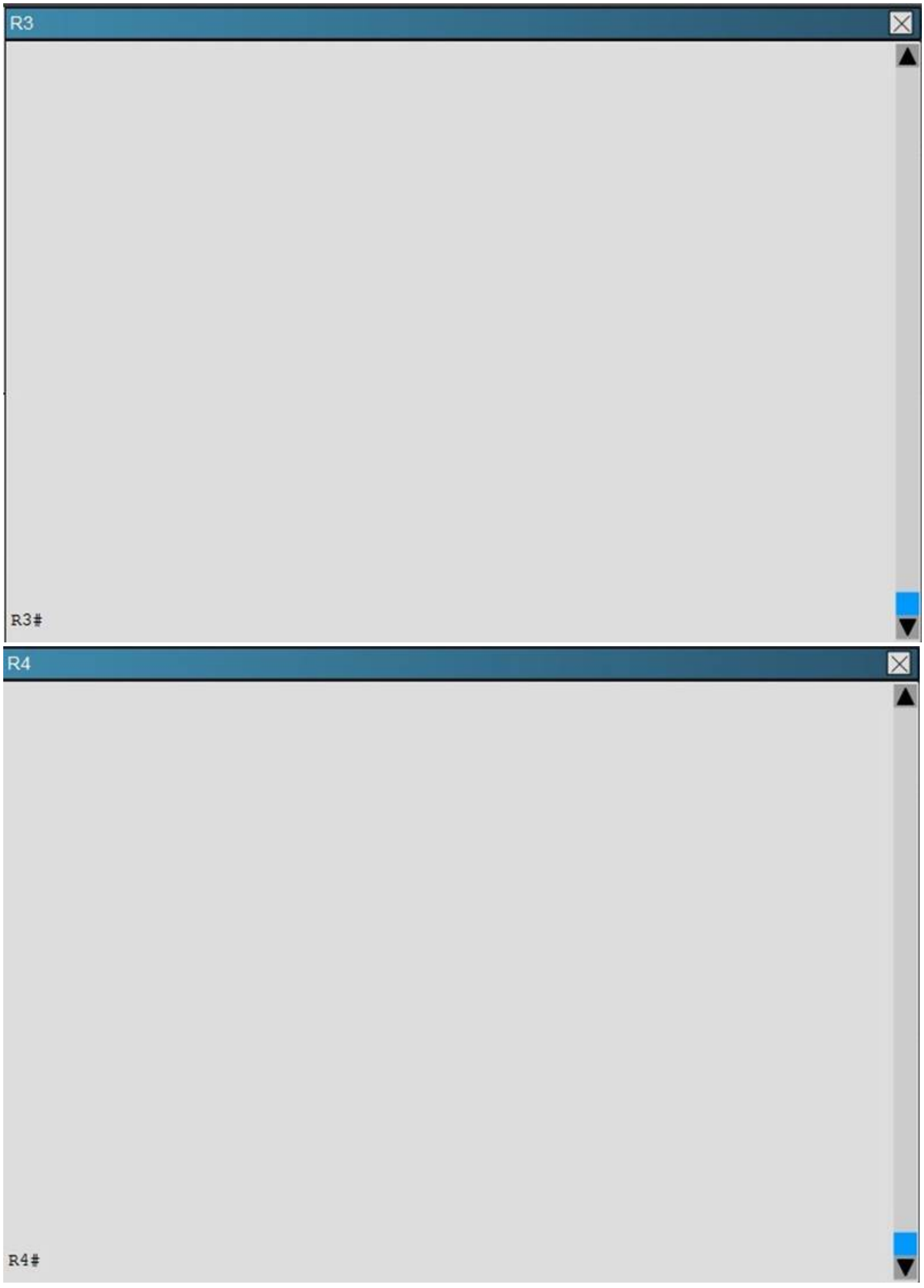
R2

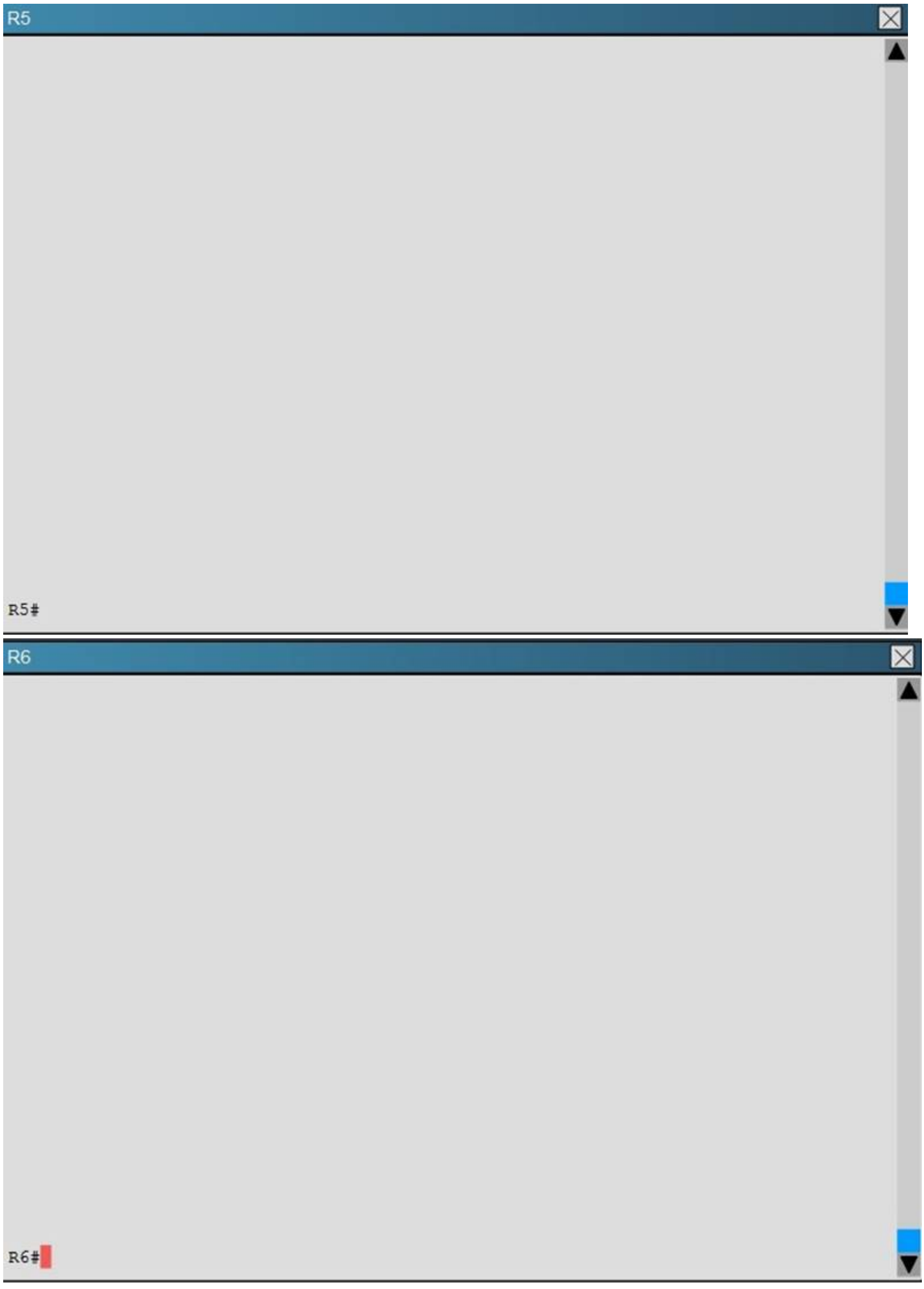
```
R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
0   192.168.12.1            Et0/0                    10 00:28:28    5   100  0
27
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
0   192.168.24.4            Et0/1                    11 00:20:36   16   100  0
1
R2#
```

NEW QUESTION 104
You have been brought in to troubleshoot an EIGRP network. A network engineer has made configuration changes to the network rendering some locations unreachable. You are to locate the problem and suggest solution to resolve the issue.




R1
R1#
R2
R2#


R3
R3#
R4
R4#



R5 has become partially isolated from the remainder of the network. R5 can reach devices on directly connected networks but nothing else. What is causing the problem?

A. An outbound distribute list in R3
B. Inbound distribute lists in R5
C. An outbound distribute list in R6
D. Incorrect EIGRP routing process ID in R5

Answer: B

Explanation: Here we see that distribute list 3 has been applied to EIGRP on router R%, but access-list 3 contains only deny statements so this will effectively block all routing advertisements from its two EIGRP neighbors, thus isolating R5 from the rest of the EIGRP network:

R5

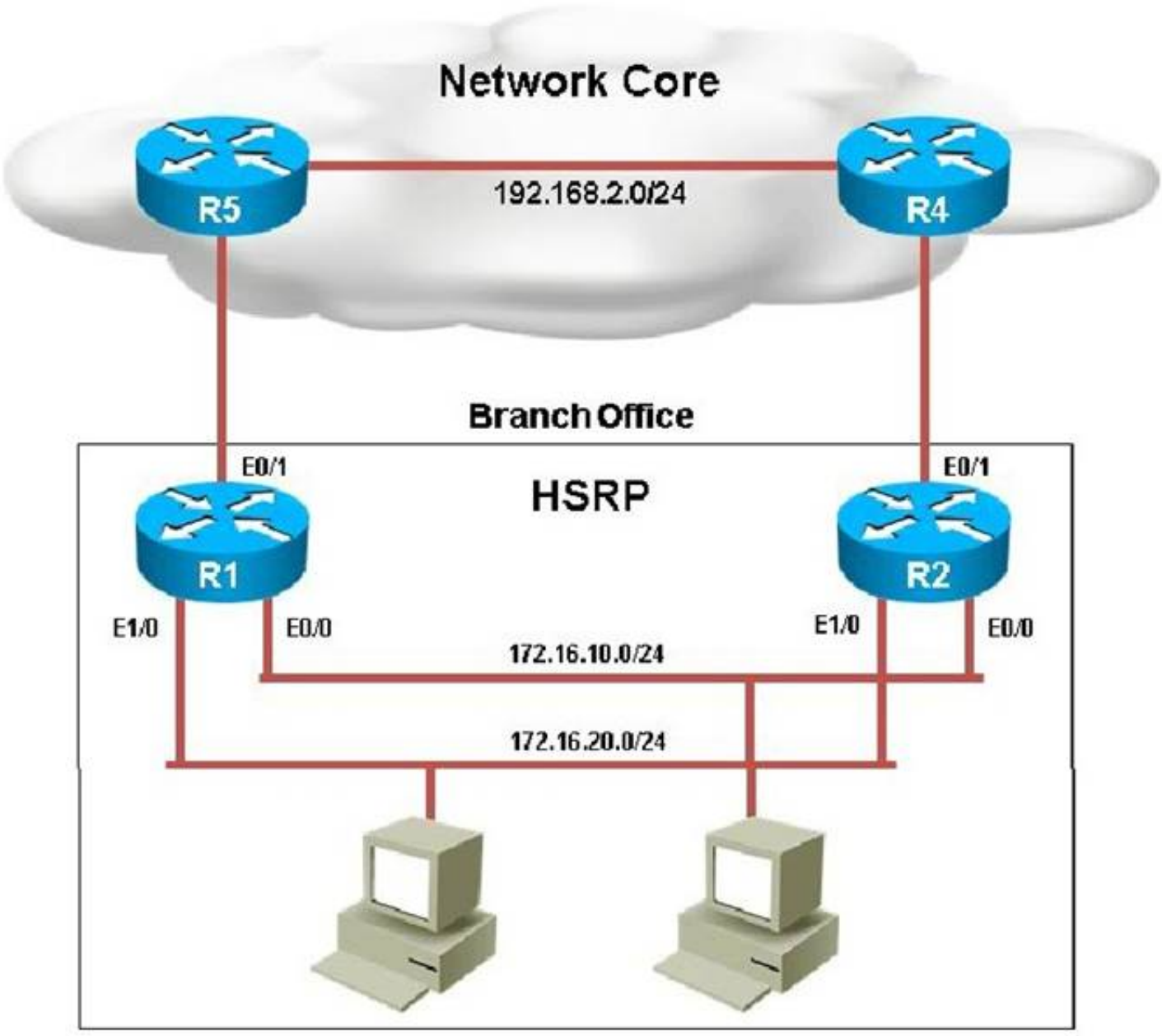
```
!
router eigrp 1
 distribute-list 3 in Ethernet0/0
 distribute-list 3 in Ethernet0/1
 network 192.168.35.0
 network 192.168.56.0
!
!
```

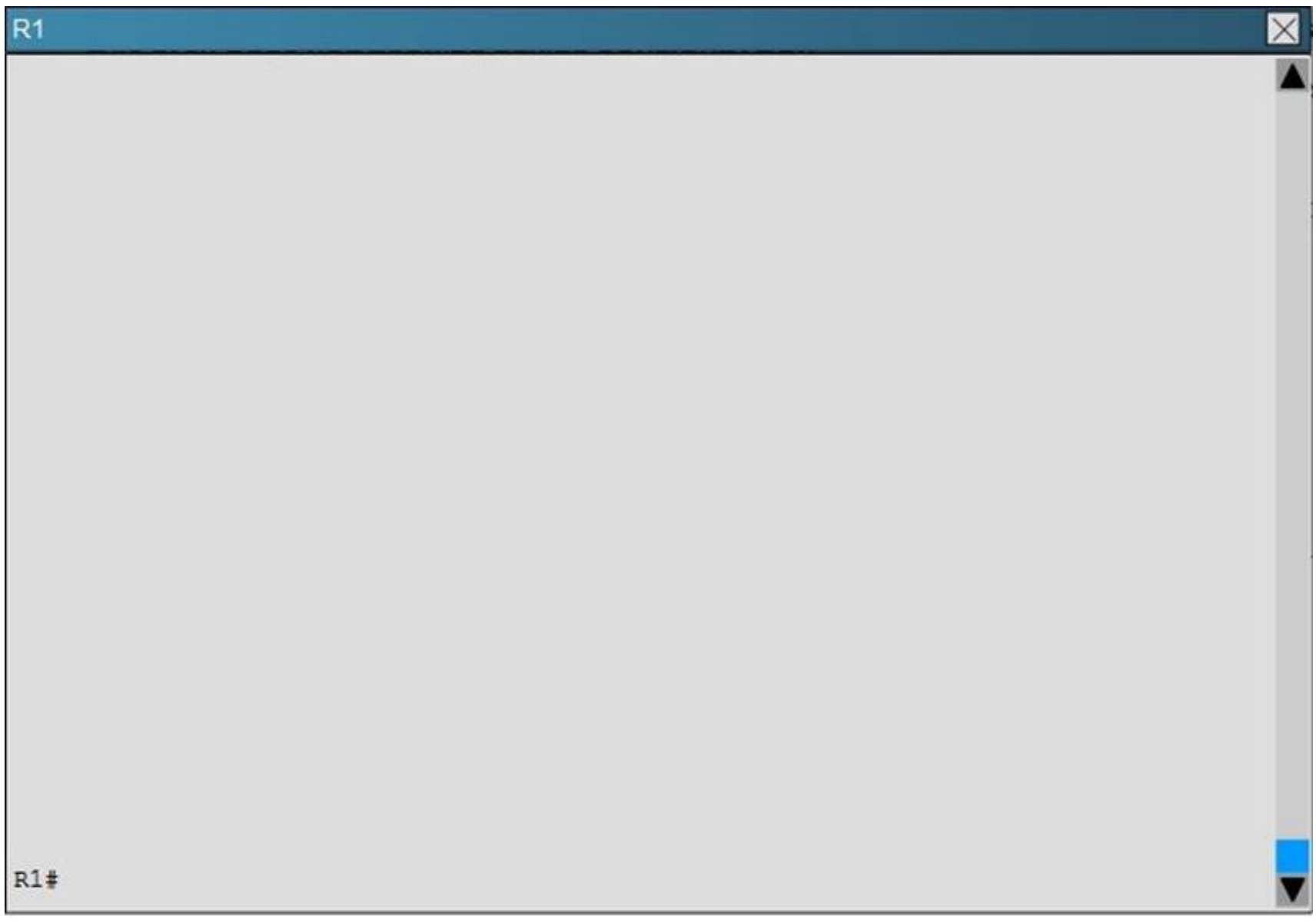
R5

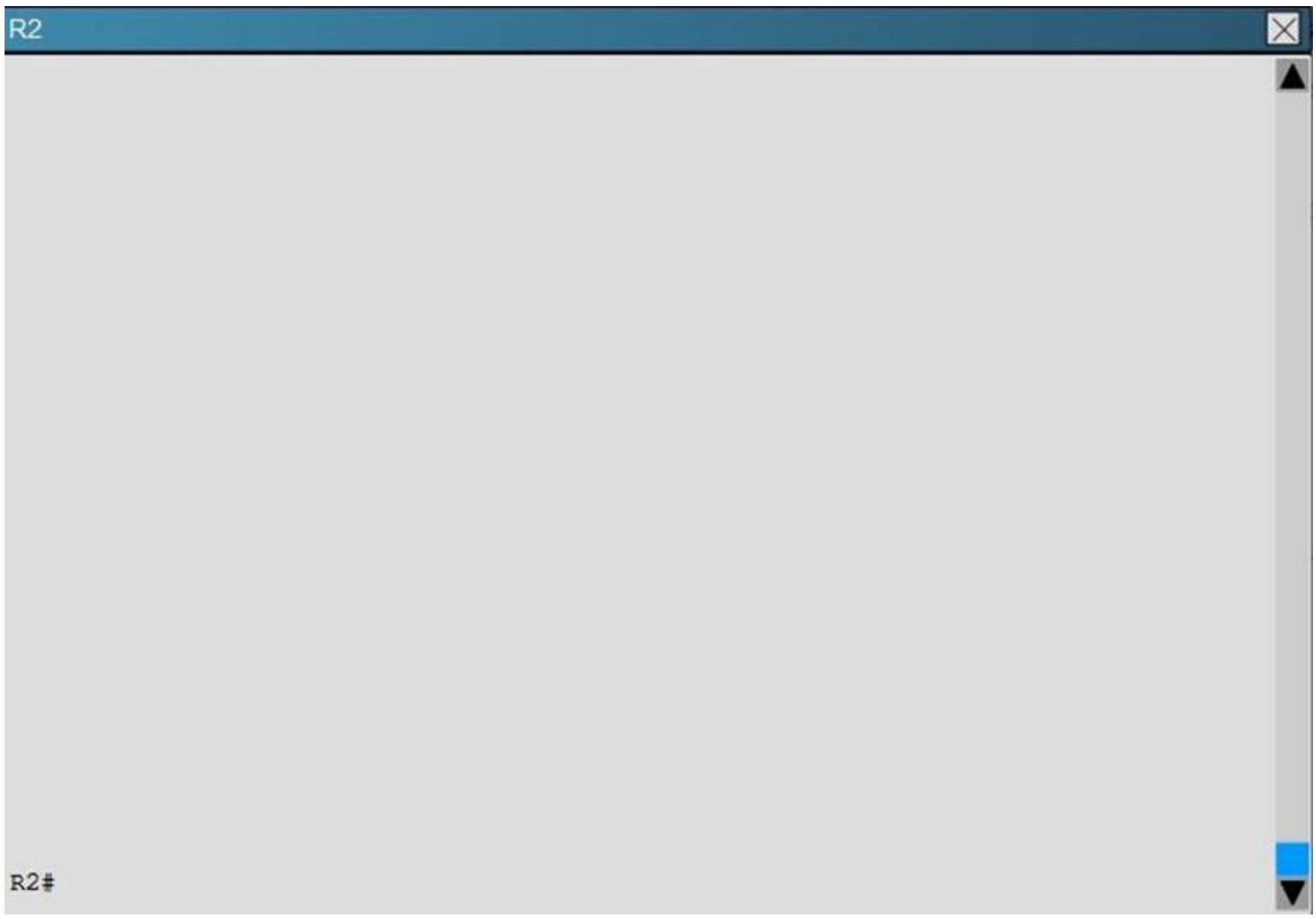
```
!
access-list 1 permit 192.168.1.15
access-list 1 permit 192.168.1.24
access-list 1 permit 192.168.1.17
access-list 1 permit 192.168.1.20
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny   150.1.1.1
access-list 3 deny   192.168.46.0 0.0.0.255
access-list 3 deny   192.168.24.0 0.0.0.255
access-list 3 deny   192.168.12.0 0.0.0.255
access-list 3 deny   192.168.13.0 0.0.0.255
access-list 3 deny   192.168.56.0 0.0.0.255
R5#
R5#
```

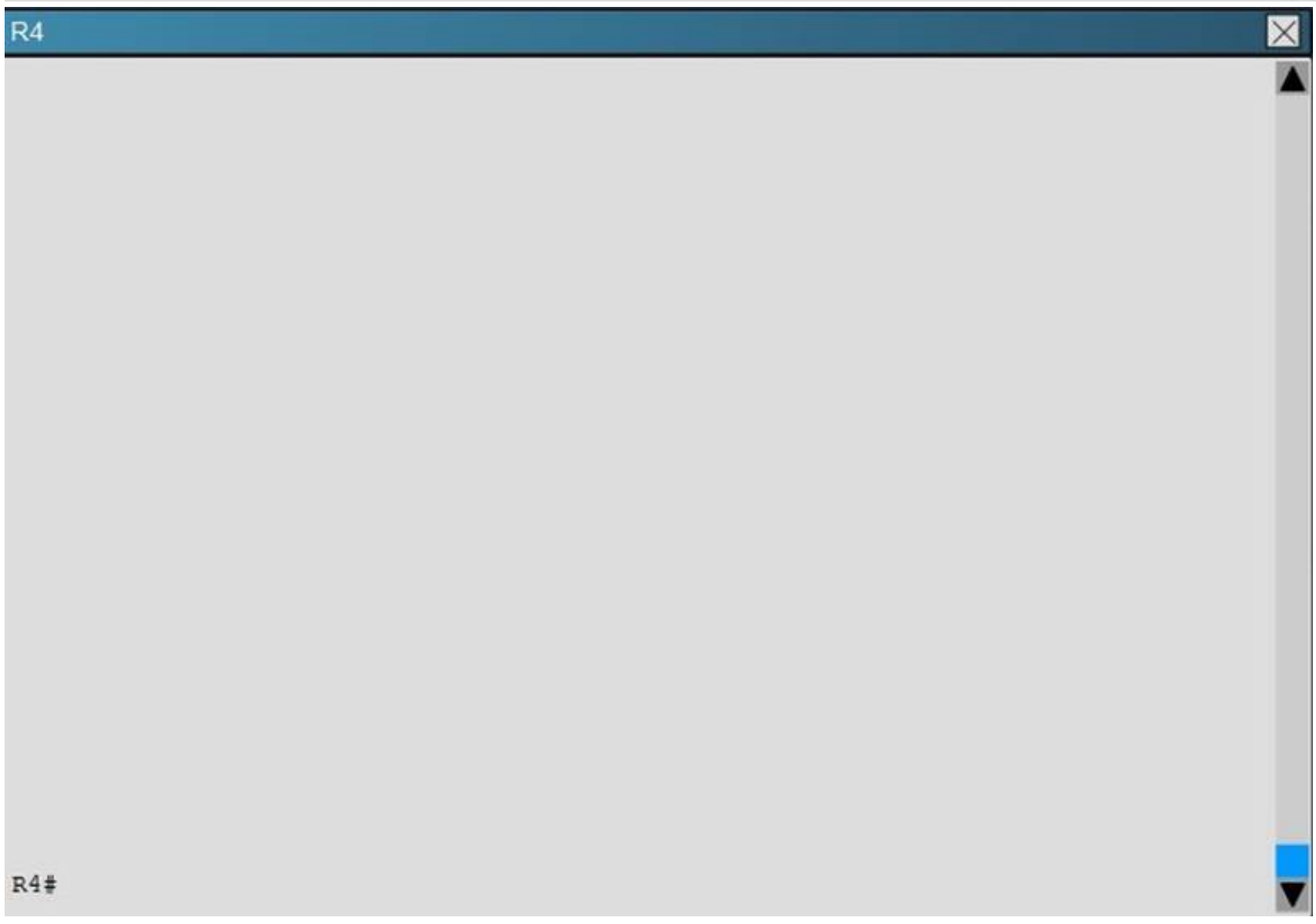
Topic 4, Troubleshooting HSRP

NEW QUESTION 107
Scenario:
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.


Network Core
R5
192.168.2.0/24
R4
Branch Office
E0/1
HSRP
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24


R1
R1#


R2
R2#


R4
R4#

The following debug messages are noticed for HSRP group 2. But still neither R1 nor R2 has identified one of them as standby router. Identify the reason causing the
issue.
Note: only show commands can be used to troubleshoot the ticket. R1#
'Mar 26 11:17:39.234: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:40.034: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
R1#
'Mar 26 11:17:40.364: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
R1#
'Mar 26 11:17:41.969: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:42.719: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
'Mar 26 11:17:42.918: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
R1#
'Mar 26 11:17:44.869: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:45.485: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
'Mar 26 11:17:45.718: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
R1#
'Mar 26 11:17:47.439: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:48.252: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
'Mar 26 11:17:48.322: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
R1#
'Mar 26 11:17:50.389: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:50.735: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
'Mar 26 11:17:50.921: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
R1#
'Mar 26 11:17:53.089: HSRP: Et1/0 Grp2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:53.338: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active pri130vlP
172.16.10.254
'Mar 26 11:17:53.633: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254

A. HSRP group priority misconfiguration

B. There is an HSRP authentication misconfiguration
C. There is an HSRP group number mismatch
D. This is not an HSRP issue: this is DHCP issue.
E. The ACL applied to interface is blocking HSRP hello packet exchange

Answer: E

Explanation: On R1 we see that access list 102 has been applied to the Ethernet 1/0 interface:

R1

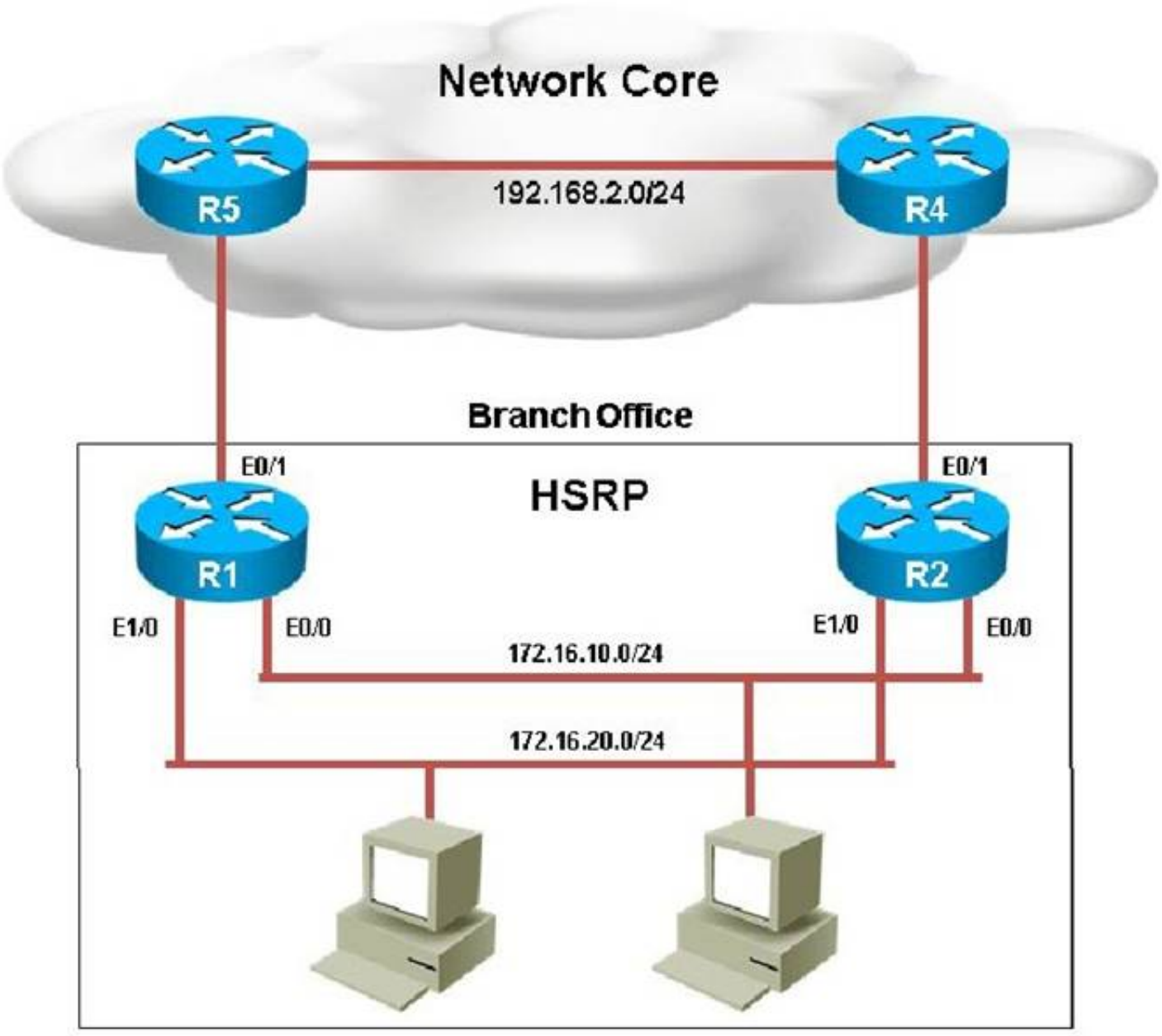
```
interface Ethernet1/0
 description connection to 172.16.20.0/24 network
 ip address 172.16.20.2 255.255.255.0
 ip access-group 102 in
 standby version 2
 standby 2 ip 172.16.20.254
 standby 2 authentication cisco123
!
```

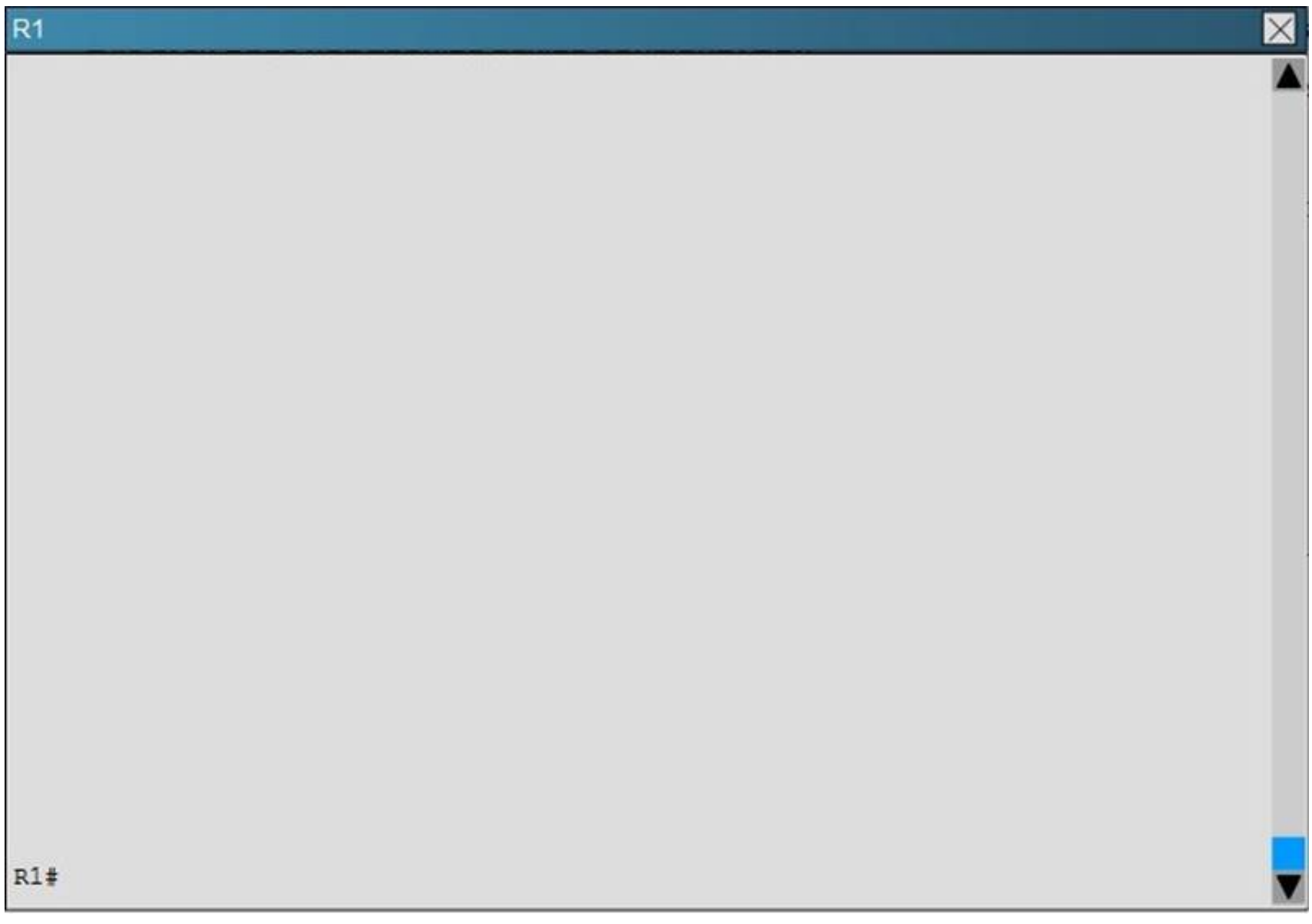
R1

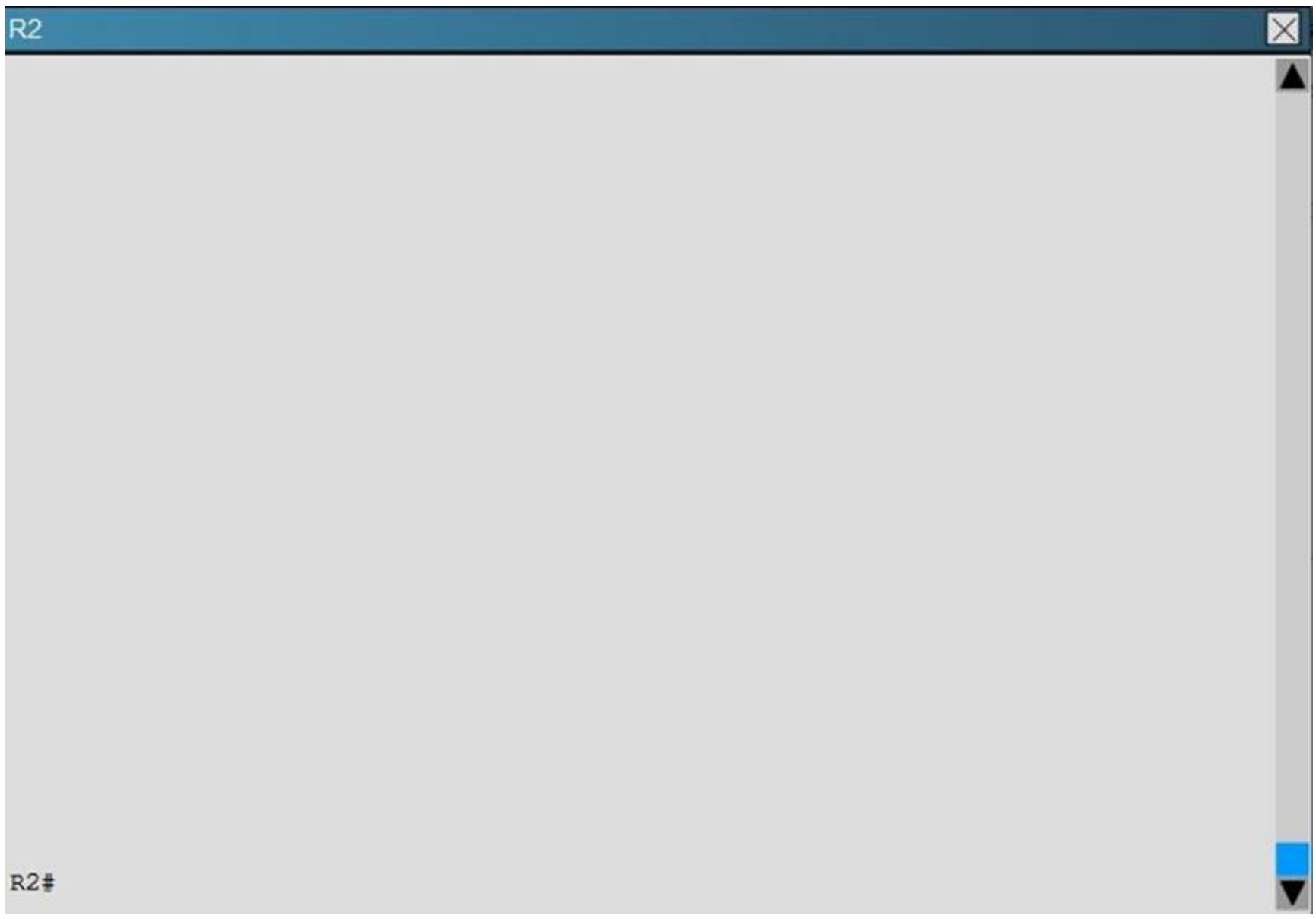
```
no ip http server
!
access-list 102 deny   ip any host 224.0.0.102
access-list 102 permit ip any any
!
!
```

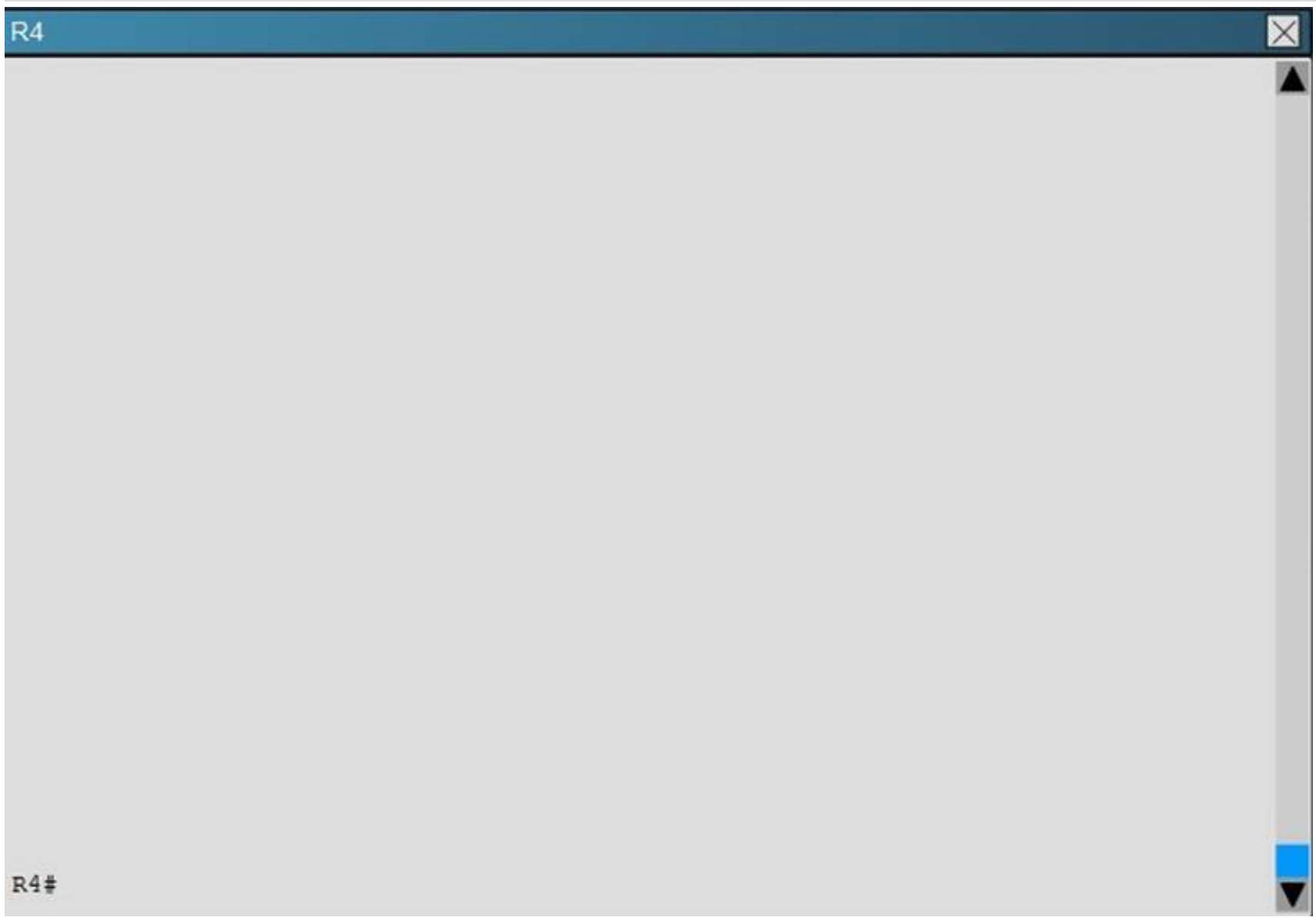
This access list is blocking all traffic to the 224.0.0.102 IP address, which is the multicast address used by HSRP.

NEW QUESTION 110
Scenario:
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.


Network Core
R5
192.168.2.0/24
R4
Branch Office
E0/1
HSRP
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24


R1
R1#


R2
R2#

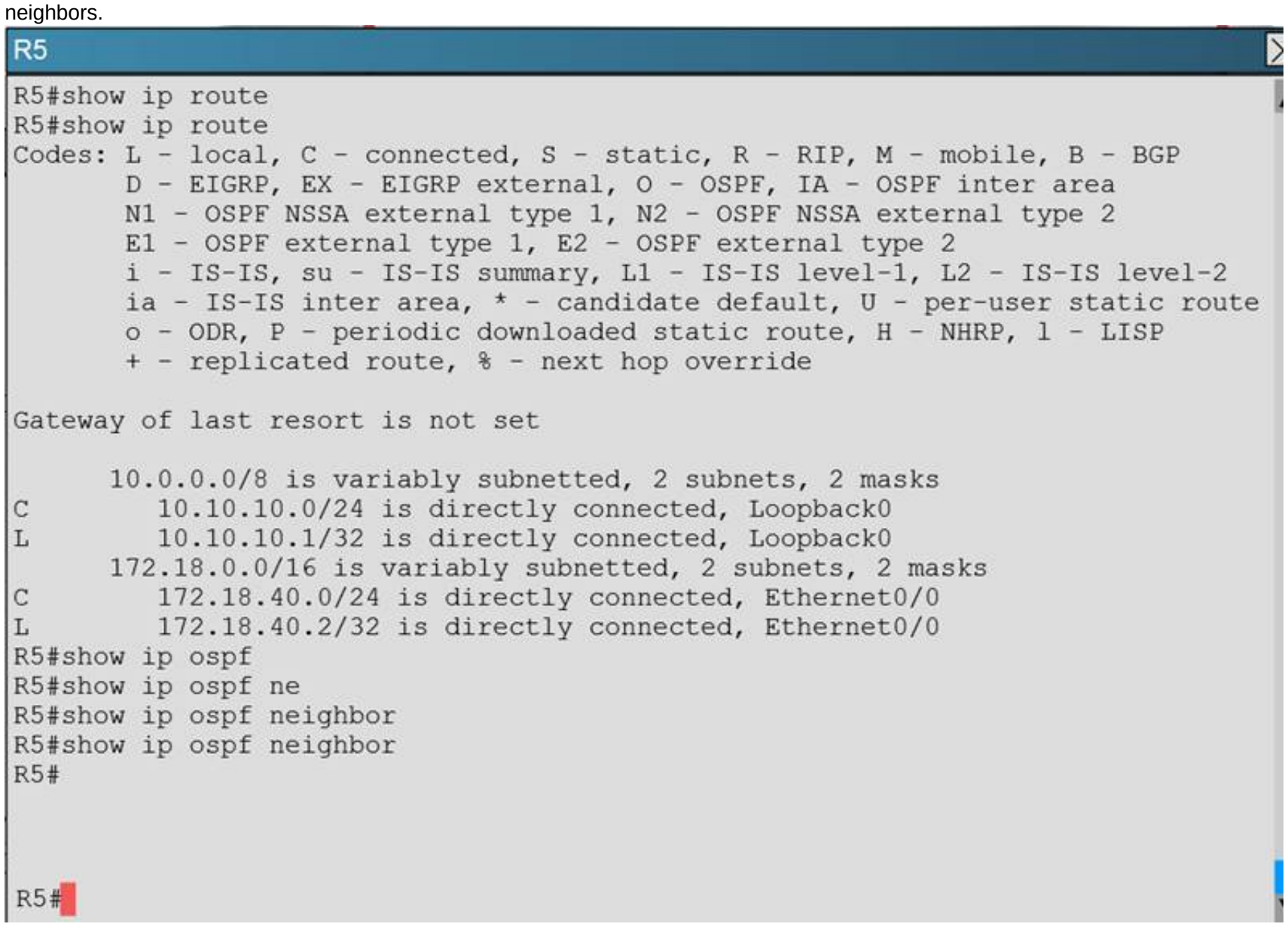

R4
R4#

Examine the configuration on R5. Router R5 do not see any route entries learned from R4; what could be the issue?

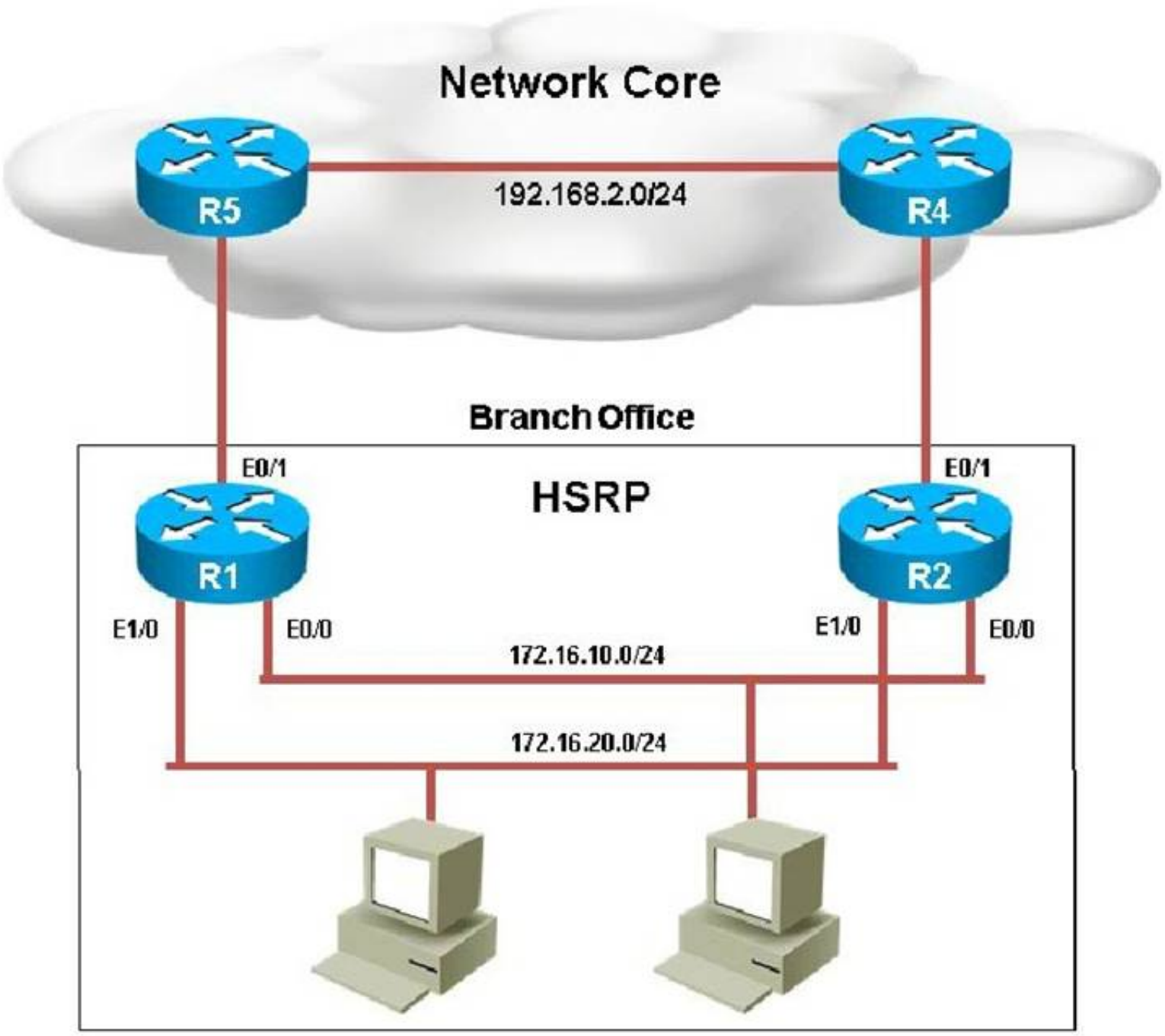
A. HSRP issue between R5 and R4
B. There is an OSPF issue between R5and R4
C. There is a DHCP issue between R5 and R4
D. The distribute-list configured on R5 is blocking route entries
E. The ACL configured on R5 is blocking traffic for the subnets advertised from R4.

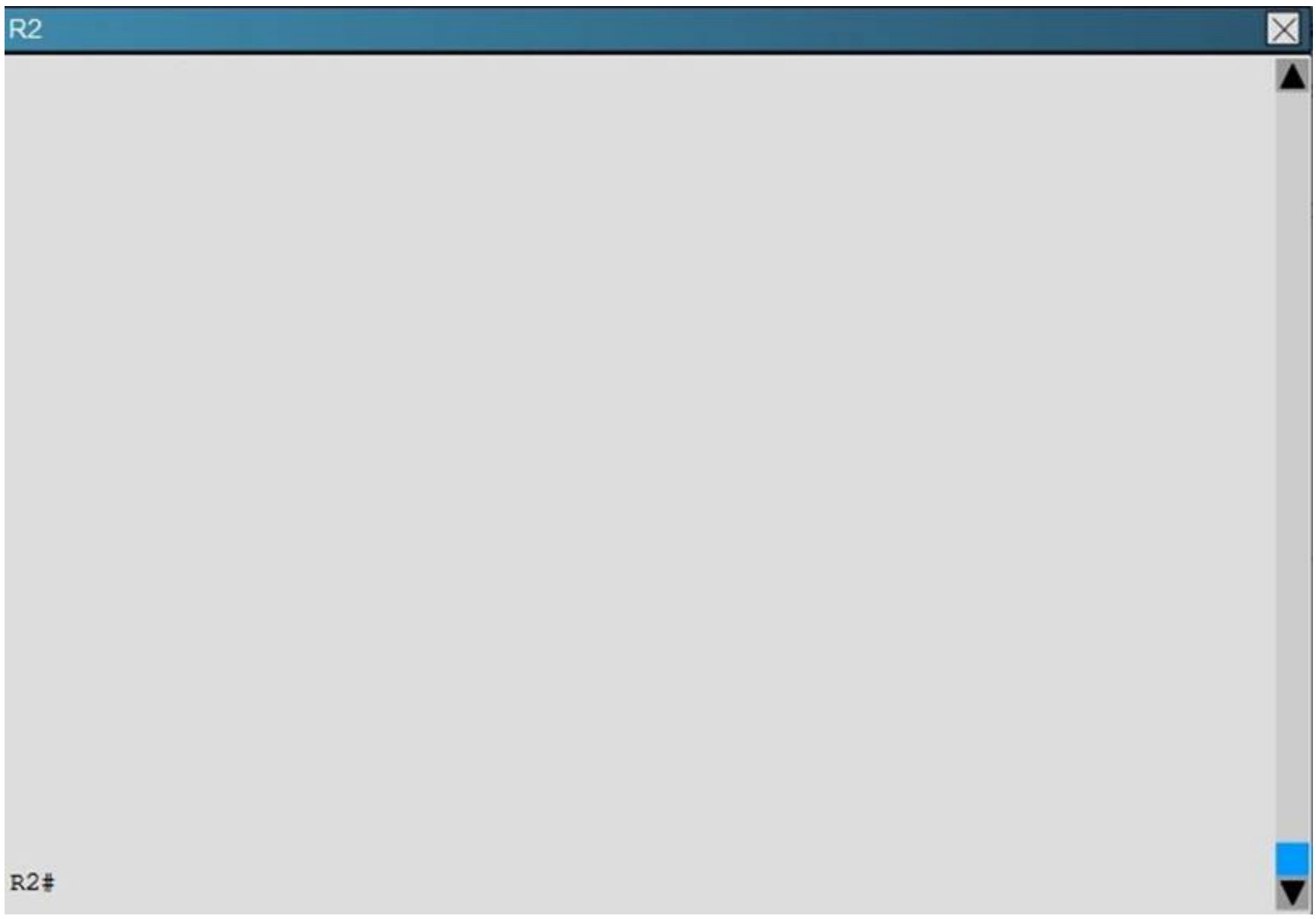
Answer: B

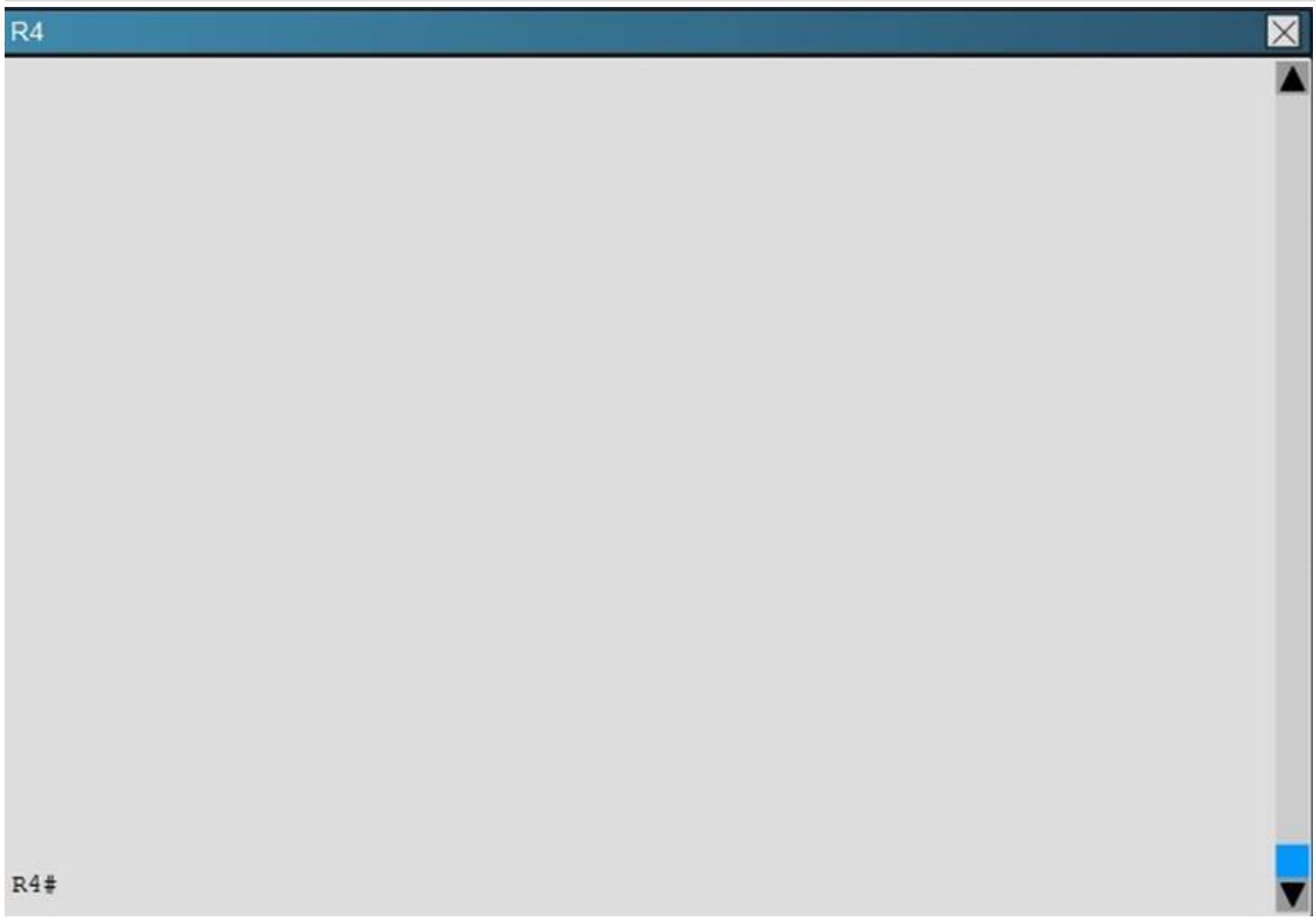
Explanation: If we issue the “show ip route” and “show ip ospf neighbor” commands on R5, we see that there are no learned OSPF routes and he has no OSPF neighbors.



NEW QUESTION 112
Scenario:
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.




R2
R2#


R4
R4#

Examine the configuration on R4. The routing table shows no entries for 172.16.10.0/24 and 172.16.20.0/24. Identify which of the following is the issue preventing route entries being installed on R4 routing table?

A. HSRP issue between R4 and R2
B. This is an OSPF issue between R4 and R2
C. This is a DHCP issue between R4 and R2
D. The distribute-list configured on R4 is blocking route entries
E. The ACL configured on R4 is blocking inbound traffic on the interface connected to R2

Answer: D

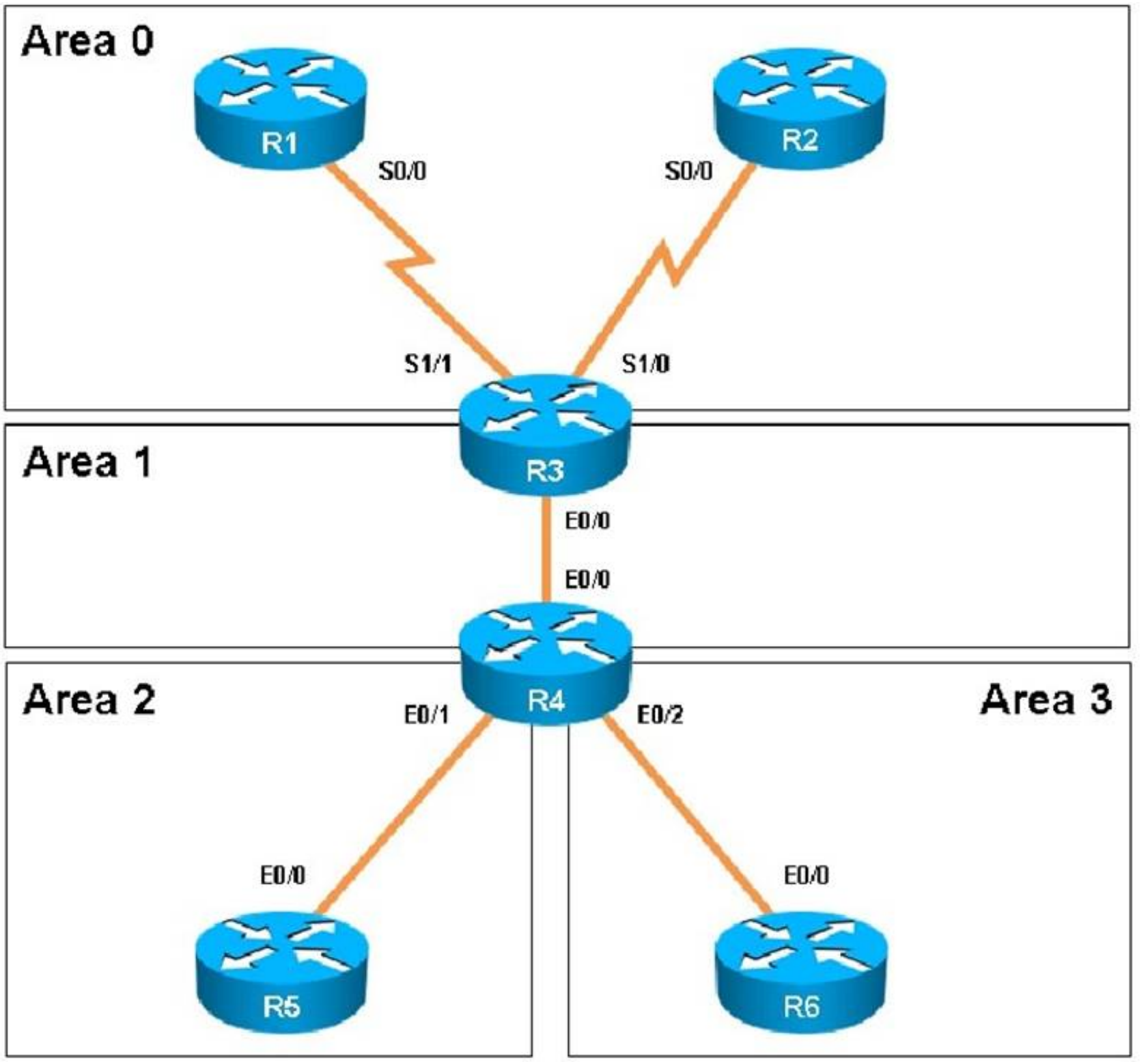
Explanation: If we look at the configuration on R4 we see that there is a distribute list applied to OSPF, which blocks the 172.16.20.0/24 and 172.16.10.0/24 networks.

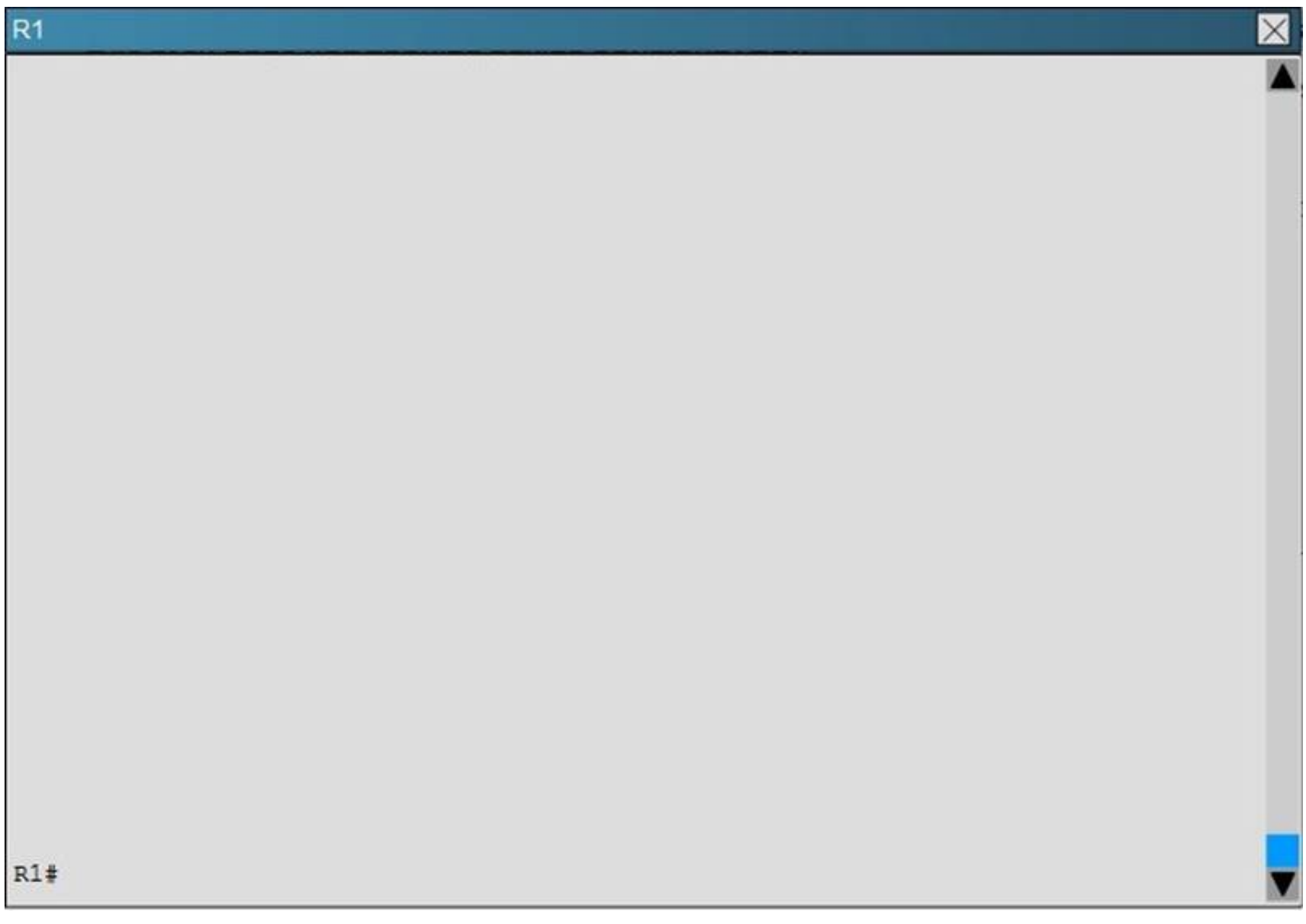
R4

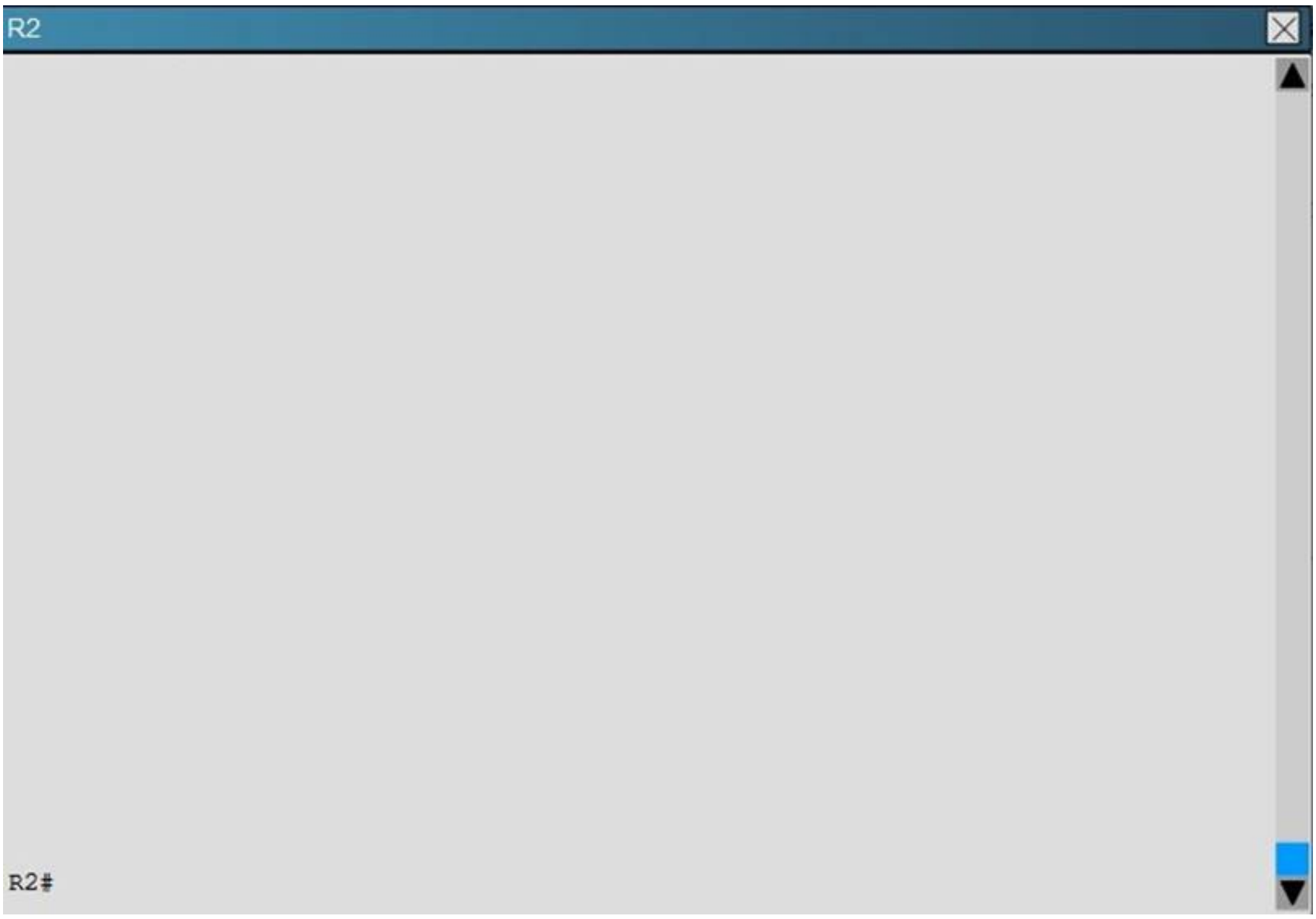
```
!
router ospf 10
 network 0.0.0.0 255.255.255.255 area 0
 distribute-list 1 in
!
!
!
no ip http server
!
access-list 1 permit 172.18.30.0
access-list 1 deny   172.16.20.0
access-list 1 permit 172.18.20.0
access-list 1 permit 172.18.10.0
access-list 1 deny   172.16.10.0
access-list 1 permit any
!
!
```

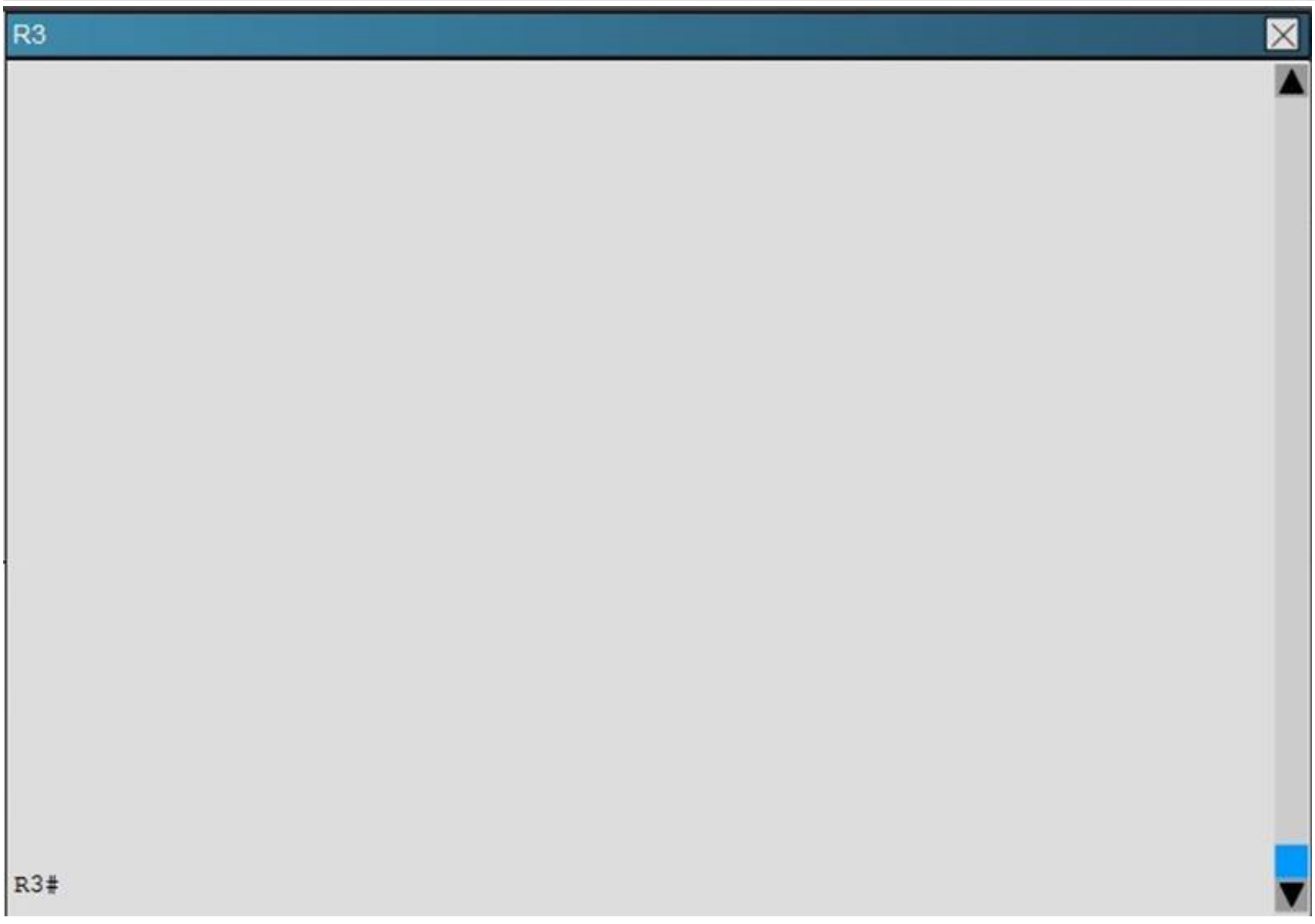
Topic 5, Troubleshooting OSPF

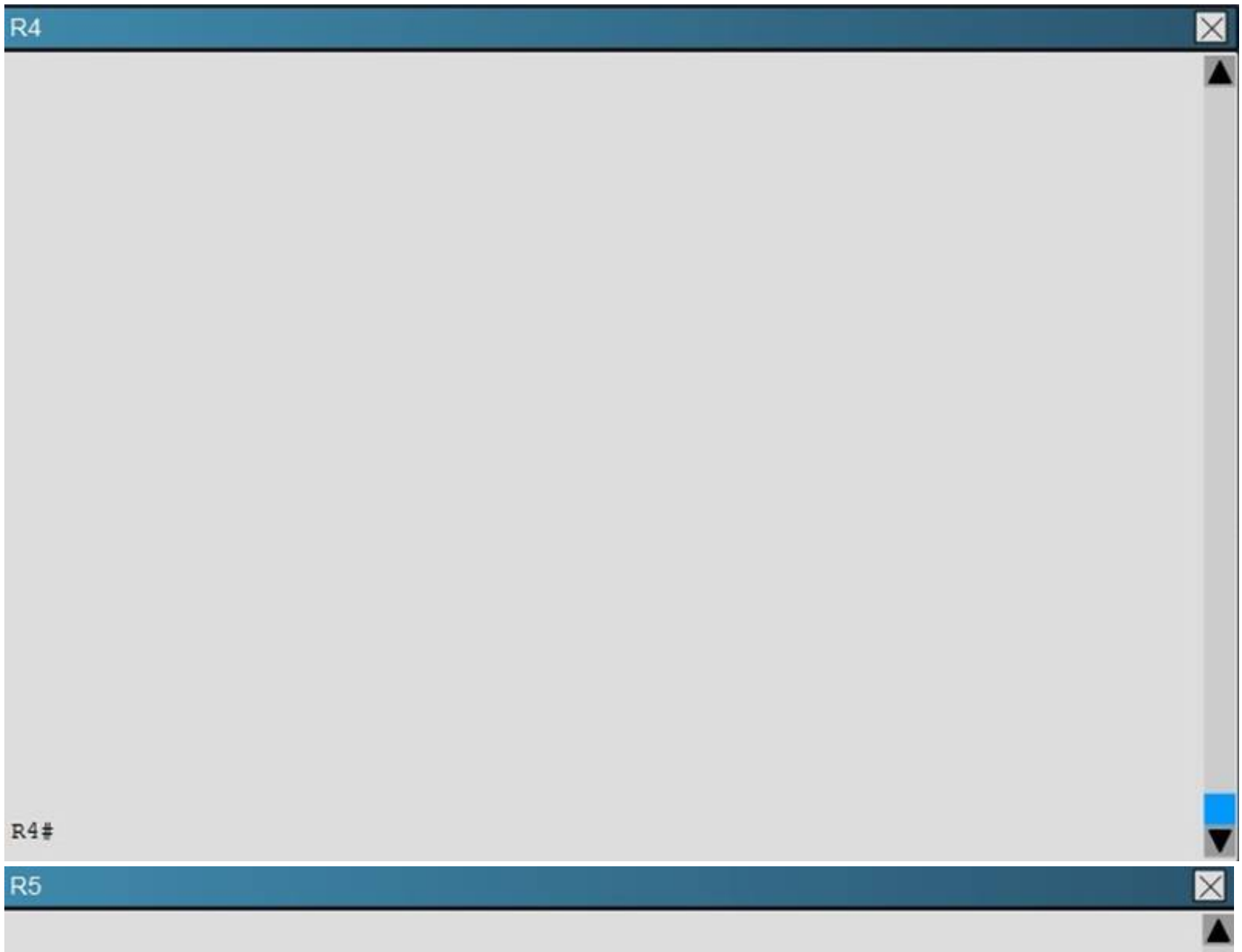
NEW QUESTION 117
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.


Area 0
R1
R2
S0/0
S0/0
S1/1
S1/0
Area 1
R3
E0/0
E0/0
R4
Area 2
E0/1
E0/2
Area 3
E0/0
E0/0
R5
R6


R1
R1#


R2
R2#


R3
R3#


R4
R4#
R5
R5#

After resolving the issues between R3 and R4. Area 2 is still experiencing routing issues. Based on the current router configurations, what needs to be resolved for routes to the networks behind R5 to be seen in the company intranet?

A. Configure R4 and R5 to use MD5 authentication on the Ethernet interfaces that connect to the common subnet.
B. Configure Area 1 in both R4 and R5 to use MD5 authentication.
C. Add ip ospf authentication-key 7 BEST to the R4 Ethernet interface that connects to R5 and ip ospf authentication-key 7 BEST to R5 Ethernet interface that connects to R4.
D. Add ip ospf authentication-key CISCO to R4 Ethernet 0/1 and add area 2 authentication to the R4 OSPF routing process.

Answer: D

Explanation: Here, we see from the running configuration of R5 that OSPF authentication has been configured on the link to R4:

R5

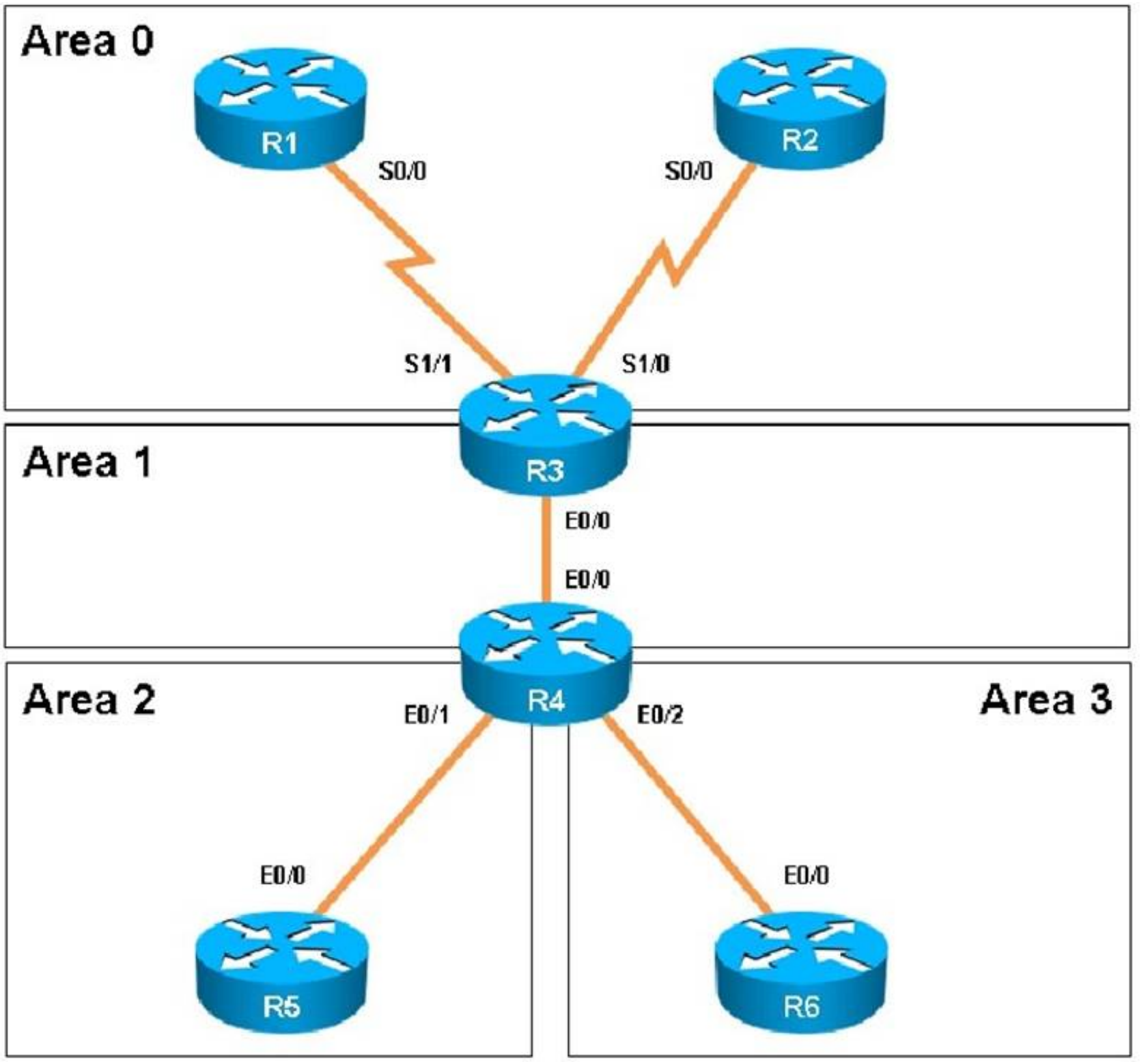
```
interface Ethernet0/0
 ip address 192.168.45.5 255.255.255.0
 ip ospf authentication-key CISCO
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
router ospf 100
 router-id 5.5.5.5
 auto-cost reference-bandwidth 3000
 area 2 authentication
 area 2 nssa
 area 2 range 5.5.0.0 255.255.252.0
 network 192.168.45.5 0.0.0.0 area 2
 distribute-list 45 in Ethernet0/1
```

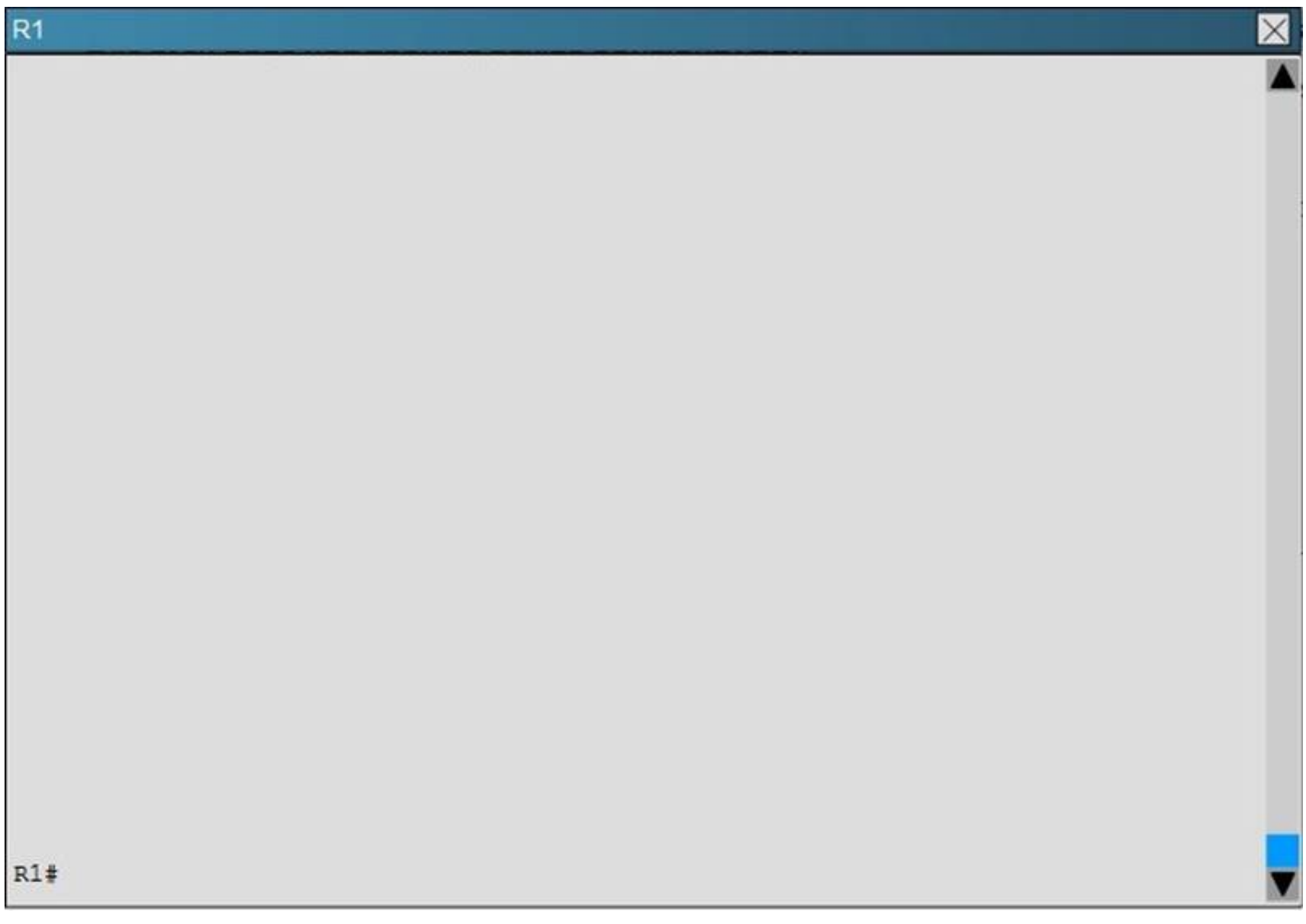
However, this has not been done on the link to R5 on R4:

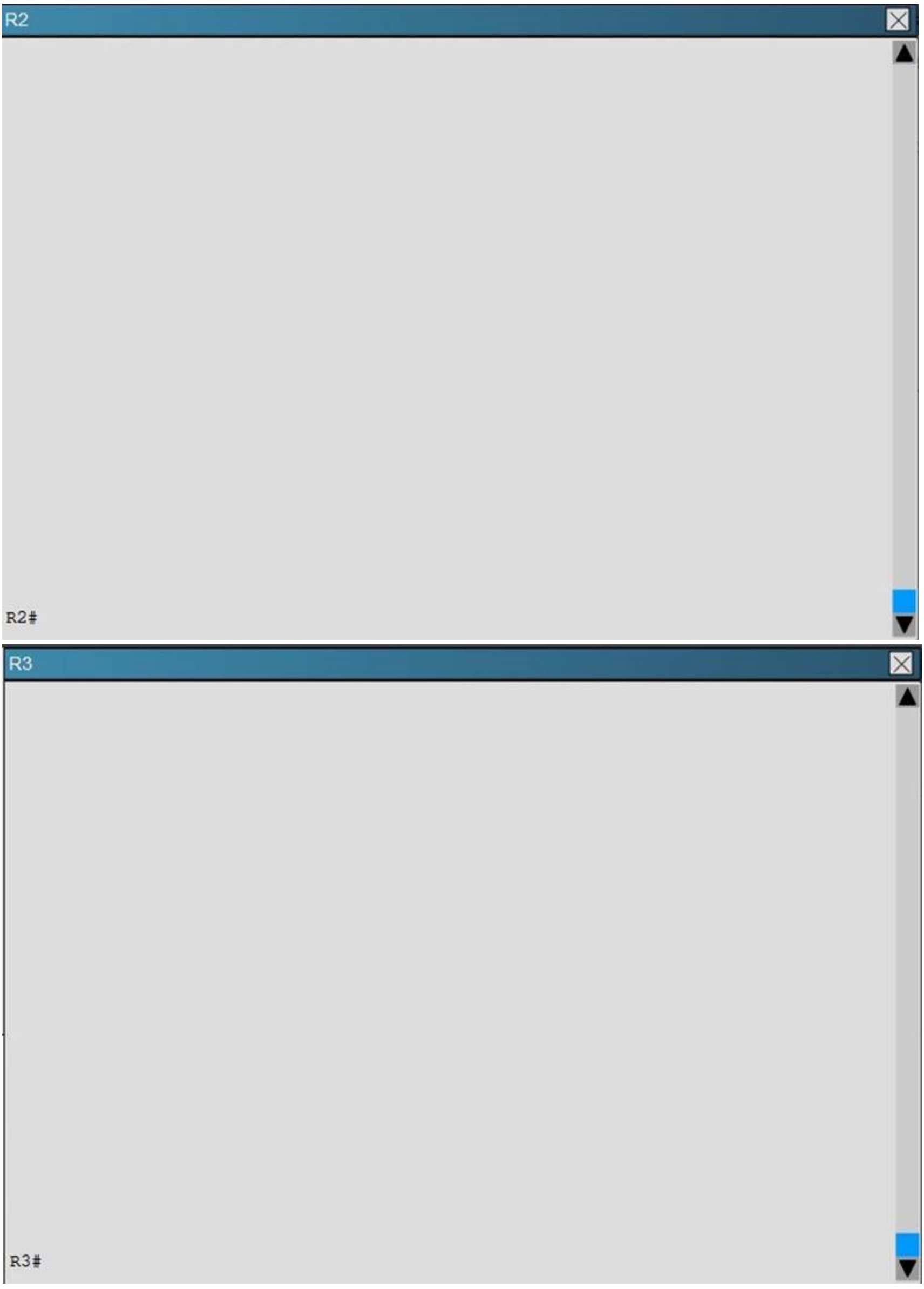
R4

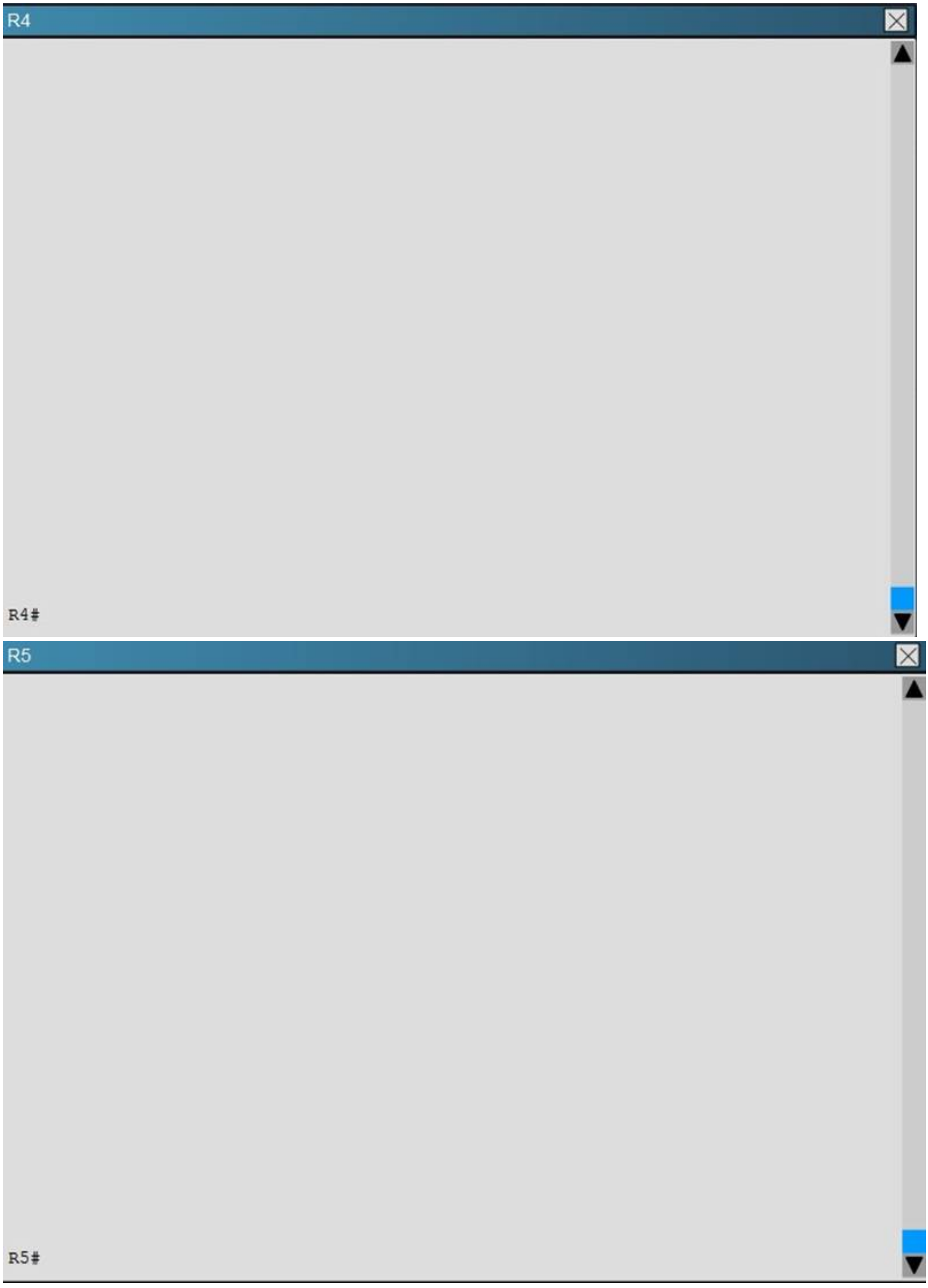
```
interface Ethernet0/1
 ip address 192.168.45.4 255.255.255.0
!
interface Ethernet0/2
 ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router ospf 100
 router-id 4.4.4.4
 auto-cost reference-bandwidth 3000
 area 1 virtual-link 3.3.3.3
 area 2 nssa
 area 2 range 5.5.0.0 255.255.252.0
 area 3 stub no-summary
 network 4.4.4.4 0.0.0.0 area 1
 network 192.168.34.0 0.0.0.255 area 1
 network 192.168.45.0 0.0.0.255 area 2
 network 192.168.46.0 0.0.0.255 area 3
 distribute-list 1 in Ethernet0/0
 distribute-list 1 in Ethernet0/1
!
```

NEW QUESTION 121
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.


Area 0
R1
R2
S0/0
S0/0
S1/1
S1/0
Area 1
R3
E0/0
E0/0
R4
Area 2
E0/1
E0/2
Area 3
E0/0
E0/0
R5
R6


R1
R1#


R2
R2#
R3
R3#

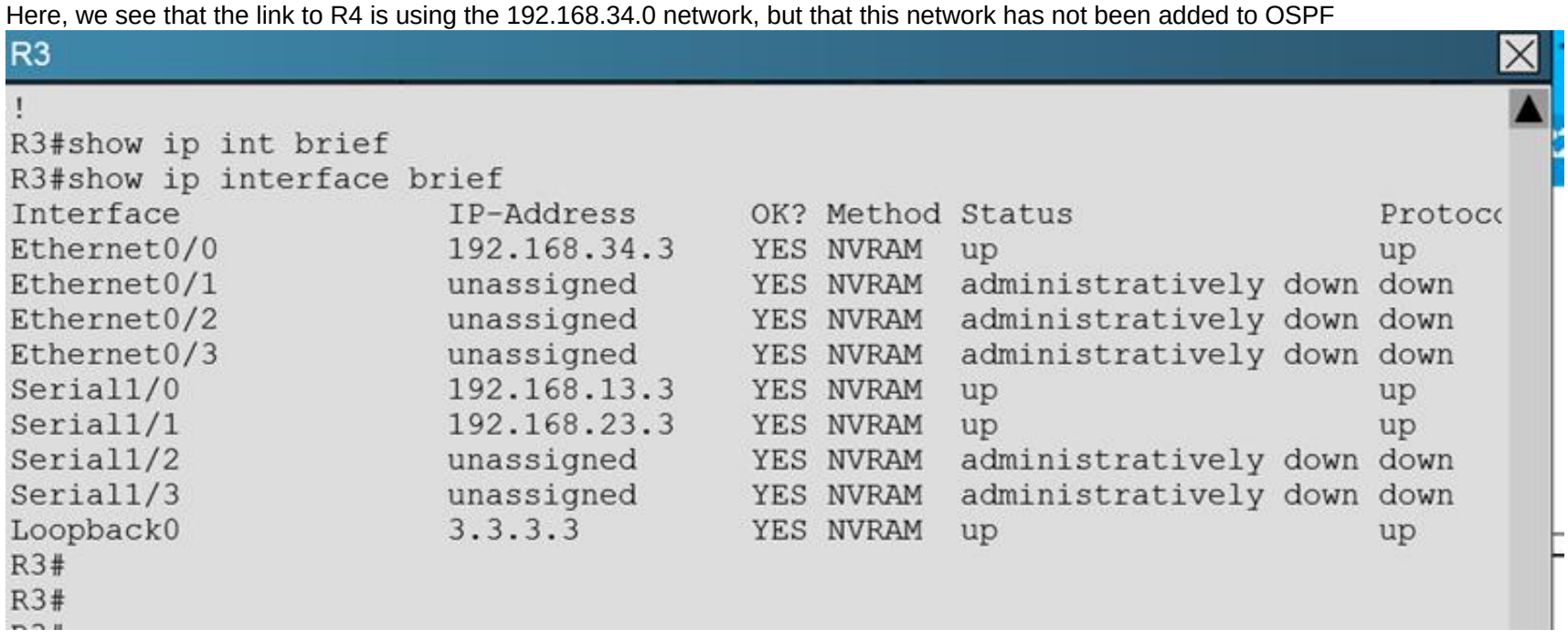

R4
R4#
R5
R5#

Connectivity from R3 to R4, R5 and R6 has been lost. How should connectivity be reestablished?

A. Configure R4 with a virtual link to 192.168.13.2
B. Change the R3 and R4 hello-interval and retransmit-interface timers to zero so the link won't go down.
C. Add an OSPF network statement for 4.4.4.4 0.0.0.0 area 1 in R3
D. Add an OSPF network statement for 192.168.34.3 0.0.0.255 area 2 in R3
E. Add an OSPF network statement for 192.168.34.0 0.0.0.255 area 1 in R3

Answer: E

Explanation: Based on the network diagram, we know that a virtual link will need to be configured to logically connect area 2 to the back area 0. However, this is not the problem as we can see that R3 has been correctly configured to do this. It is, however, missing the network statement for the link to R4.
Here, we see that the link to R4 is using the 192.168.34.0 network, but that this network has not been added to OSPF

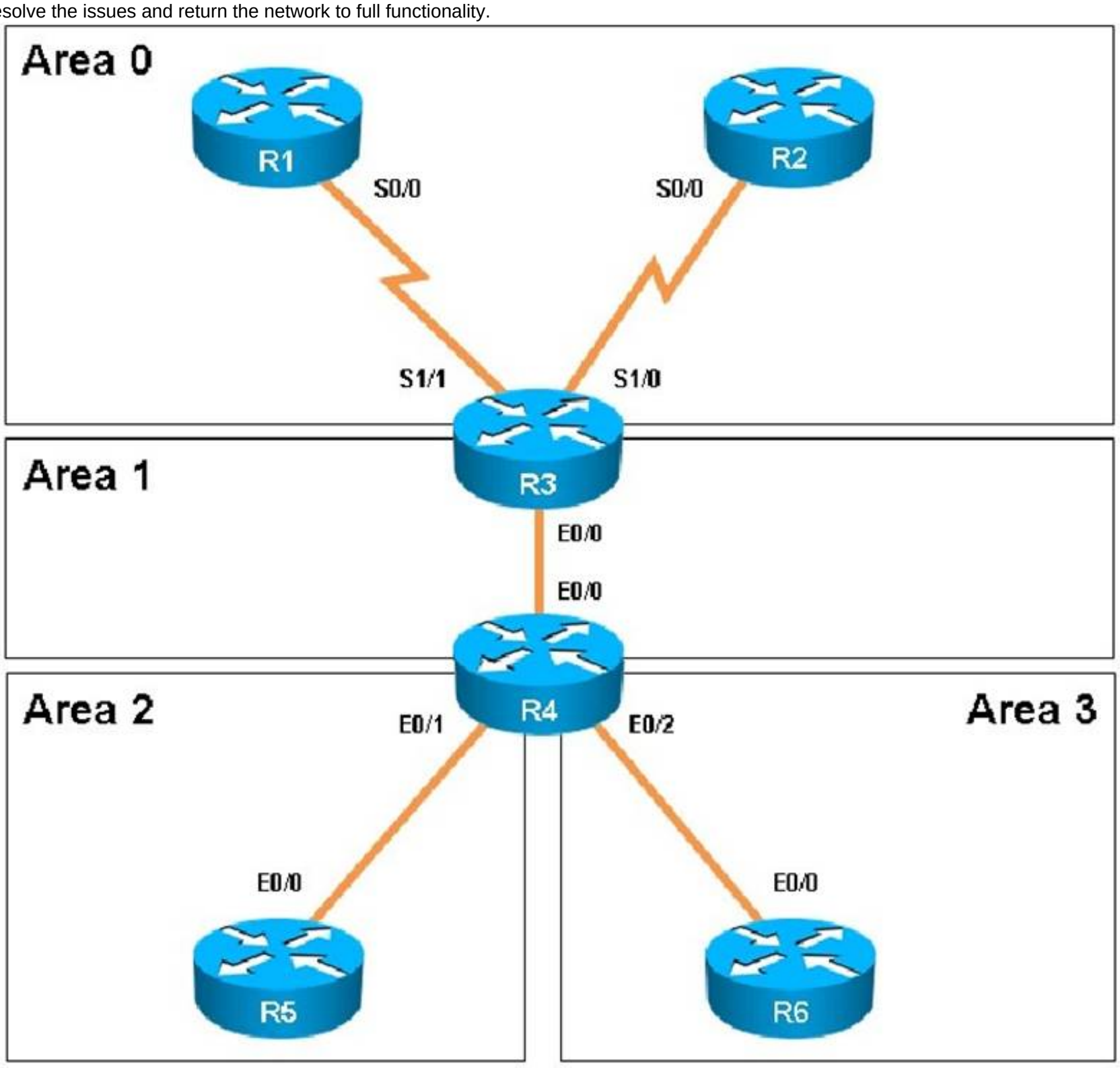


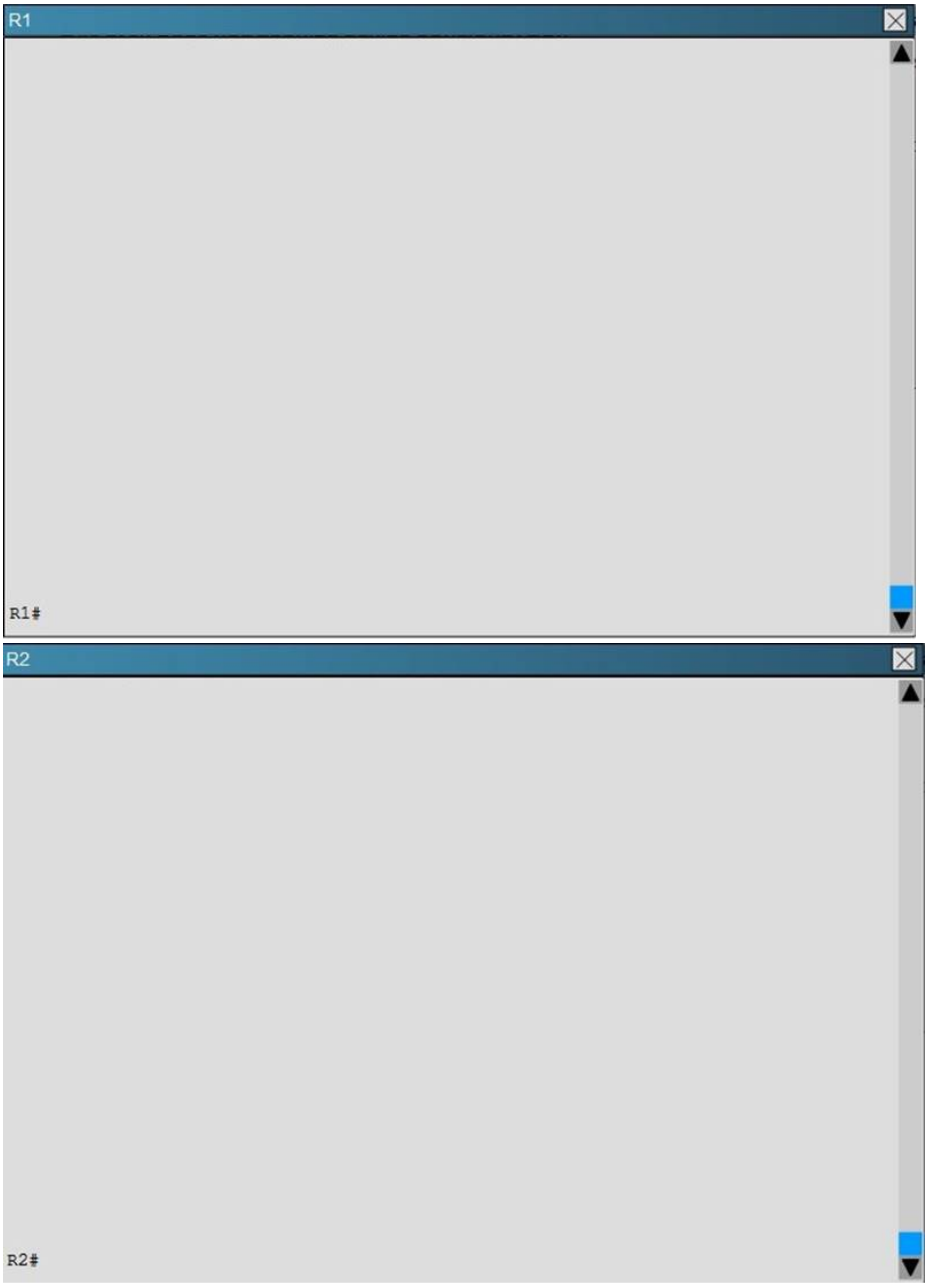
R3

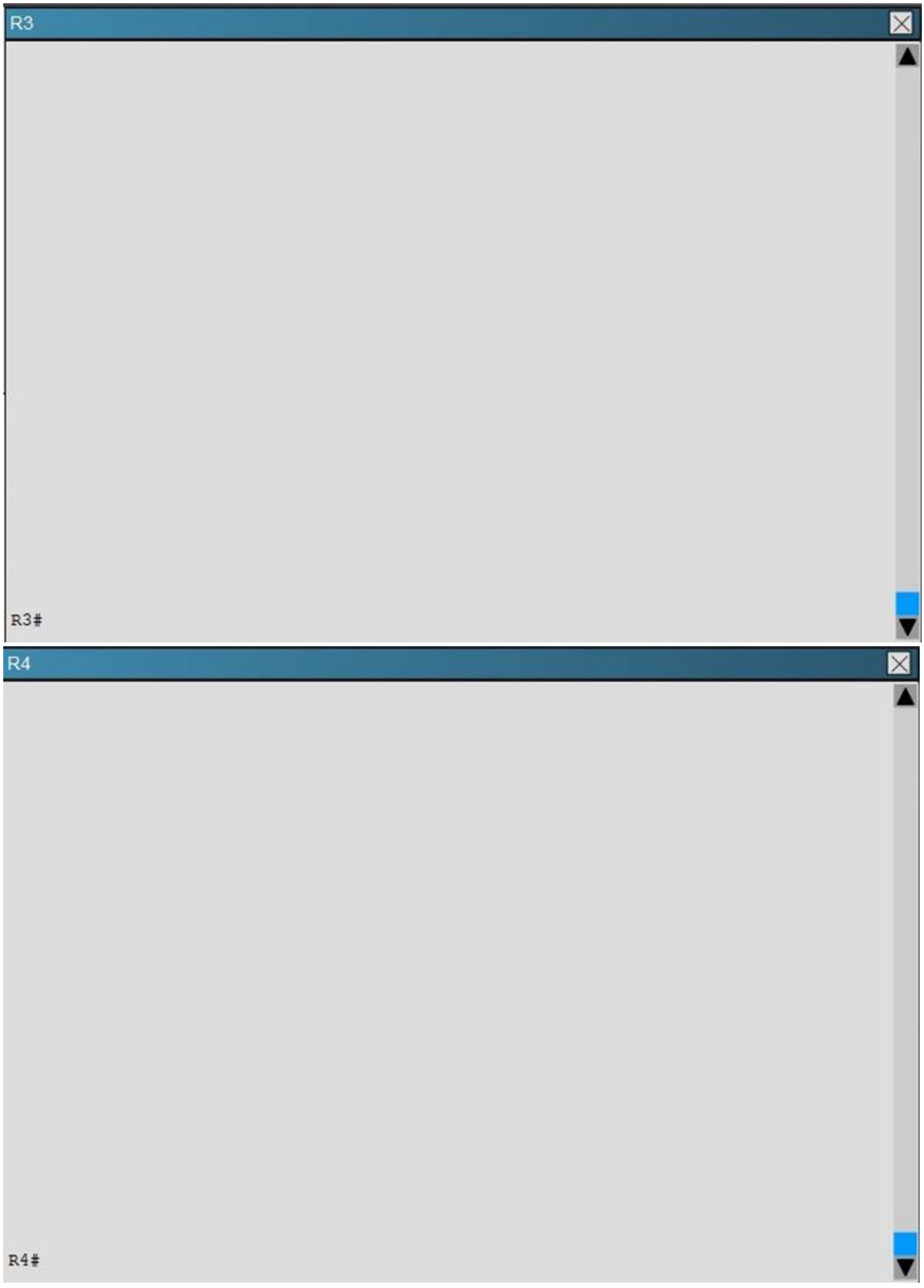
```
!
router ospf 100
 router-id 3.3.3.3
 area 1 virtual-link 4.4.4.4
 network 3.3.3.3 0.0.0.0 area 1
 network 192.168.13.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
 neighbor 192.168.13.1
!
!
```

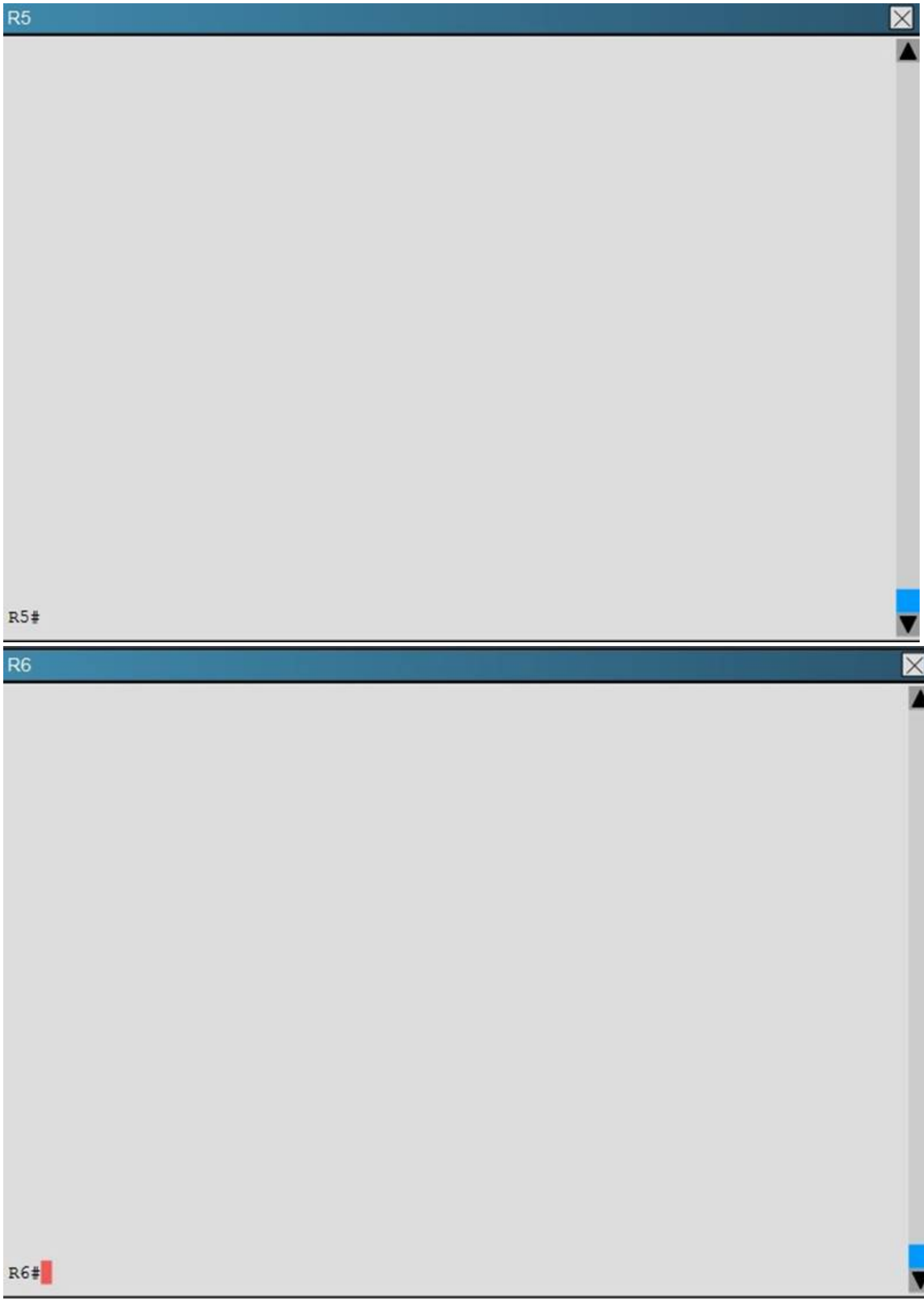
Based on the network diagram, this link should be added to Area 1, not Area 2.

NEW QUESTION 123
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.




R1
R1#
R2
R2#


R3
R3#
R4
R4#



The 6.6.0.0 subnets are not reachable from R4. how should the problem be resolved?

A. Edit access-list 46 in R6 to permit all the 6.6.0.0 subnets
B. Apply access-list 46 in R6 to a different interface
C. Apply access-list 1 as a distribute-list out under router ospf 100 in R4
D. Remove distribute-list 64 out on R6
E. Remove distribute-list 1 in ethernet 0/1 in R4
F. Remove distribute-list 1 in ethernet 0/0 in R4

Answer: D

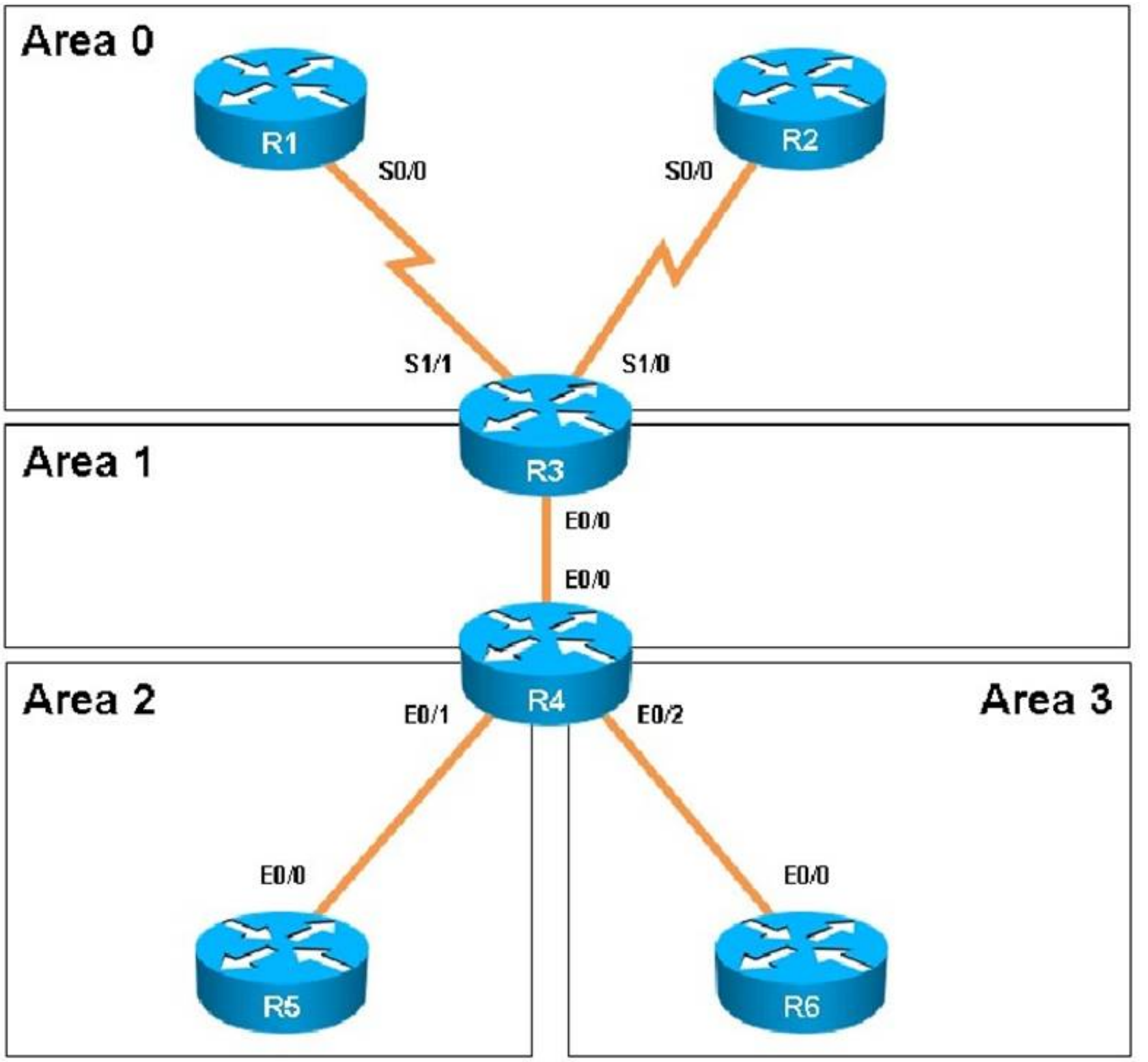
Explanation: Here we see from the running configuration of R6 that distribute list 64 is being used in the outbound direction to all OSPF neighbors.

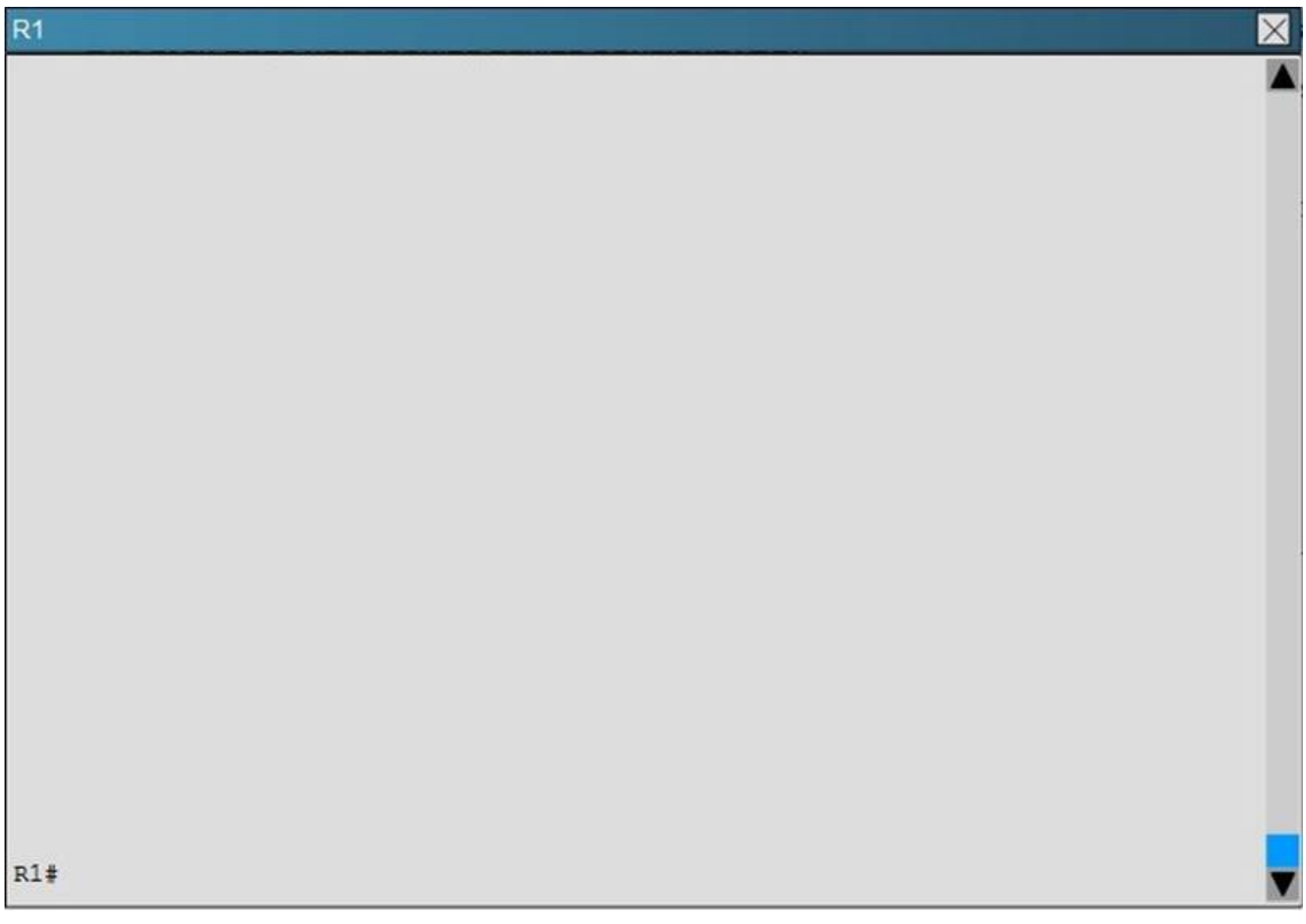
R6

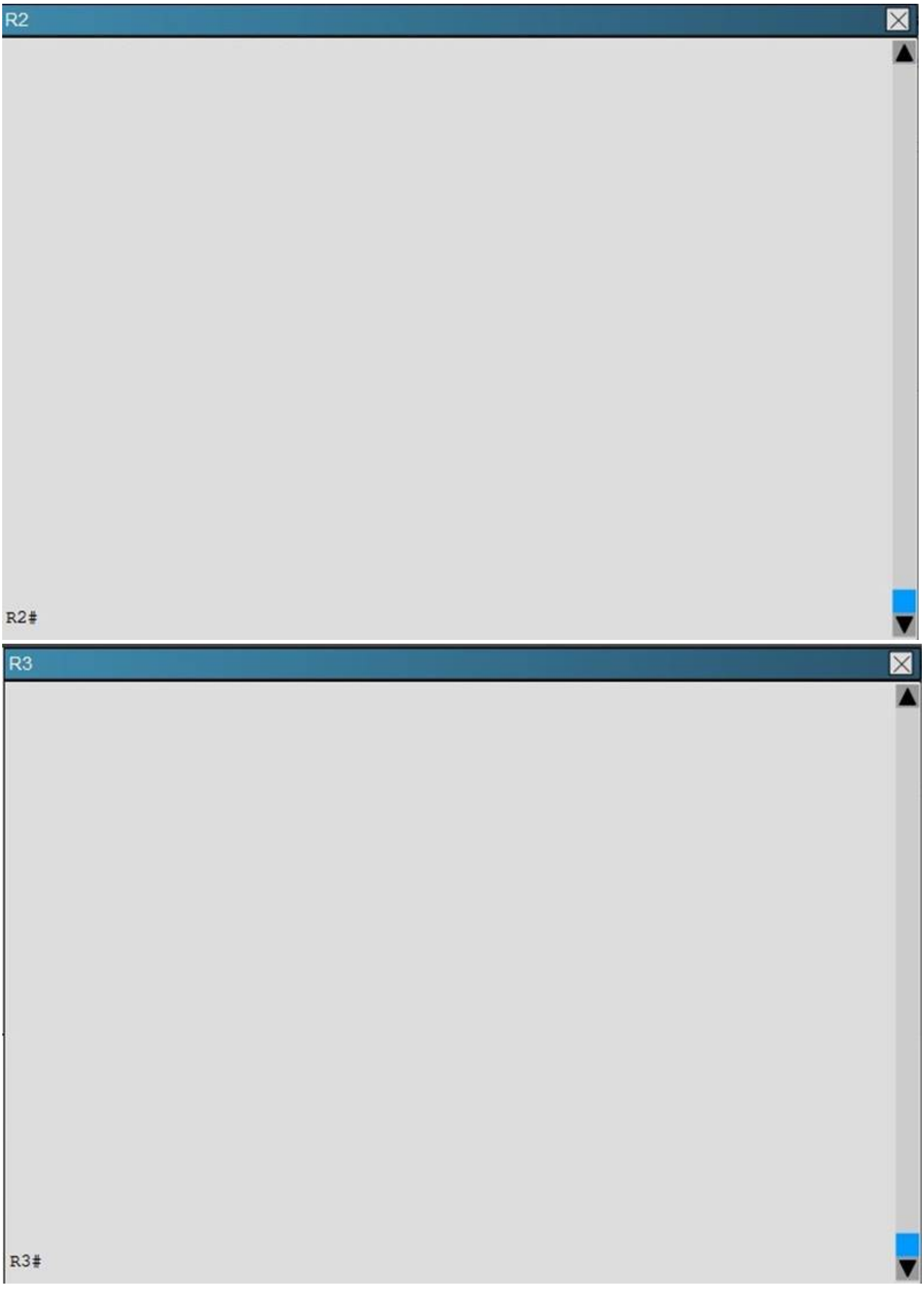
```
!
router ospf 100
 router-id 6.6.6.6
 auto-cost reference-bandwidth 3000
 area 3 stub no-summary
 redistribute connected
 network 192.168.46.0 0.0.0.255 area 3
 distribute-list 64 in Ethernet0/1
 distribute-list 46 in Loopback0
 distribute-list 64 out
!
!
!
no ip http server
!
access-list 46 deny   6.6.0.0 0.0.255.255
access-list 46 permit 6.0.0.0 0.255.255.255
access-list 64 deny   6.0.0.0 0.255.255.255
access-list 64 permit 6.6.0.0 0.0.255.255
!
!
!
```

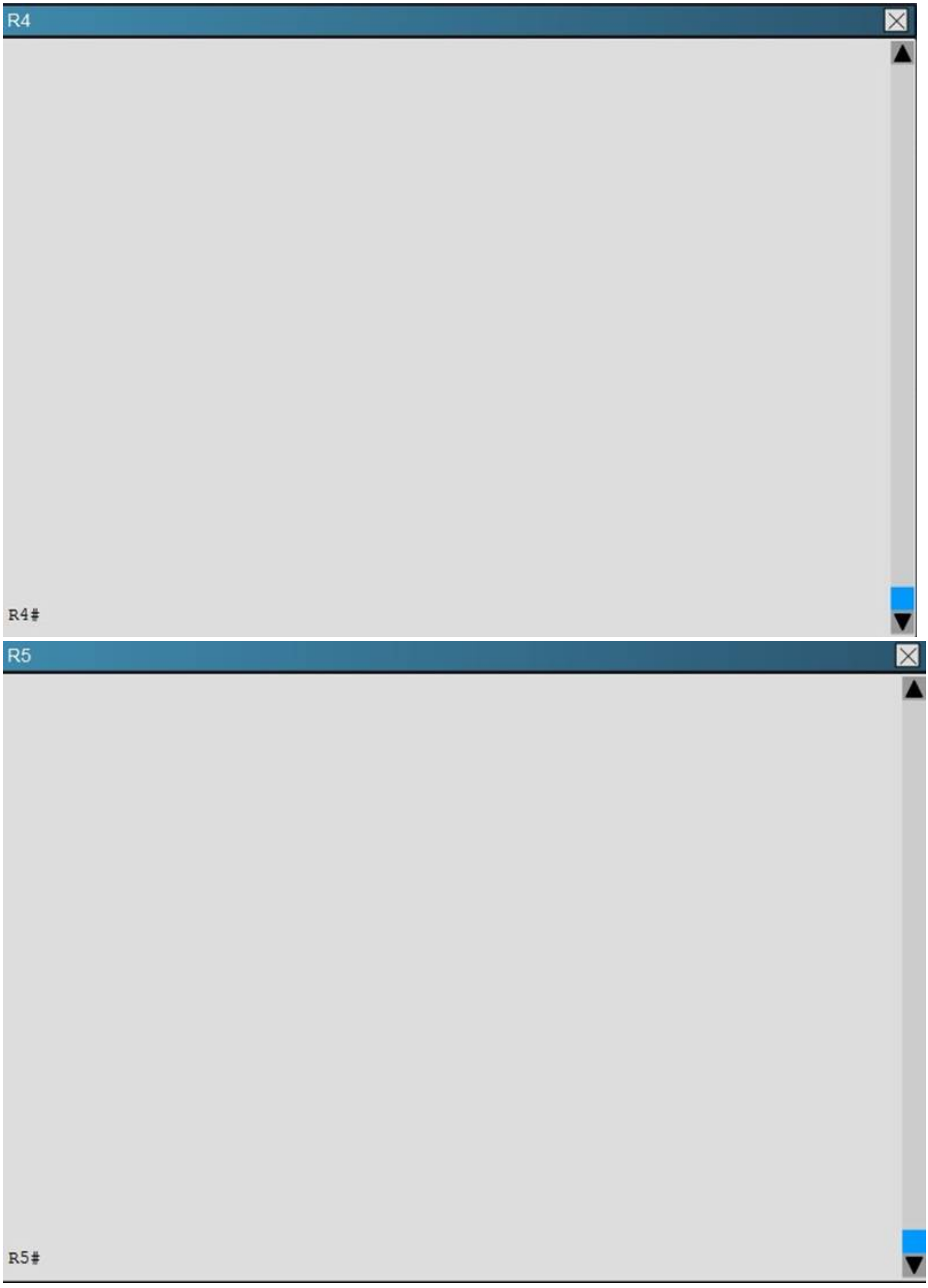
However, no packets will match the 6.6.0.0 in this access list because the first line blocks all 6.0.0.0 networks, and since the 6.6.0.0 networks will also match the first line of this ACL, these OSPF networks will not be advertised because they are first denied in the first line of the ACL.

NEW QUESTION 128
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.


Area 0
R1
R2
S0/0
S0/0
S1/1
S1/0
Area 1
R3
E0/0
E0/0
R4
Area 2
E0/1
E0/2
Area 3
E0/0
E0/0
R5
R6


R1
R1#


R2
R2#
R3
R3#


R4
R4#
R5
R5#

The OSPF neighbour relationship has been lost between R1 and R3. What is causing this problem?

A. The serial interface in R1 should be taken out of the shutdown state.
B. A neighbor statement needs to be configured in R1 and R3 pointing at each other.
C. The R1 network type should be changed to point-to-multipoint non-broadcast.
D. The hello, dead and wait timers on R1 need to be reconfigured to match the values on R3.

Answer: C

Explanation: In order for two OSPF routers to become neighbors, they must have matching network types across the links. In this case, we see that R1 has been configured as non-broadcast and R3 is using point to point non-broadcast.

R1

```
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Serial0/0
 ip address 192.168.13.1 255.255.255.0
 ip ospf network non-broadcast
 no fair-queue
 serial restart-delay 0
!
```

R3

```
!
interface Serial1/0
 ip address 192.168.13.3 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
 no fair-queue
 serial restart-delay 0
!
```

This can be seen by issuing the “show running-config” command on each router, or the “show ip ospf interface” command:

R1

```
Serial0/0 is up, line protocol is up
  Internet Address 192.168.13.1/24, Area 0, Attached via Network Statement
  Process ID 100, Router ID 1.1.1.1, Network Type NON_BROADCAST, Cost: 1943
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1943      no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.13.1
  Backup Designated router (ID) 3.3.3.3, Interface address 192.168.13.3
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 9
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

R3

```
Serial1/0 is up, line protocol is up
  Internet Address 192.168.13.3/24, Area 0, Attached via Network Statement
  Process ID 100, Router ID 3.3.3.3, Network Type POINT_TO_MULTIPOINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:19
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 7
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
OSPF_VL0 is down, line protocol is down
  Internet Address 0.0.0.0/0, Area 0, Attached via Not Attached
  Process ID 100, Router ID 3.3.3.3, Network Type VIRTUAL_LINK, Cost: 65535
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           65535     no          no            Base
```

Topic 6, Ticket 1: Switch Port Trunk

Topology Overview (Actual Troubleshooting lab design is for below network design)

Client Should have IP 10.2.1.3

EIGRP 100 is running between switch DSW1 & DSW2

OSPF (Process ID 1) is running between R1, R2, R3, R4

Network of OSPF is redistributed in EIGRP

BGP 65001 is configured on R1 with Webserver cloud AS 65002

HSRP is running between DSW1 & DSW2 Switches

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.

This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.

R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.

R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.

ASW1 and ASW2 are layer 2 switches.

NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.

The client workstations receive their IP address and default gateway via R4's DHCP server.

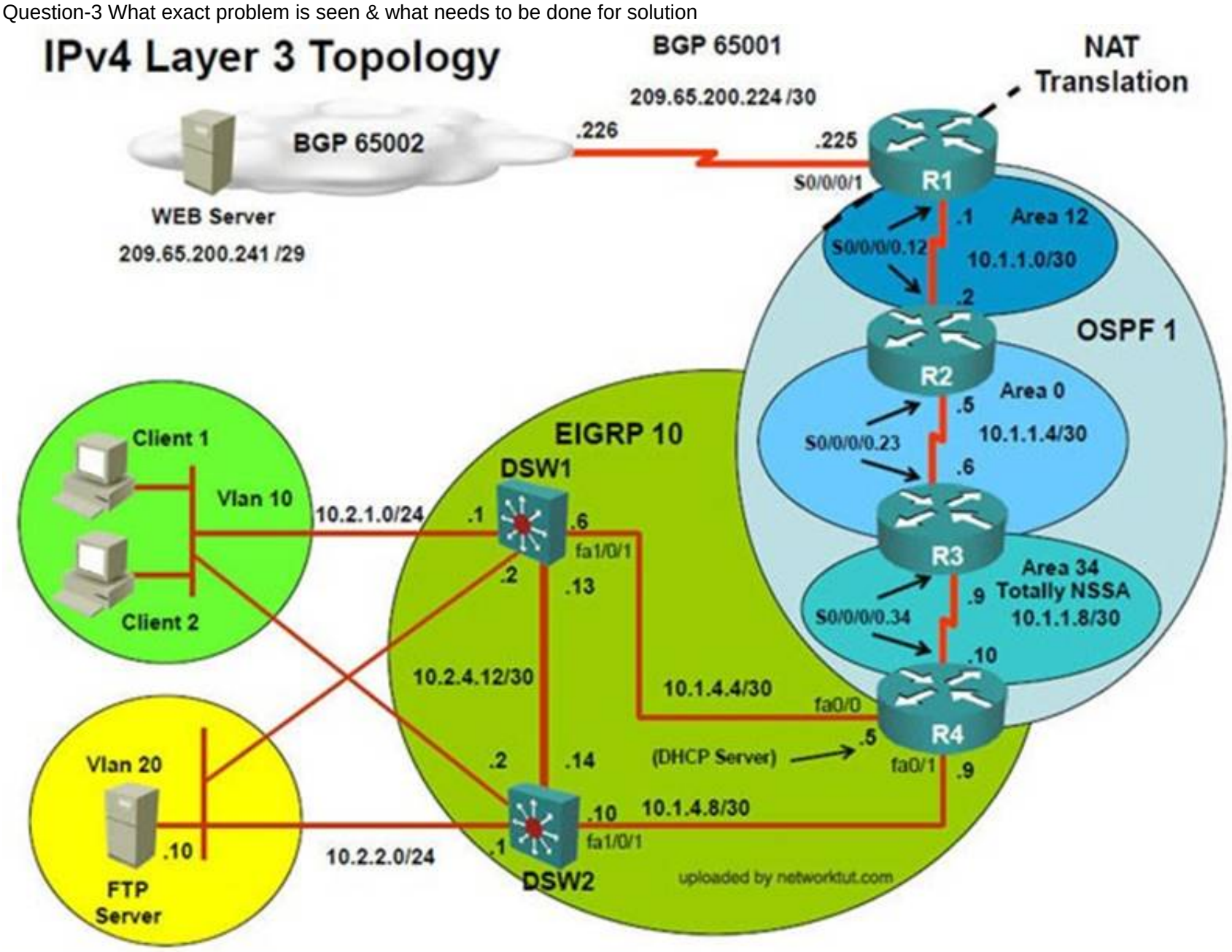
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

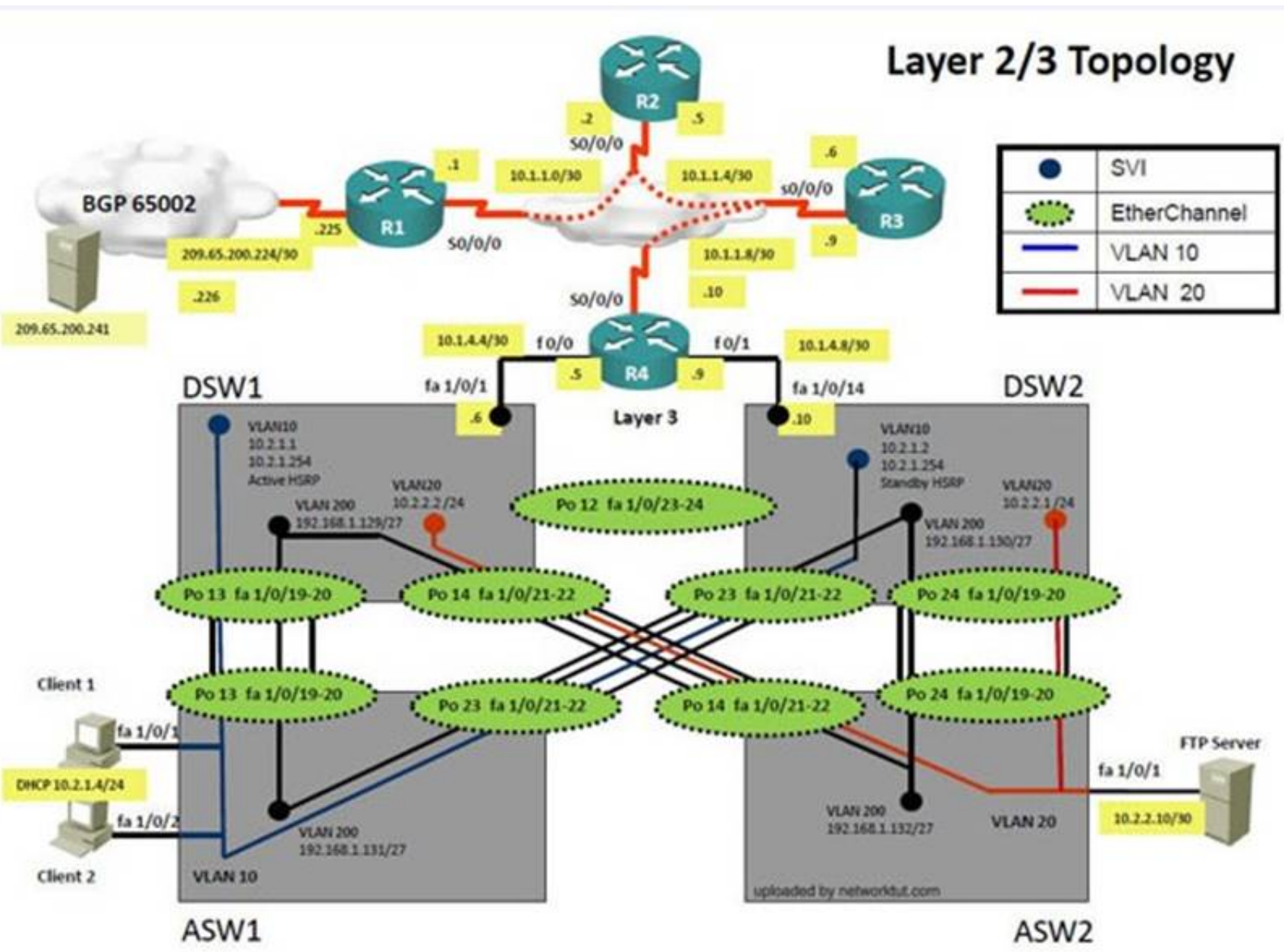
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.

The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

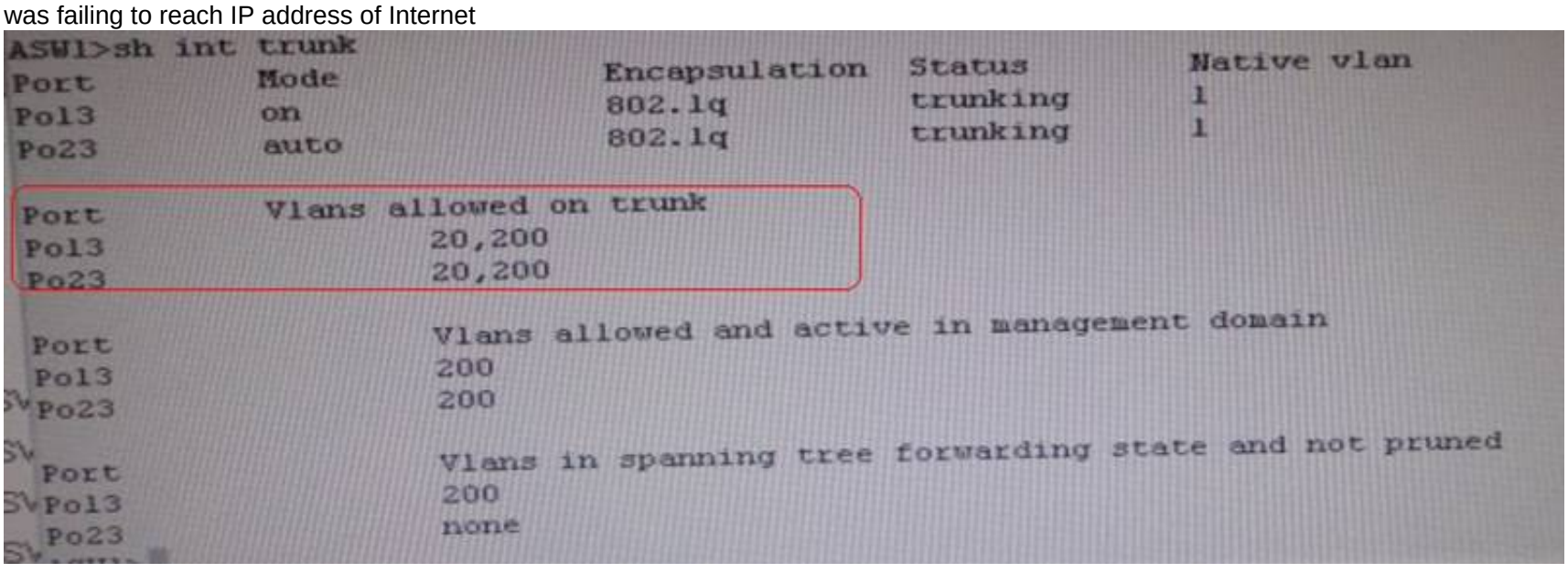
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution





Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 Ipconfig ----- Client will be getting 169.X.X.X
On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24
Sh run ------- & check for running config of int fa1/0/1 & fa1/0/2

==========
interface FastEthernet1/0/1switchport mode accessswitchport access vlan 10interface FastEthernet1/0/2switchport mode accessswitchport access vlan 10
==========
We need to check on ASW 1 trunk port the trunk Po13 & Po23 were receiving VLAN 20 & 200 but not VLAN 10 so that switch could not get DHCP IP address and was failing to reach IP address of Internet



Change required: On ASW1 below change is required for switch-to-switch connectivity..
int range portchannel13,portchannel23 switchport trunk allowed vlan none switchport trunk allowed vlan 10,200

NEW QUESTION 132
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, and FHRP services, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

A. NTP
B. Switch-to-Switch Connectivity
C. Access Vlans
D. Port Security
E. VLAN ACL / Port ACL
F. Switch Virtual Interface

Answer: B

Explanation: Since the Clients are getting an APIPA we know that DHCP is not working. However, upon closer examination of the ASW1 configuration we can see that the problem is not with DHCP, but the fact that the trunks on the port channels are only allowing VLANs 1-9, when the clients belong to VLAN 10. VLAN 10 is not traversing the trunk on ASW1, so the problem is with switch to switch connectivity, specifically the trunk configuration on ASW1.

NEW QUESTION 135
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, and FHRP services, a trouble ticket has been operated indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to Isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

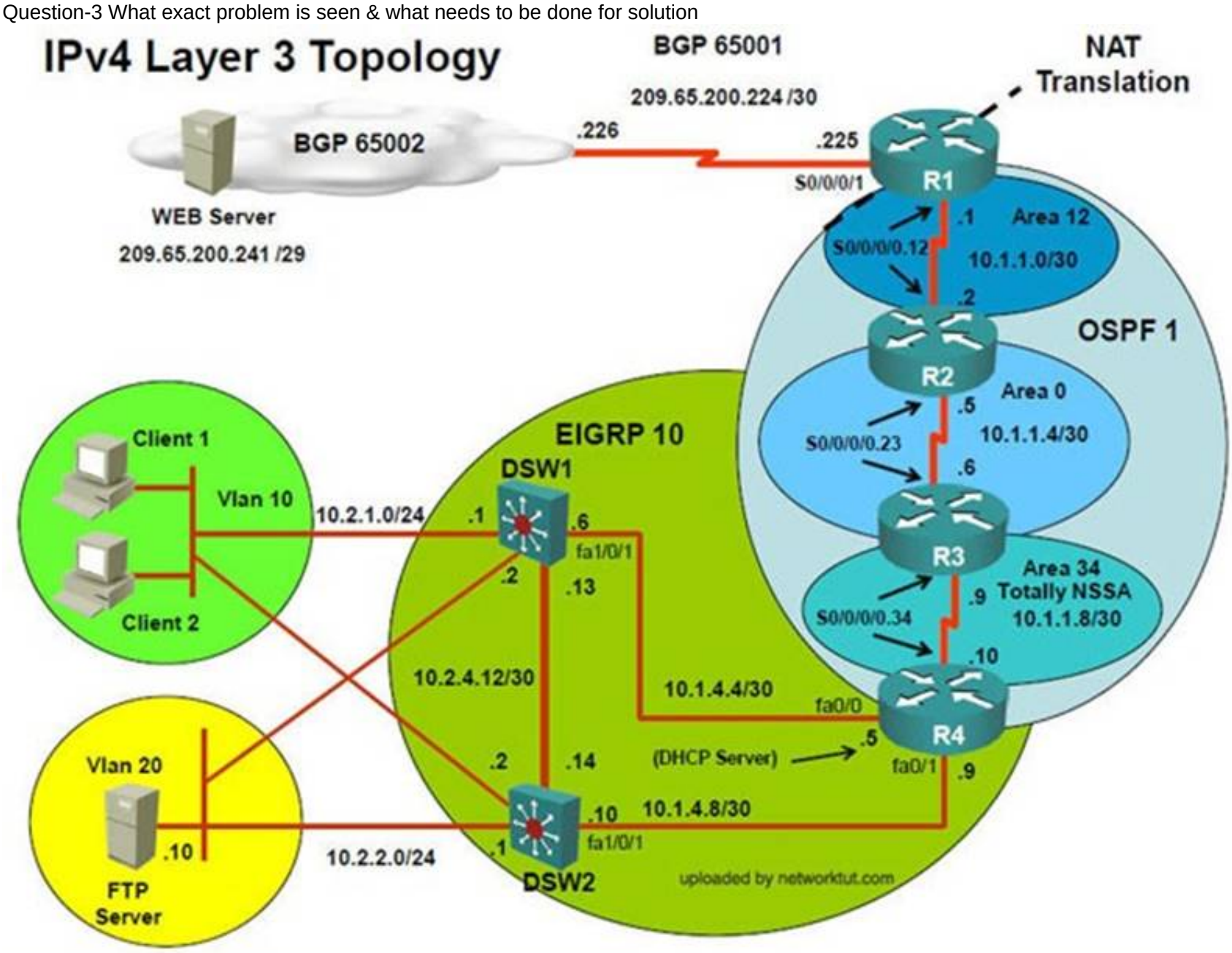
A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

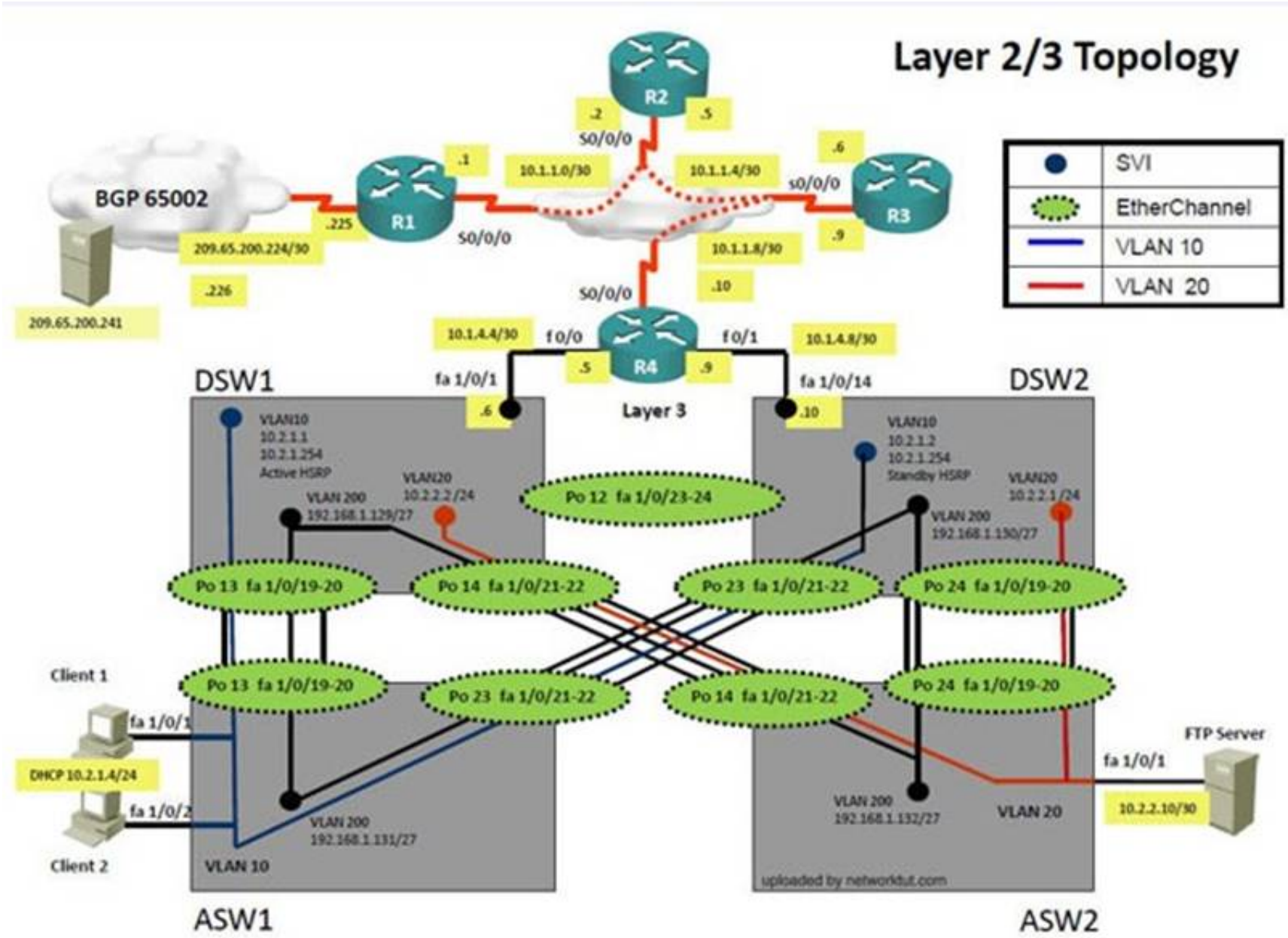
Answer: G

Explanation: Since the Clients are getting an APIPA we know that DHCP is not working. However, upon closer examination of the ASW1 configuration we can see that the problem is not with DHCP, but the fact that the trunks on the port channels are only allowing VLANs 1-9, when the clients belong to VLAN 10. VLAN 10 is not traversing the trunk on ASW1, so the problem is with the trunk configuration on ASW1.

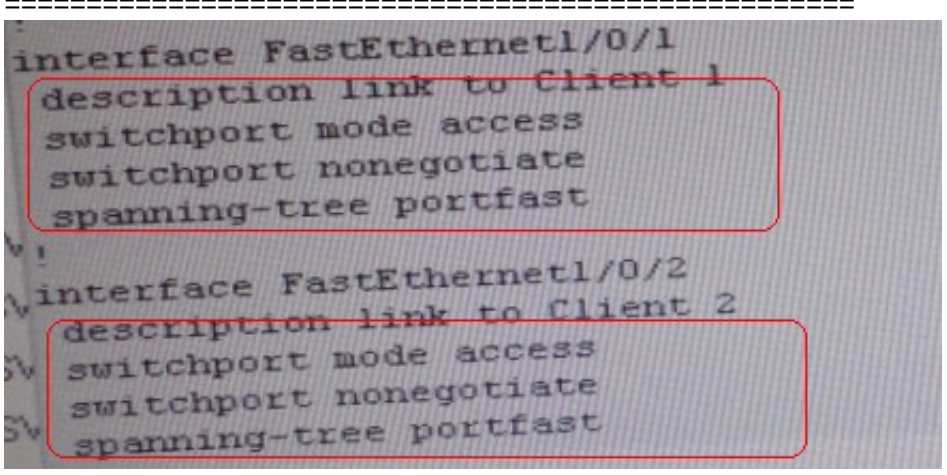
Topic 7, Ticket 2 : ACCESS VLAN
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.

R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several
implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution





Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 Ipconfig ----- Client will be getting 169.X.X.X
On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24
Sh run ------- & check for running config of int fa1/0/1 & fa1/0/2
==========



==========
Here we are not able to see access Vlan10 configured for Port Fa1/0/1 & Fa1/0/2
Change required: On ASW1, for configuring Access Vlan under interface fa1/0/1 & 1/0/2 we have to enable command switchport access vlan 10

NEW QUESTION 138
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: G

Explanation: The problem here is that VLAN 10 is not configured on the proper interfaces on switch ASW1.

NEW QUESTION 142
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

A. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport mode access vlan 10 command.
B. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport access mode vlan 10 command.
C. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport vlan 10 access command.
D. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport access vlan 10 command.

Answer: D

Explanation: The problem here is that VLAN 10 is not configured on the proper interfaces on switch ASW1.

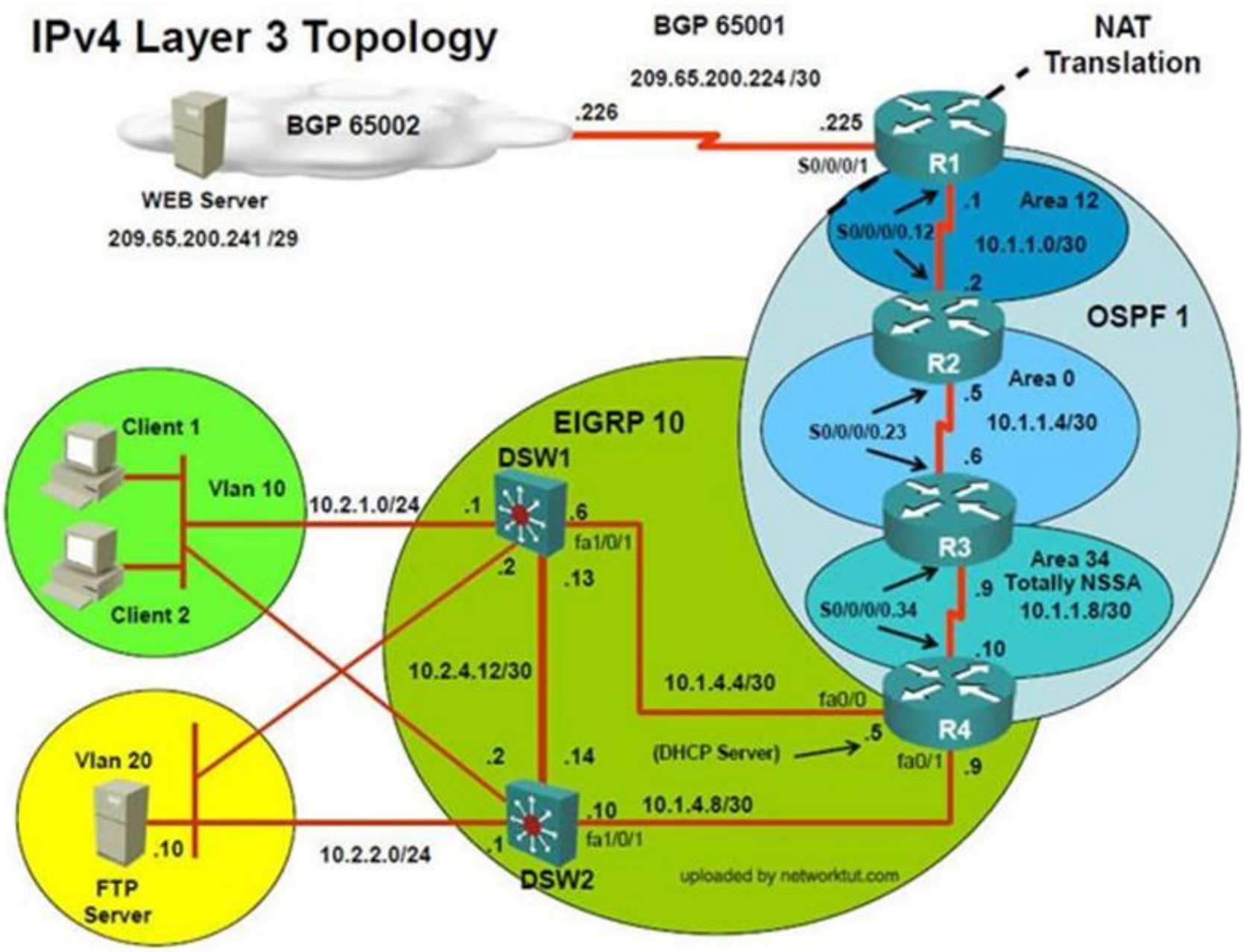
NEW QUESTION 145
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to switch technology?

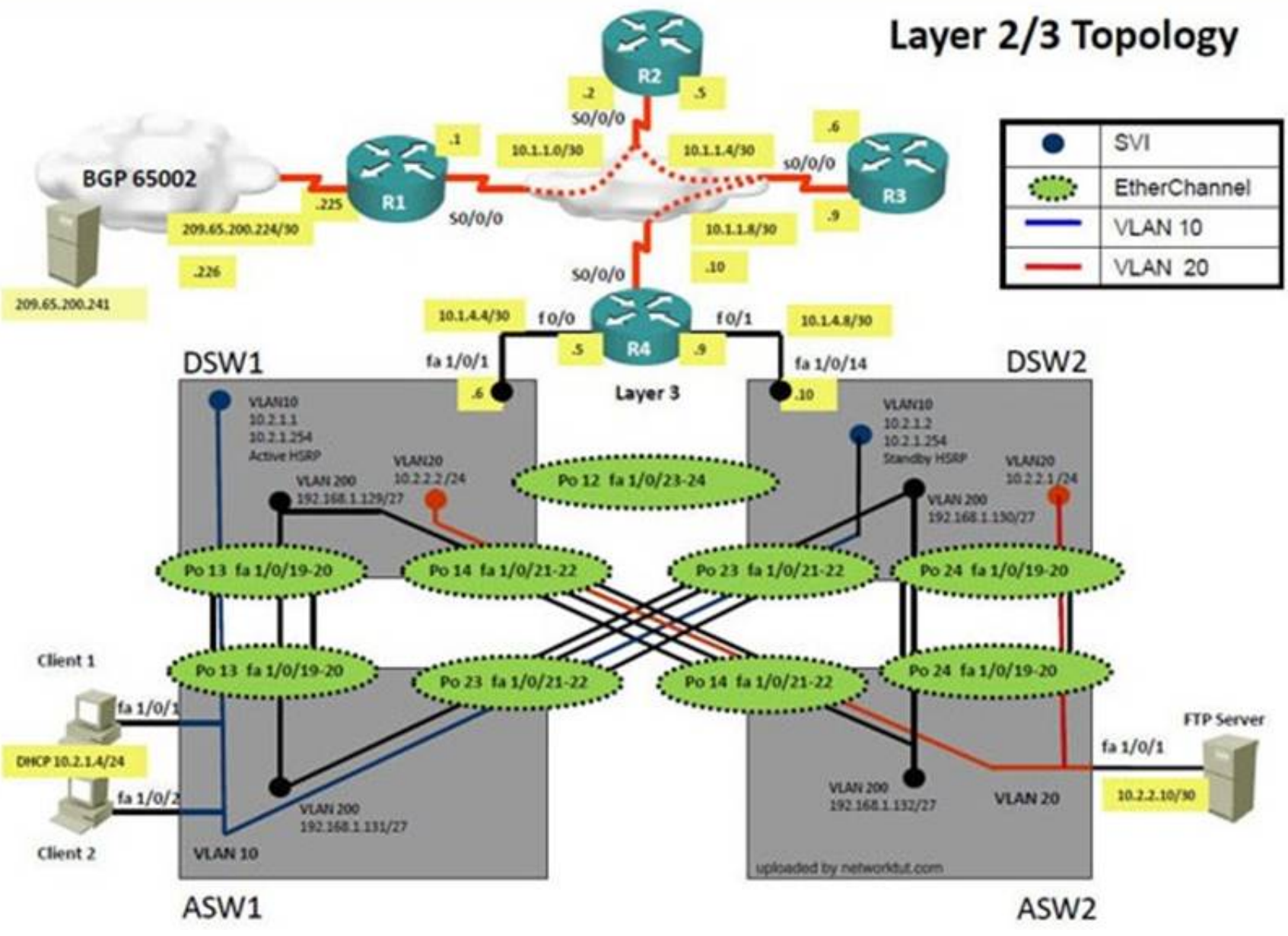
A. NTP
B. Switch-to-Switch Connectivity
C. Loop Prevention
D. Access Vlans
E. VLAN ACL Port ACL
F. Switch Virtual Interface
G. Port Security

Answer: D

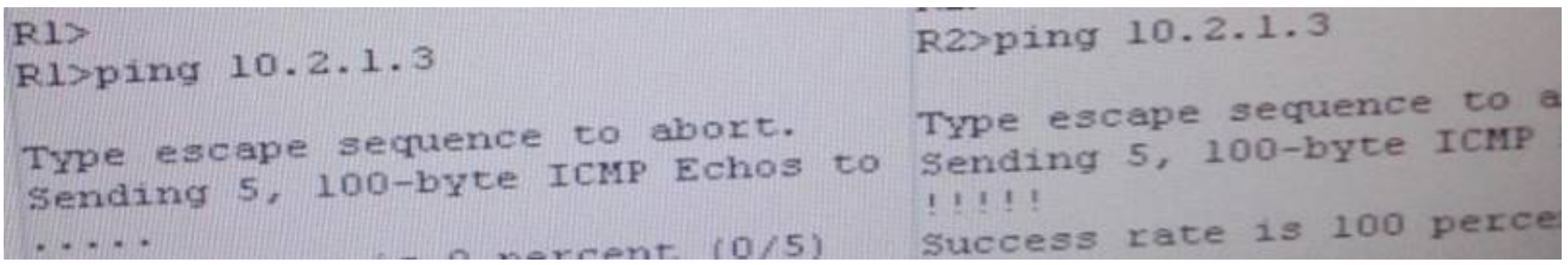
Explanation: The problem here is that VLAN 10 is not configured on the proper interfaces on switch ASW1.

Topic 8, Ticket 3 : OSPF Authentication
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several
implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========

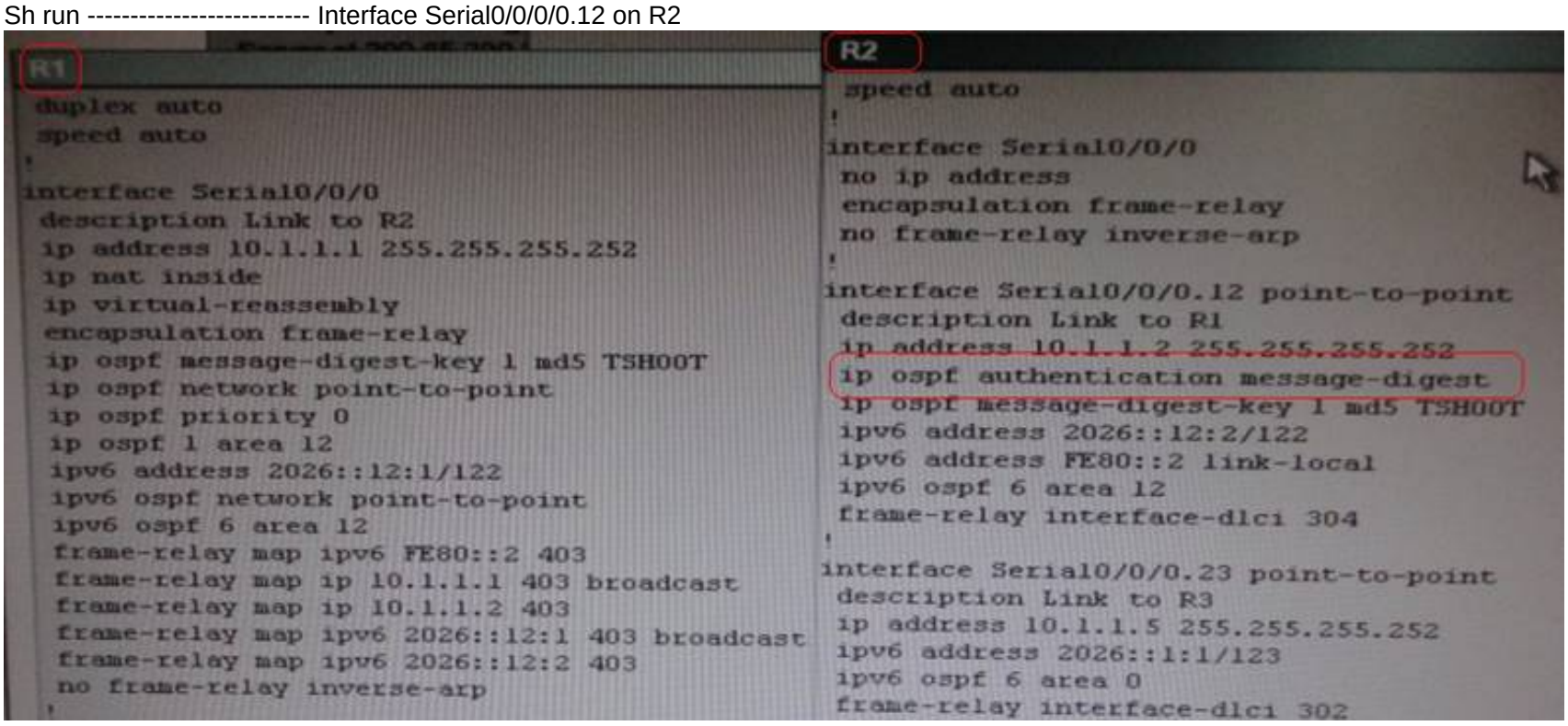




Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 Ipconfig ----- Client will be receiving IP address 10.2.1.3
IP 10.2.1.3 will be able to ping from R4 , R3, R2 but not from R1



Check for neighborship of ospf
sh ip ospf nei ----- Only one neighborship is forming with R2 & i.e. with R3
Since R2 is connected to R1 & R3 with routing protocol ospf than there should be 2 neighbors seen but only one is seen
Need to check running config of R2 & R3 for interface
Sh run ------------------------- Interface Serial0/0/0/0.12 on R2



Sh run ------------------------- Interface Serial0/0/0/0 on R1
Change required: On R1, for IPV4 authentication of OSPF command is missing and required to configure------ ip ospf authentication message-digest

NEW QUESTION 149
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: A

Explanation: On R1, for IPV4 authentication of OSPF the command is missing and required to configure------ ip ospf authentication message-digest

NEW QUESTION 150
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

A. BGP
B. NTP
C. IP NAT
D. IPv4 OSPF Routing
E. IPv4 OSPF Redistribution
F. IPv6 OSPF Routing
G. IPv4 layer 3 security

Answer: D

Explanation: On R1, for IPV4 authentication of OSPF the command is missing and required to configure------ ip ospf authentication message-digest

NEW QUESTION 153
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at

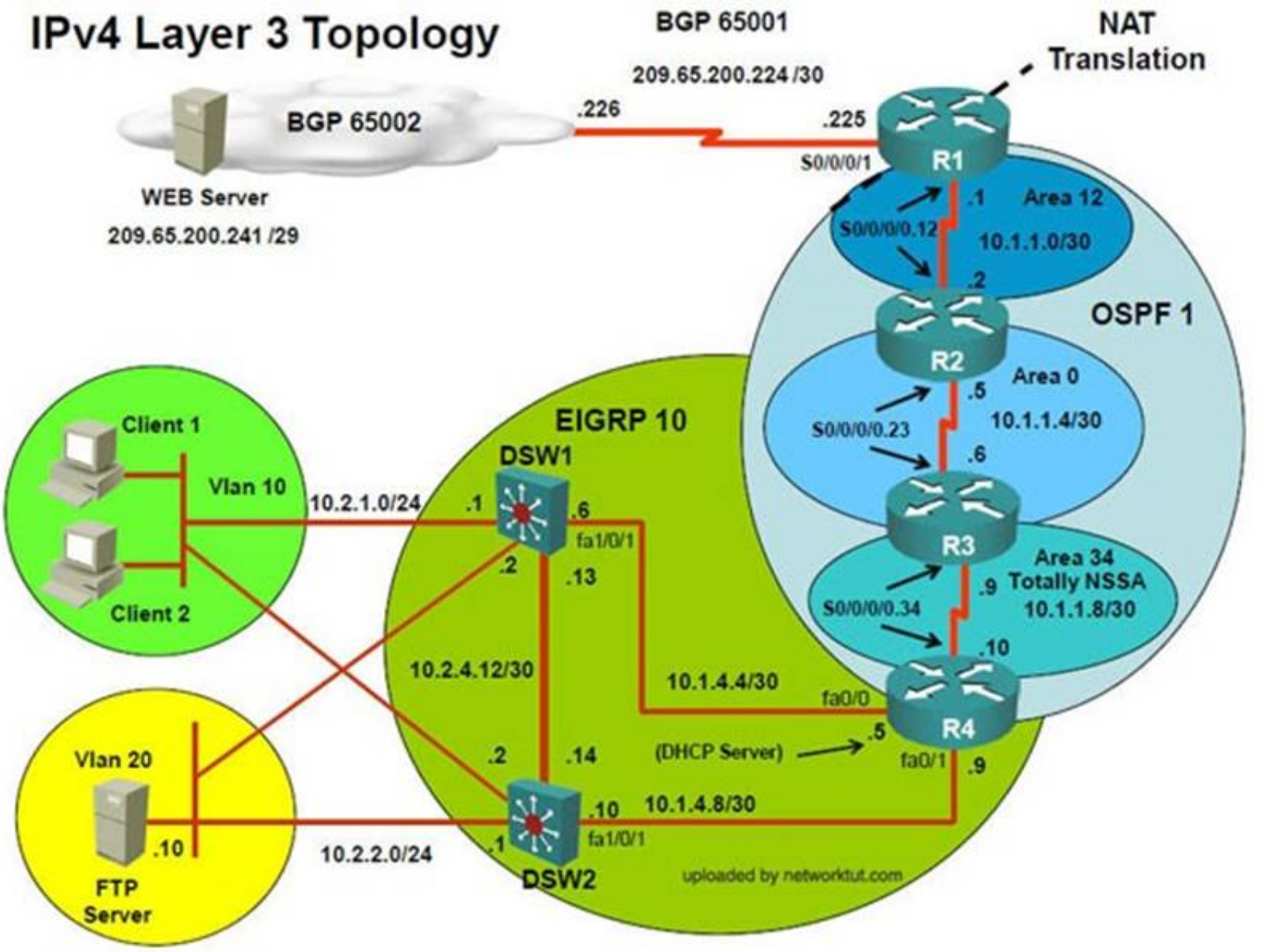
209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

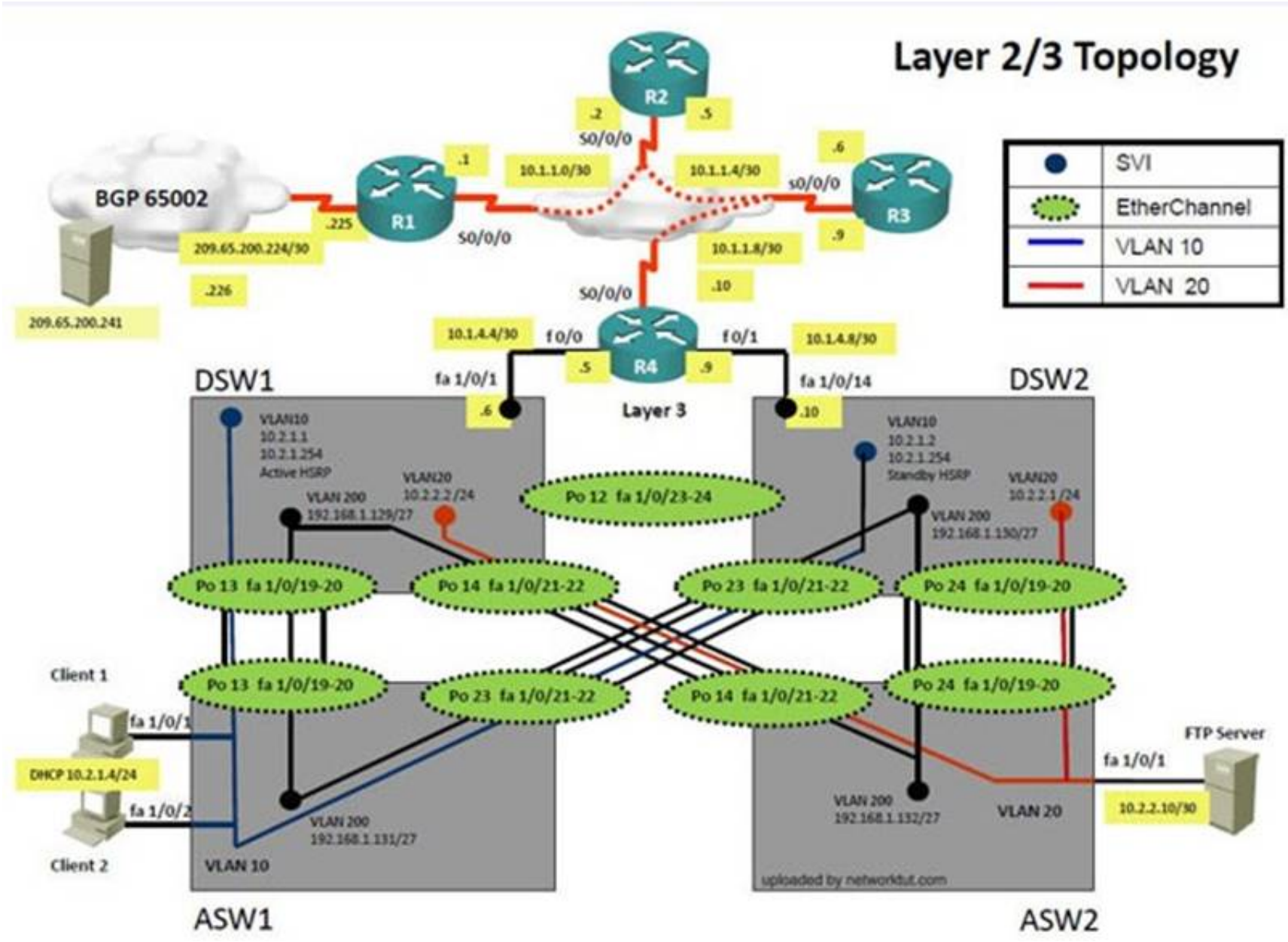
A. Enable OSPF authentication on the s0/0/0 interface using the ip ospf authentication message-digest command
B. Enable OSPF routing on the s0/0/0 interface using the network 10.1.1.0 0.0.0.255 area 12 command.
C. Enable OSPF routing on the s0/0/0 interface using the network 209.65.200.0 0.0.0.255 area 12 command.
D. Redistribute the BGP route into OSPF using the redistribute BGP 65001 subnet command.

Answer: A

Explanation: On R1, for IPV4 authentication of OSPF the command is missing and required to configure------ ip ospf authentication message-digest

Topic 9, Ticket 4 : BGP Neighbor
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be
presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution





Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ----- Client will be receiving IP address 10.2.1.3
IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1
Look for BGP Neighbourship
Sh ip bgp summary ----- No O/P will be seen
Check for interface IP & ping IP 209.65.200.225 ---- Reply will be received from Webserver interface
Look for peering IP address via sh run on R1 interface serial 0/0/1

```
interface Serial0/0/1
 description Link to ISP
 ip address 209.65.200.225 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 ntp broadcast client
 ntp broadcast key 1
```

```
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 neighbor 209.56.200.226 remote-as 65002
 no auto-summary
```

Since we are receiving icmp packets from Webserver interface on R1 so peering IP address under router BGP is configured wrong IP but with correct AS nos.
Change required: On R1 under router BGP Change neighbor 209.56.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65002

NEW QUESTION 156
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1

Answer: A

Explanation: The BGP neighbor statement is wrong on R1.

NEW QUESTION 159
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

A. Under the BGP process, enter the bgp redistribute-internal command.
B. Under the BGP process, bgp confederation identifier 65001command.
C. Deleted the current BGP process and reenter all of the command using 65002 as the AS number.
D. Under the BGP process, delete the neighbor 209.56.200.226 remote-as 65002 command and enter the neighbor 209.65.200.226 remote-as 65002 command.

Answer: D

Explanation: On R1 under router BGP change neighbor 209.56.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65002

NEW QUESTION 164
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1

Answer: A

Explanation: On R1 we need to add the client IP address for reachability to server to the access list that is used to specify which hosts get NATed.

NEW QUESTION 169
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

A. BGP
B. NTP
C. IP NAT
D. IPv4 OSPF Routing
E. IPv4 OSPF Redistribution
F. IPv6 OSPF Routing
G. IPv4 layer 3 security

Answer: G

Explanation: On R1, we need to permit IP 209.65.200.222/30 under the access list.

NEW QUESTION 171
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

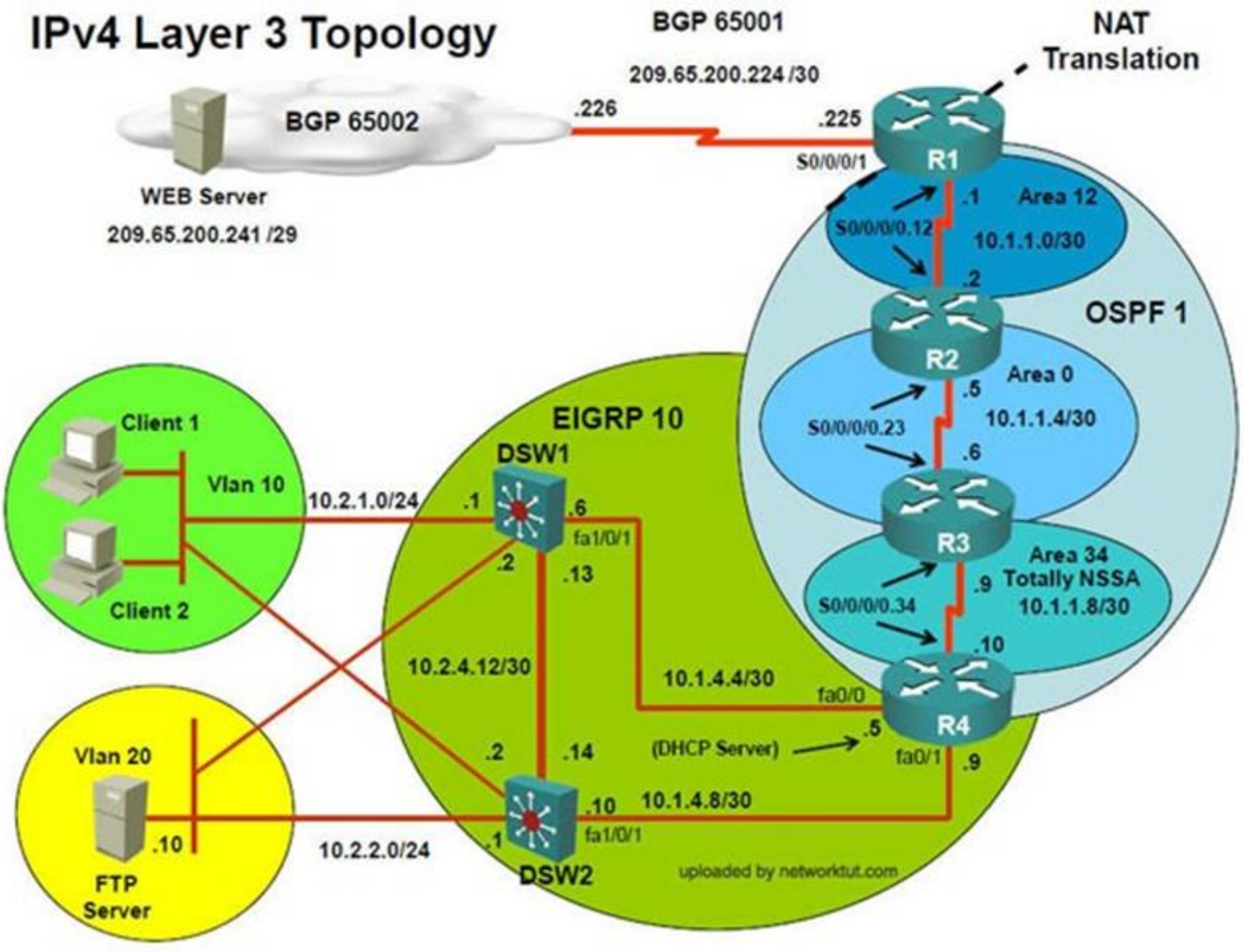
A. Under the interface Serial0/0/1 enter the ip access-group edge_security out command.
B. Under the ip access-list extended edge_security configuration add the permit ip 209.65.200.224 0.0.0.3 any command.
C. Under the ip access-list extended edge_security configuration delete the deny ip 10.0.0.0.0 0.255.255.255 any command.
D. Under the interface Serial0/0/0 configuration delete the ip access-group edge_security in command and enter the ip access-group edge_security out command.

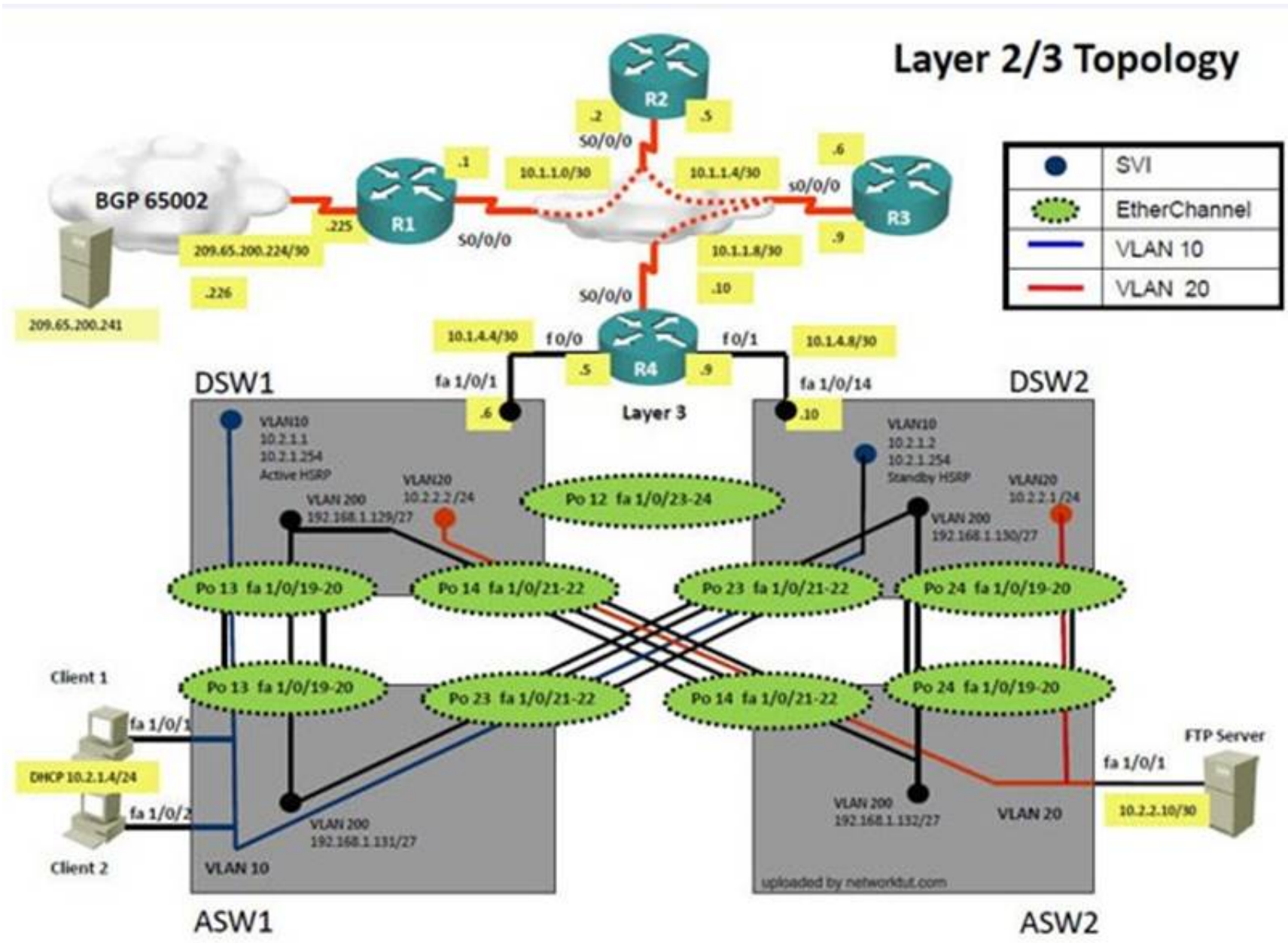
Answer: B

Explanation: On R1, we need to permit IP 209.65.200.222/30 under the access list.

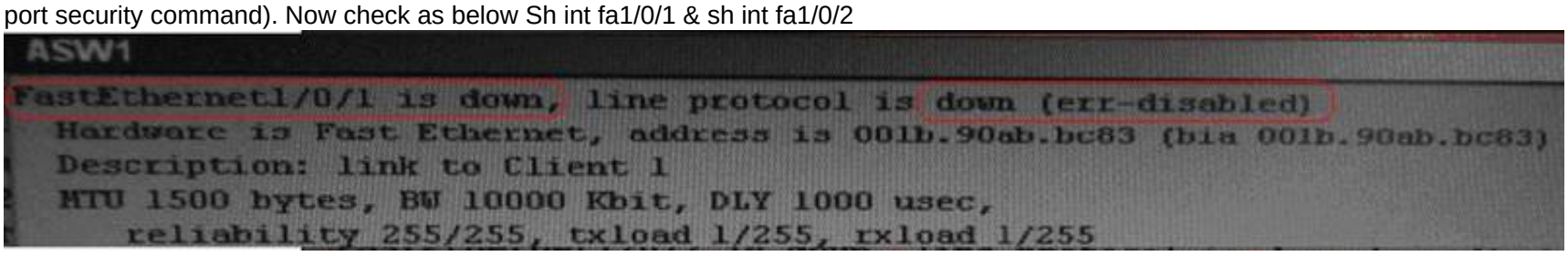
Topic 12, Ticket 7 : Port Security
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2

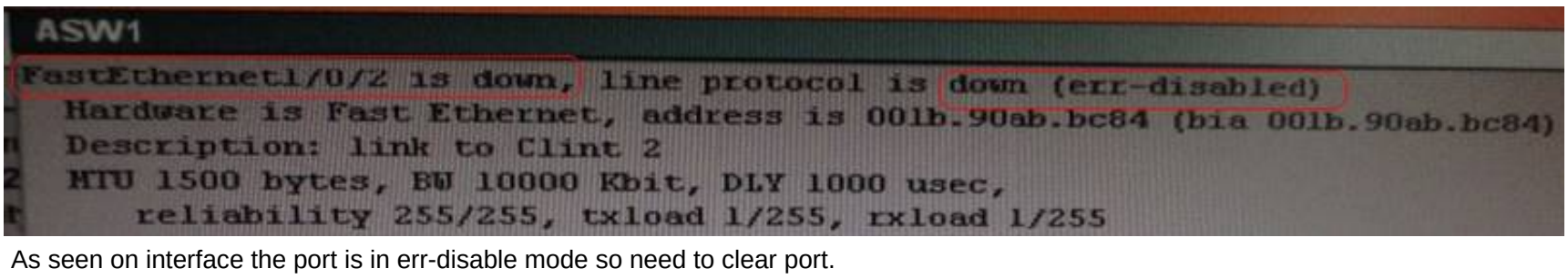
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several
implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========





Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ----- Client will be getting 169.X.X.X
On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned but when we checked interface it was showing down
Sh run ------- check for running config of int fa1/0/1 & fa1/0/2 (switchport access Vlan 10 will be there with switch
port security command). Now check as below Sh int fa1/0/1 & sh int fa1/0/2





As seen on interface the port is in err-disable mode so need to clear port.
Change required: On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2.

NEW QUESTION 175
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: G

Explanation: port security needs is configured on ASW1.

NEW QUESTION 180
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

A. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security interface configuration command
B. Then in exec mode clear errdisable interface fa 1/01 – 2 vlan 10 command
C. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security, followed by shutdown, no shutdown interface configuration commands.
D. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security interface configuration commands.
E. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security interface configuration command
F. Then in exec mode clear errdisable interface fa 1/0/1, then clear errdisable interface fa 1/0/2 commands.

Answer: B

Explanation: On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2. Reference:
http://www.cisco.com/en/US/tech/ABC389/ABC621/technologies_tech_note09186a00806cd87b.shtml
==========

NEW QUESTION 185
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: D

Explanation: On R4, in the redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue. It references route-map OSPF_to_EIGRP but the actual route map is called OSPF->EIGRP.

NEW QUESTION 190
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

A. NTP
B. IP DHCP Server
C. IPv4 OSPF Routing
D. IPv4 EIGRP Routing
E. IPv4 Route Redistribution
F. IPv6 RIP Routing
G. IPv6 OSPF Routing
H. IPv4 and IPv6 Interoperability
I. IPv4 layer 3 security

Answer: E

Explanation: On R4, in the redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue. It references route-map OSPF_to_EIGRP but the actual route map is called OSPF->EIGRP.

NEW QUESTION 191
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: D

Explanation: The EIGRP AS number configured on R4 is wrong.

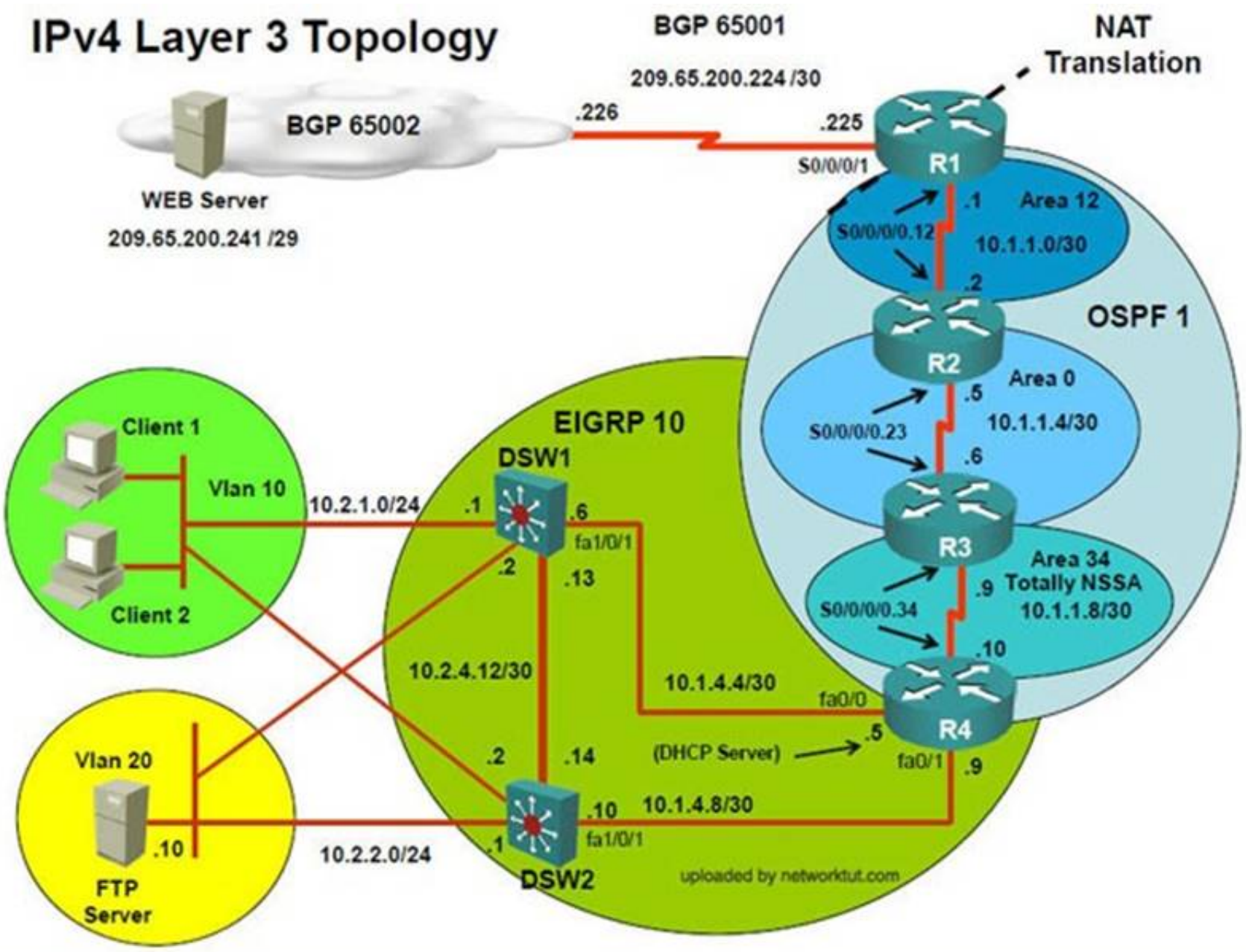
NEW QUESTION 196
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

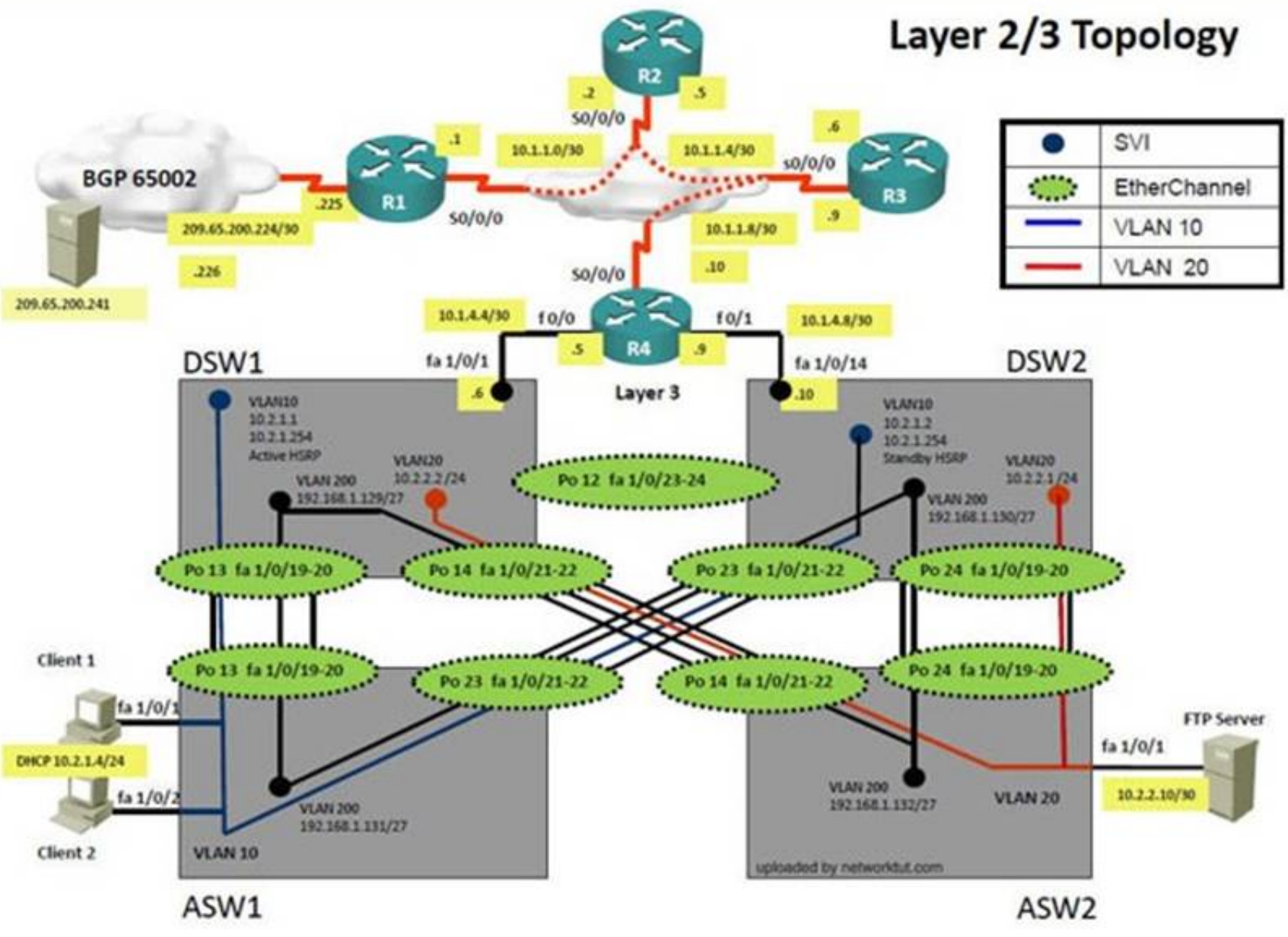
A. NTP
B. IP DHCP Server
C. IPv4 OSPF Routing
D. IPv4 EIGRP Routing
E. IPv4 Route Redistribution
F. IPv6 RIP Routing
G. IPv6 OSPF Routing
H. IPv4 and IPv6 Interoperability
I. IPv4 layer 3 security

Answer: D

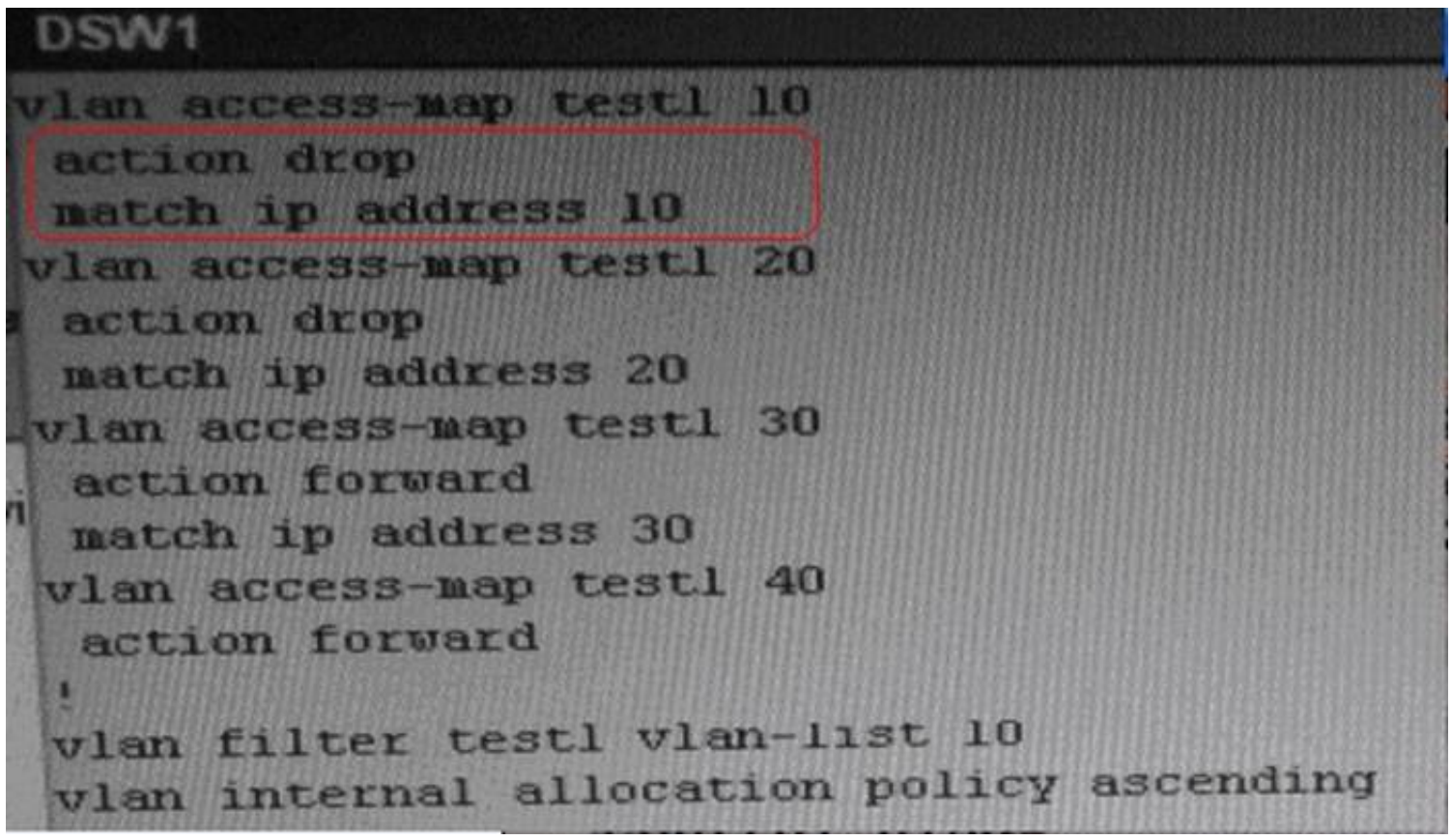
Explanation: On R4, IPV4 EIGRP Routing, need to change the EIGRP AS number from 1 to 10 since DSW1 & DSW2 is configured to be in EIGRP AS number 10.

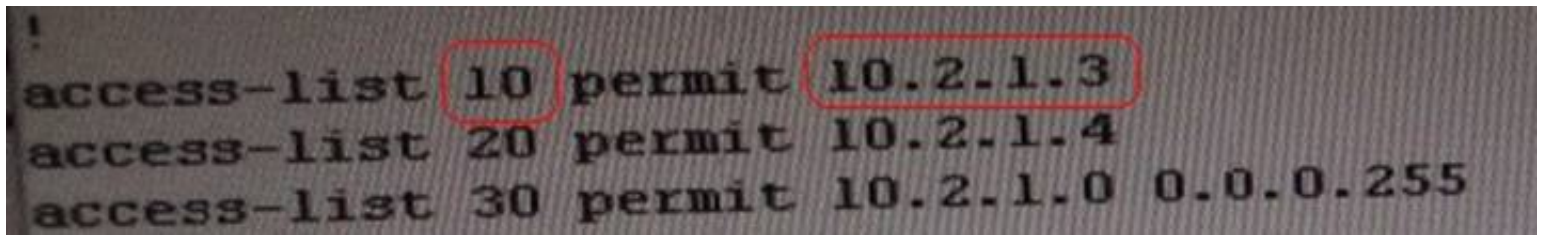
Topic 15, Ticket 10 : VLAN Access Map
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several
implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========





Client 1 is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ----- Client will be receiving IP address 10.2.1.3
From Client PC we can ping 10.2.1.254….
But IP 10.2.1.3 is not able to ping from R4, R3, R2, R1





Change required: On DSW1, VALN ACL, Need to delete the VLAN access-map test1 whose action is to drop access-list 10; specifically 10.2.1.3

NEW QUESTION 197
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: E

Explanation: On DSW1, VALN ACL, Need to delete the VLAN access-map test1 whose action is to drop access-list 10; specifically 10.2.1.3

NEW QUESTION 200
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

A. NTP
B. IP DHCP Helper
C. IPv4 EIGRP Routing
D. IPv6 RIP Routing
E. IPv4 layer 3 security
F. Switch-to-Switch Connectivity
G. Loop Prevention
H. Access Vlans
I. Port Security
J. VLAN ACL / Port ACL
K. Switch Virtual Interface

Answer: J

Explanation: On DSW1, VALN ACL, Need to delete the VLAN access-map test1 whose action is to drop access-list 10; specifically 10.2.1.3

NEW QUESTION 204

The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened DSW1 will not become the active router for HSRP group 10.
Use the supported commands to isolated the cause of this fault and answer the following questions. What is the solution to the fault condition?

A. Under the interface vlan 10 configuration enter standby 10 preempt command.
B. Under the track 1 object configuration delete the threshold metric up 1 down 2 command and enter the threshold metric up 61 down 62 command.
C. Under the track 10 object configuration delete the threshold metric up 61 down 62 command and enter the threshold metric up 1 down 2 command.
D. Under the interface vlan 10 configuration delete the standby 10 track1 decrement 60 command and enter the standby 10 track 10 decrement 60 command.

Answer: D

Explanation: On DSW1, related to HSRP, under VLAN 10 change the given track 1 command to instead use the track 10 command.

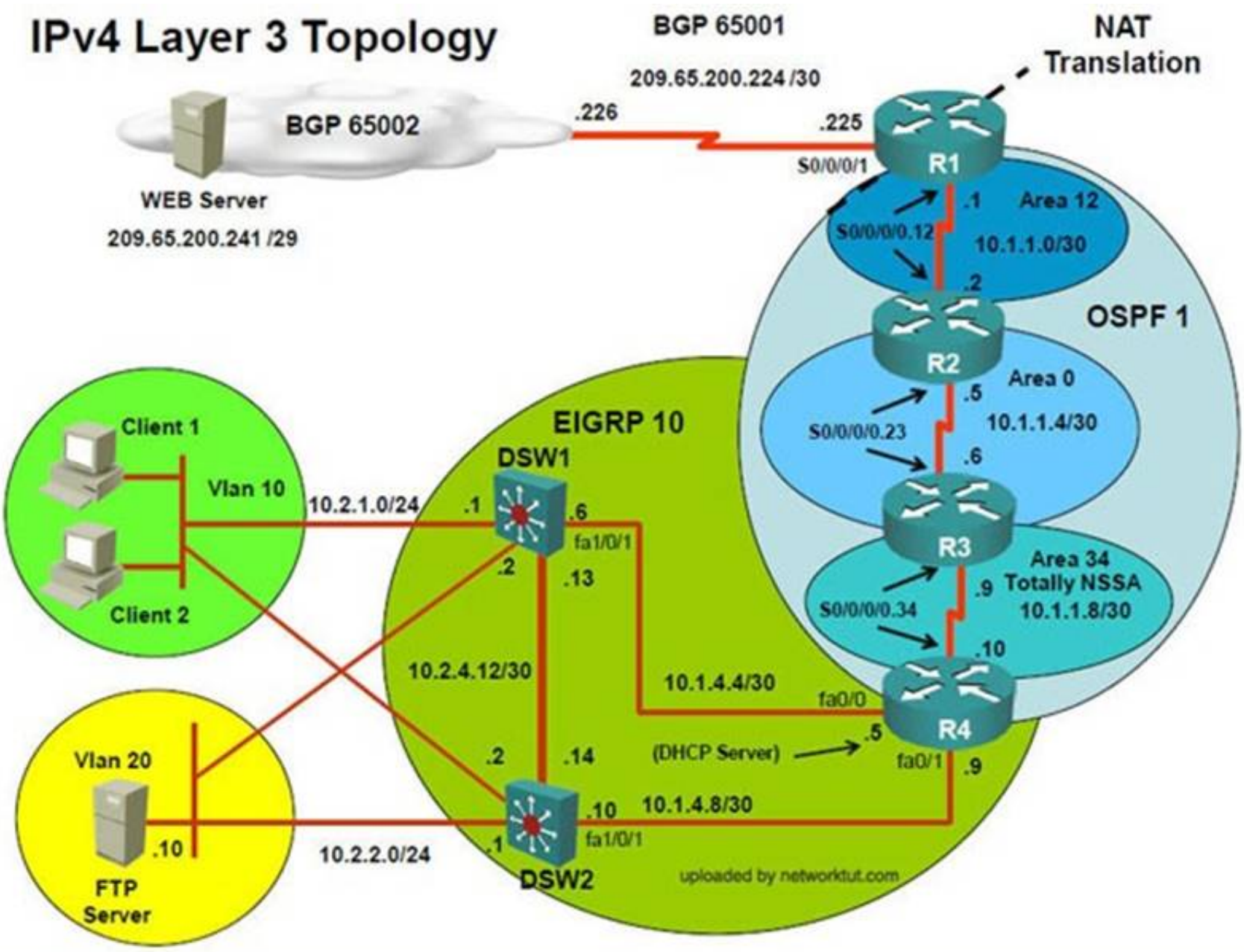
NEW QUESTION 206
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network
addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened DSW1 will not become the active router for HSRP group 10.
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

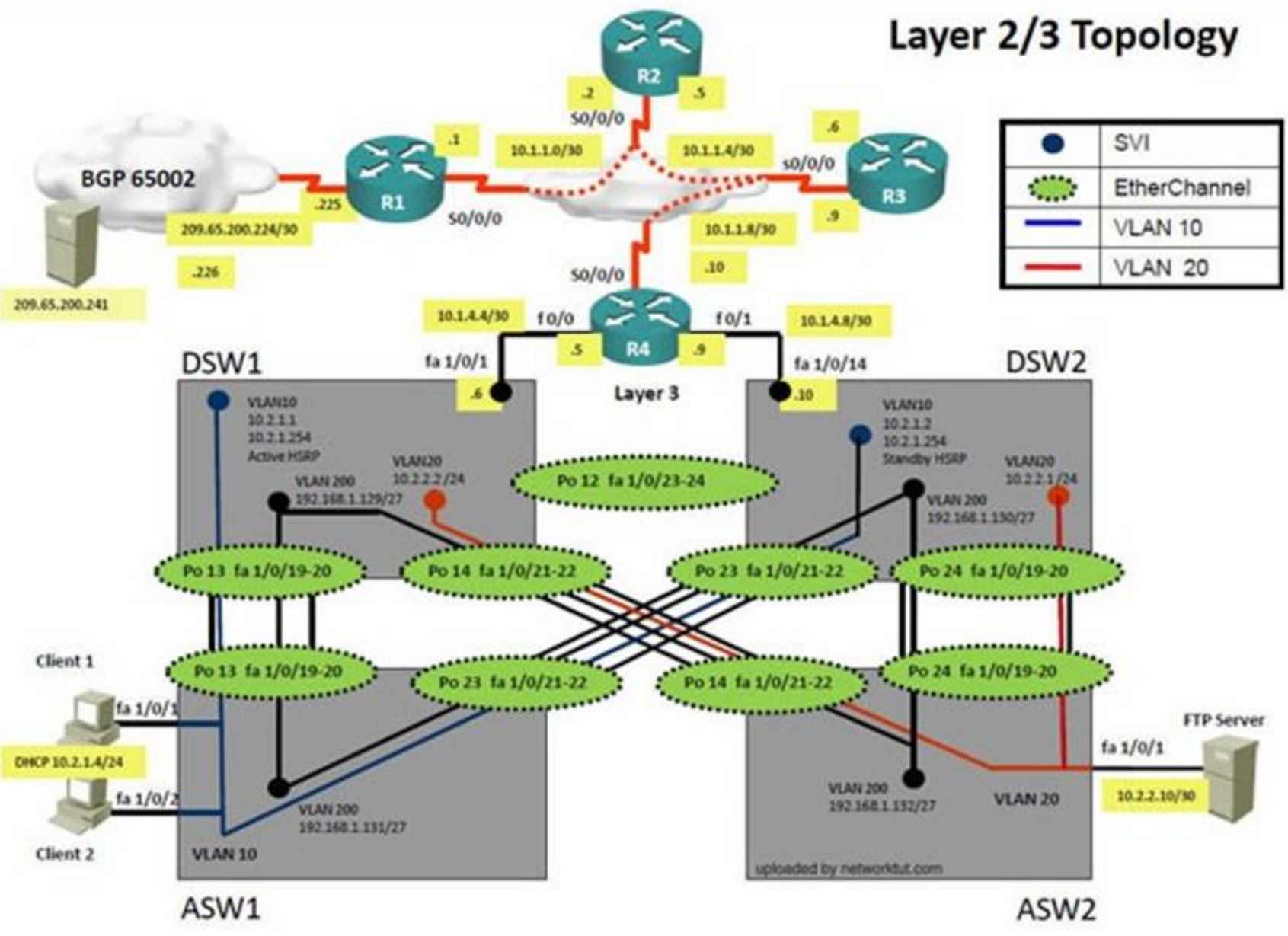
A. NTP
B. HSRP
C. IP DHCP Helper
D. IPv4 EIGRP Routing
E. IPv6 RIP Routing
F. IPv4 layer 3 security
G. Switch-to-Switch Connectivity
H. Loop Prevention
I. Access Vlans
J. Port Security
K. VLAN ACL/Port ACL
L. Switch Virtual Interface

Answer: B

Explanation: On DSW1, related to HSRP, under VLAN 10 change the given track 1 command to instead use the track 10 command.

Topic 18, Ticket 13: DHCP Issue
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be
presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========





The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and, device security, a trouble ticket has been opened indicating DSW1 will not become the active router for HSRP group 10.

Solution

Steps need to follow as below:-

When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ----- Client will be receiving Private IP address 169.254.X.X

From ASW1 we can ping 10.2.1.254….

On ASW1 VLAN10 is allowed in trunk & access command will is enabled on interface but DHCP IP address is not recd.

On R4 the DHCP IP address is not allowed for network 10.2.1.0/24 which clearly shows the problem lies on R4 & the problem is with DHCP

NEW QUESTION 211
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolate the cause of this fault and answer the following question. The fault condition is related to which technology?

A. NTP
B. IP DHCP Server
C. Ipv4 OSPF Routing
D. Ipv4 EIGRP Routing.
E. Ipv4 Route Redistribution.
F. Ipv6 RIP Routing
G. Ipv6 OSPF Routing
H. Ipv4 and Ipv6 Interoperability
I. Ipv4 layer 3 security.

Answer: B

Explanation: On R4 the DHCP IP address is not allowed for network 10.2.1.0/24 which clearly shows the problem lies on R4 & the problem is with DHCP

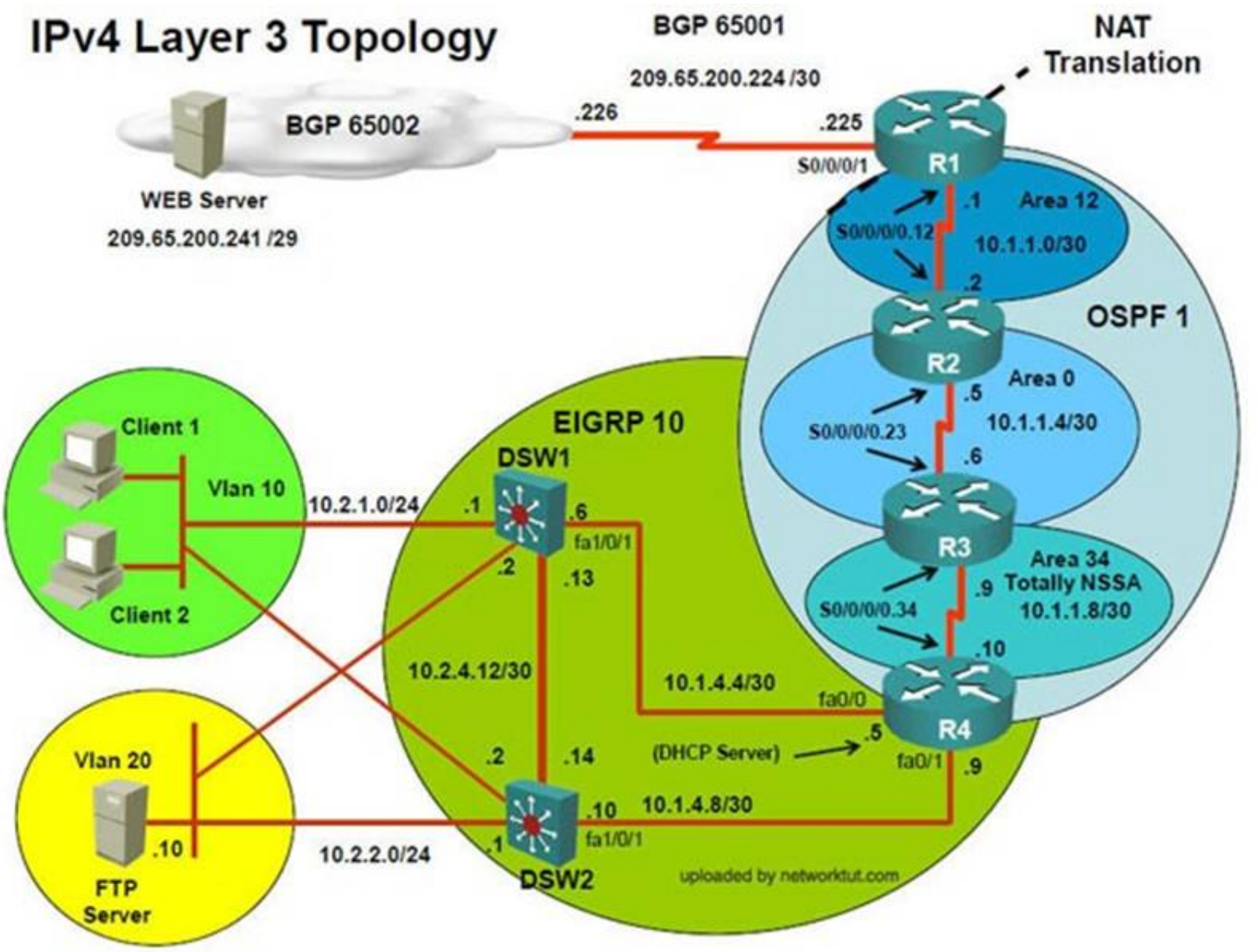
NEW QUESTION 216
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolate the cause of this fault and answer the following question. What is the solution to the fault condition?

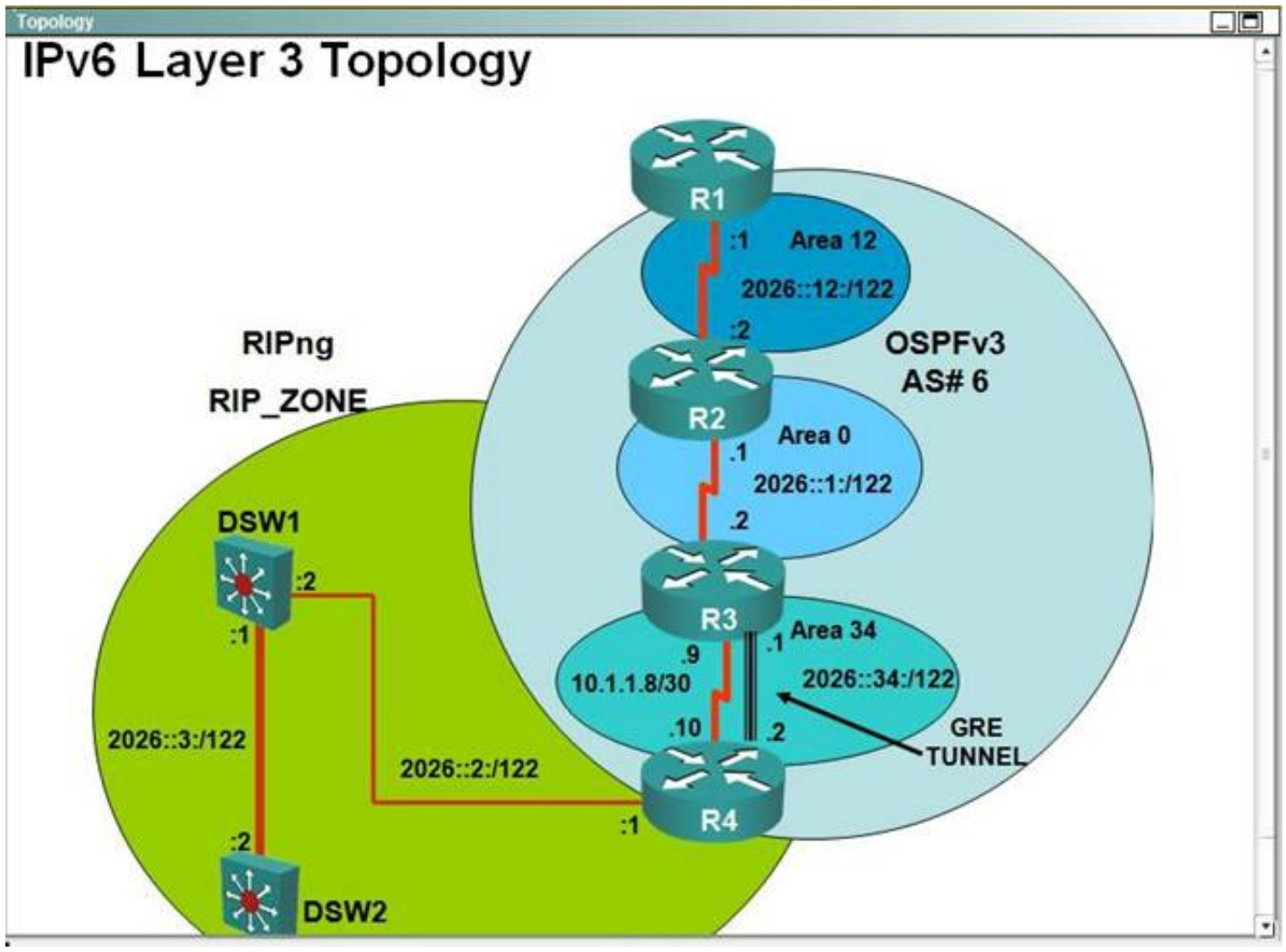
A. Under the global configuration, delete the no ip dhcp use vrf connected command.
B. Under the IP DHCP pool configuration, delete the default -router 10.2.1.254 command and enter the default-router 10.1.4.5 command.
C. Under the IP DHCP pool configuration, delete the network 10.2.1.0 255.255.255.0 command and enter the network 10.1.4.0 255.255.255.0 command.
D. Under the IP DHCP pool configuration, issue the no ip dhcp excluded-address 10.2.1.1 10.2.1.253 command and enter the ip dhcp excluded-address 10.2.1.1 10.2.1.2 command.

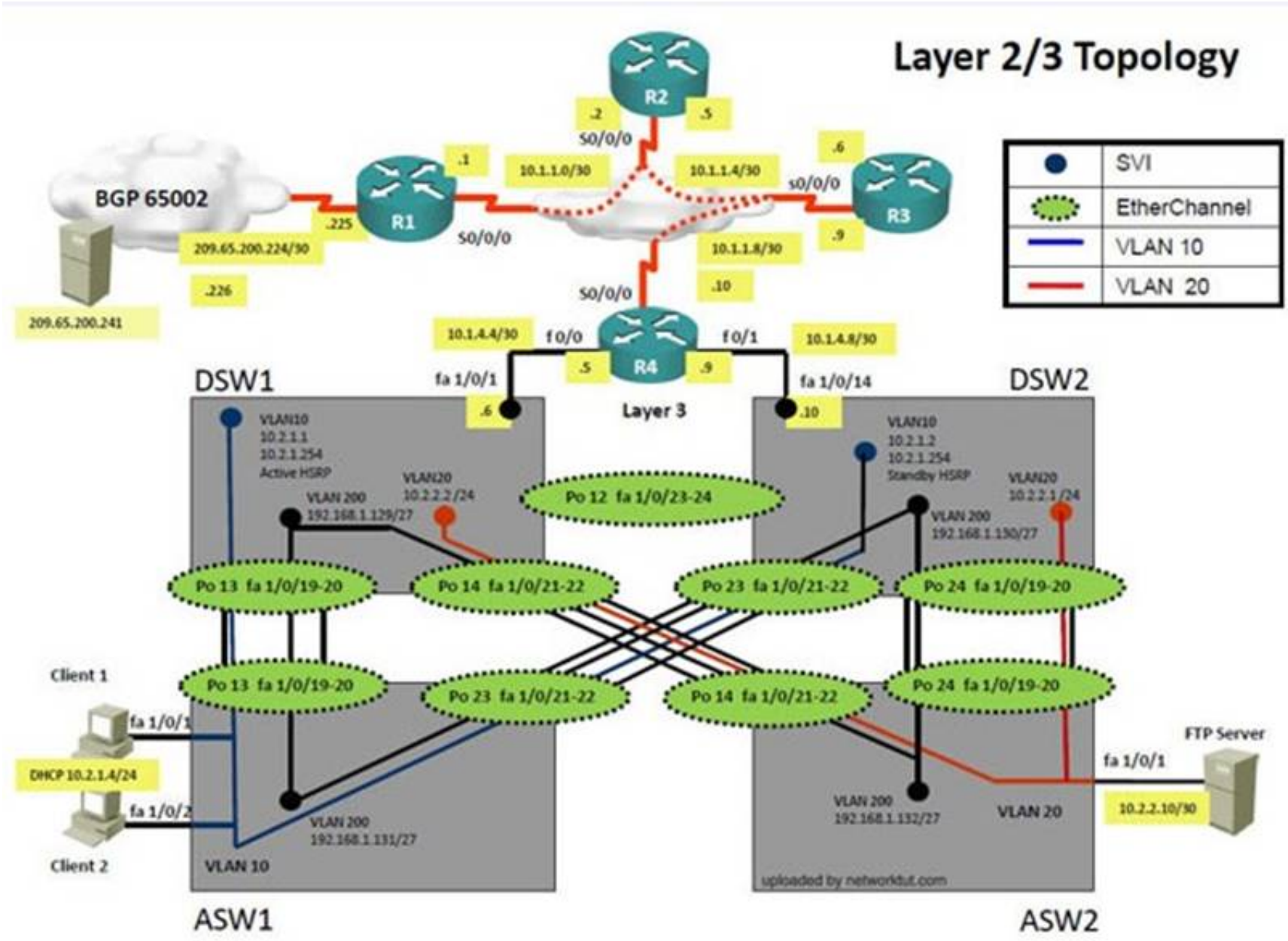
Answer: D

Explanation: On R4 the DHCP IP address is not allowed for network 10.2.1.0/24 which clearly shows the problem lies on
R4 & the problem is with DHCP

Topic 19, Ticket 14: IPv6 Routing Issue 1
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be
presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========


IPv4 Layer 3 Topology
BGP 65001
NAT Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
DSW1
Client 1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.10
Client 2
.2
.13
10.2.4.12/30
10.1.4.4/30
fa0/0
R4
.5
Vlan 20
.2
.14
(DHCP Server)
fa0/1
.9
.10
10.1.4.8/30
.10
.1
fa1/0/1
10.2.2.0/24
FTP Server
DSW2
uploaded by networktut.com


Topology
IPv6 Layer 3 Topology
R1
:1
Area 12
2026::12:/122
:2
RIPng
RIP_ZONE
OSPFv3
AS# 6
R2
Area 0
.1
2026::1:/122
.2
DSW1
R3
:2
:1
.1
Area 34
.9
10.1.1.8/30
2026::34:/122
.10
.2
GRE
TUNNEL
2026::3:/122
2026::2:/122
R4
:1
:2
DSW2



Questions

The implementation group has been using the test bed to do an IPv6 'proof-of-concept'. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Using the supported commands to isolate the cause of this fault and answer the following questions.

NEW QUESTION 217
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).
Use the supported commands to isolate the cause of this fault and answer the following question.
On which device is the fault condition located?

A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: B

Explanation: Start to troubleshoot this by pinging the loopback IPv6 address of DSW2 (2026::102:1). This can be pinged from DSW1, R4, and R3, which leads us to believe that the issue is with R2. Going further, we can see that R2 only has an IPV6 OSPF neighbor of R1, not R3:
Screen Shot 2015-03-11 at 10

```
R2>show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.1.10.1         1   FULL/  -        00:00:32    6               Serial0/0/0.12


R2>
```

We can then see that OSPFv3 has not been enabled on the interface to R3: Screen Shot 2015-03-11 at 10

```
!
interface Serial0/0/0.12 point-to-point
 description Link to R1
 ip address 10.1.1.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 TSHOOT
 ipv6 address 2026::12:2/122
 ipv6 address FE80::2 link-local
 ipv6 ospf 6 area 12
 frame-relay interface-dlci 304
!
interface Serial0/0/0.23 point-to-point
 description Link to R3
 ip address 10.1.1.5 255.255.255.252
 ipv6 address 2026::1:1/123
 frame-relay interface-dlci 302
!
interface Serial0/0/1
```

So the problem is with R2, related to IPV6 Routing, and the fix is to enable the “ipv6 ospf 6 area 0”command under the serial 0/0/0.23 interface.

NEW QUESTION 222
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).
Use the supported commands to isolate the cause of this fault and answer the following question. The fault condition is related to which technology?

A. NTP
B. IPv4 OSPF Routing
C. IPv6 OSPF Routing
D. IPv4 layer 3 security

Answer: C

Explanation: Since we are unable to ping the IPv6 address, the problem is with IPv6 OSPF Routing.

NEW QUESTION 227
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).
Use the supported commands to isolate the cause of this fault and answer the following question. What is the solution to the fault condition?

A. Under the interface SerialO/0/0.23 configuration enter the ipv6 ospf 6 area 0 command.
B. Under the interface SerialO/0/0.12 configuration enter the ipv6 ospf 6 area 12 command.
C. Under ipv6 router ospf 6 configuration enter the network 2026::1:/122 area 0 command.
D. Under ipv6 router ospf 6 configuration enter the no passive-interface default command

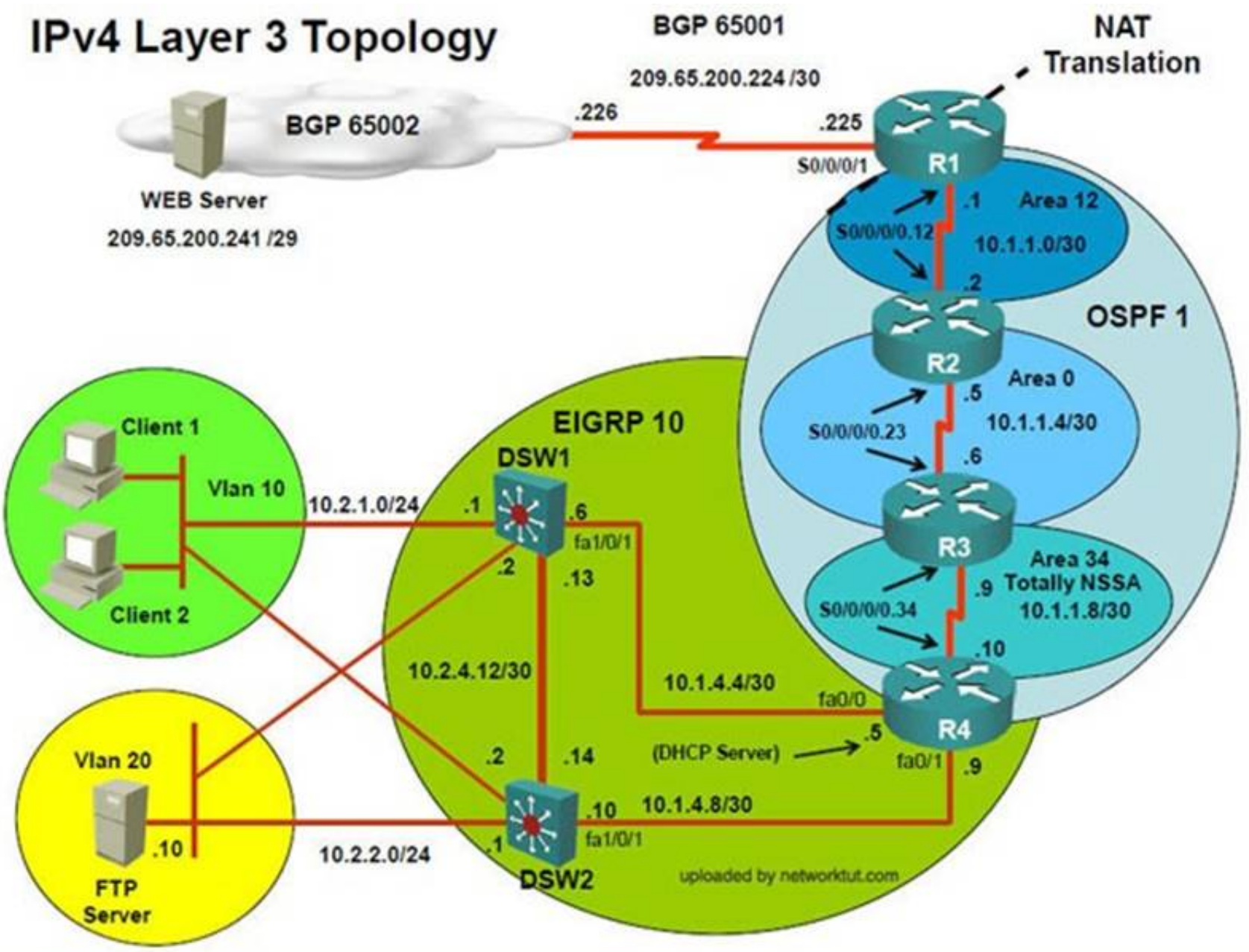
Answer: A

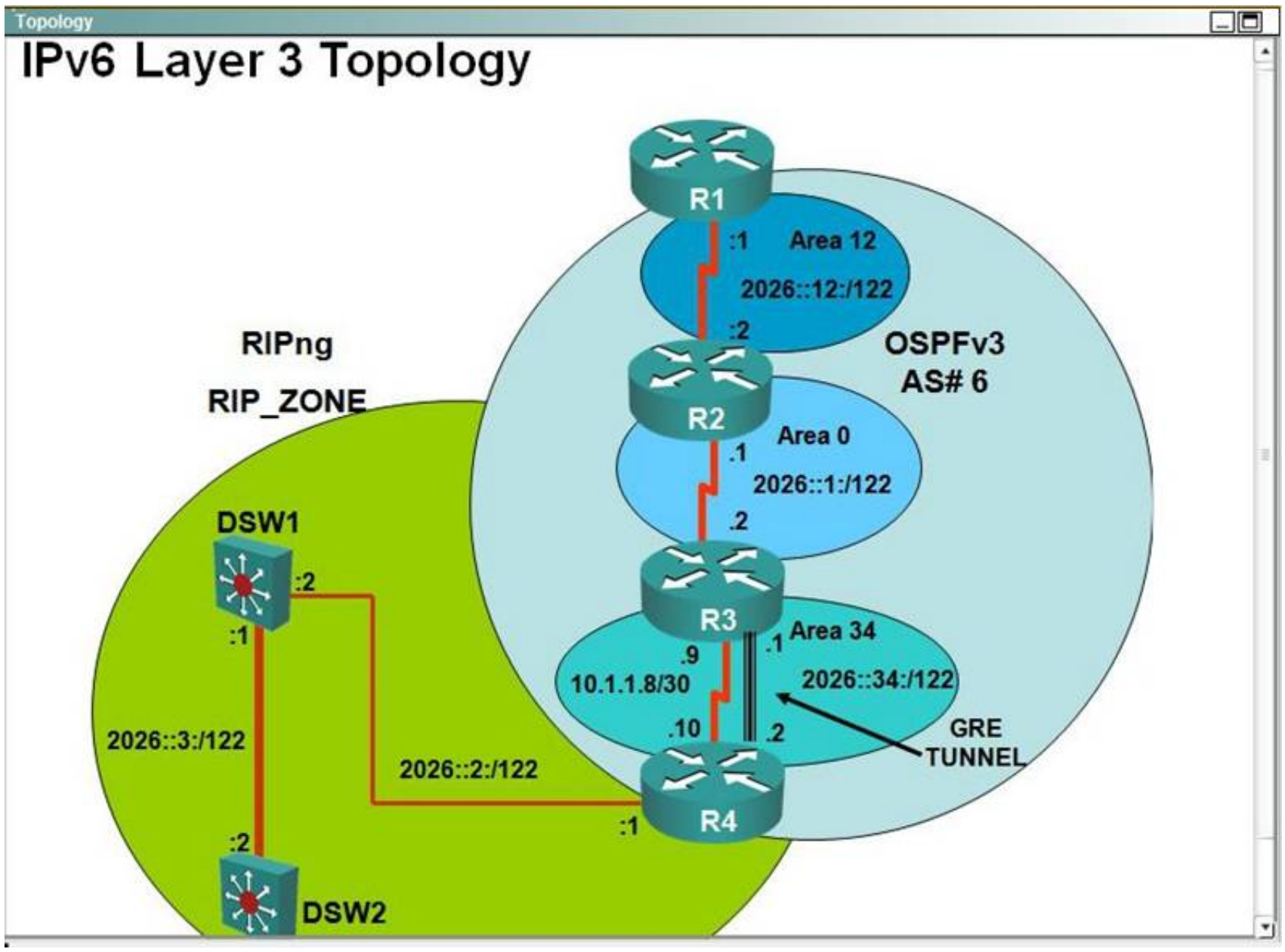
Explanation: As explained in question one of this ticket, we can then see that OSPFv3 has not been enabled on the interface to R3:
Screen Shot 2015-03-11 at 10

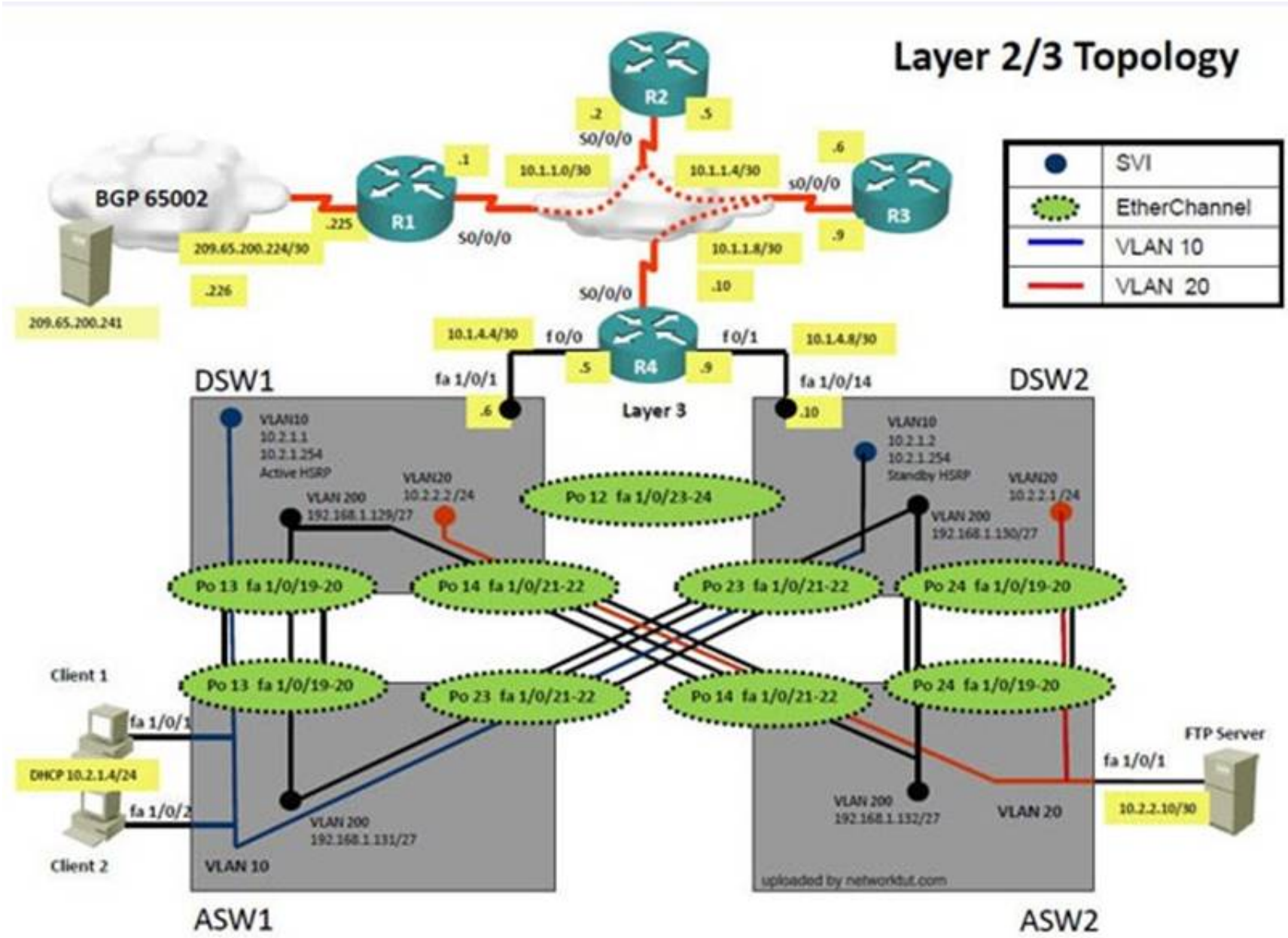
```
!
interface Serial0/0/0.12 point-to-point
 description Link to R1
 ip address 10.1.1.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 TSHOOT
 ipv6 address 2026::12:2/122
 ipv6 address FE80::2 link-local
 ipv6 ospf 6 area 12
 frame-relay interface-dlci 304
!
interface Serial0/0/0.23 point-to-point
 description Link to R3
 ip address 10.1.1.5 255.255.255.252
 ipv6 address 2026::1:1/123
 frame-relay interface-dlci 302
!
interface Serial0/0/1
```

So the problem is with R2, related to IPV6 Routing, and the fix is to enable the “ipv6 ospf 6 area 0”command under the serial 0/0/0.23 interface. We need to enable this interface for area 0 according to the topology diagram.

Topic 20, Ticket 15: IPv6 Routing Issue 2
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured on R1 with Webserver cloud AS 65002
HSRP is running between DSW1 & DSW2 Switches
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be
presented with a series of trouble tickets related to issues introduced during these configurations.
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same. Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========


IPv4 Layer 3 Topology
BGP 65001
NAT Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
DSW1
Client 1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.2
.13
.9
S0/0/0/0.34
10.1.1.8/30
Client 2
.10
10.2.4.12/30
10.1.4.4/30
fa0/0
R4
.5
Vlan 20
.2
.14
(DHCP Server)
fa0/1
.9
.10
10.1.4.8/30
.10
fa1/0/1
.1
10.2.2.0/24
FTP Server
DSW2
uploaded by networktut.com


Topology
IPv6 Layer 3 Topology
R1
:1
Area 12
2026::12:/122
:2
RIPng
RIP_ZONE
OSPFv3
AS# 6
R2
Area 0
.1
2026::1:/122
.2
DSW1
R3
:2
:1
.1
Area 34
.9
10.1.1.8/30
2026::34:/122
.10
.2
GRE
TUNNEL
2026::3:/122
2026::2:/122
R4
:1
:2
DSW2



Questions

The implementation group has been using the test bed to do an IPv6 'proof-of-concept'. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Using the supported commands to isolate the cause of this fault and answer the following questions.

NEW QUESTION 231
Drag each debug command on the left to the type of issue it can debug on the right.

Debug ip cef packet	802.1Q traffic issue
Debug ip mpacket	all ipv6 information
Debug ip packet	hsrp issues
Debug ipv6 packet	hardware routed packets
Debug standby errors	multicast packet
Debug vlan packets	all ipv4 information

Answer:

Explanation: Debug ip cef packet –>hardware routed packetsDebug ip mpacket–> multicast packetDebug ip packet –> all ipv4 informationDebug ipv6 packet –> all ipv6 informationDebug standby errors –> hsrp issuesDebug vlan packets –> 802.1Q traffic issue

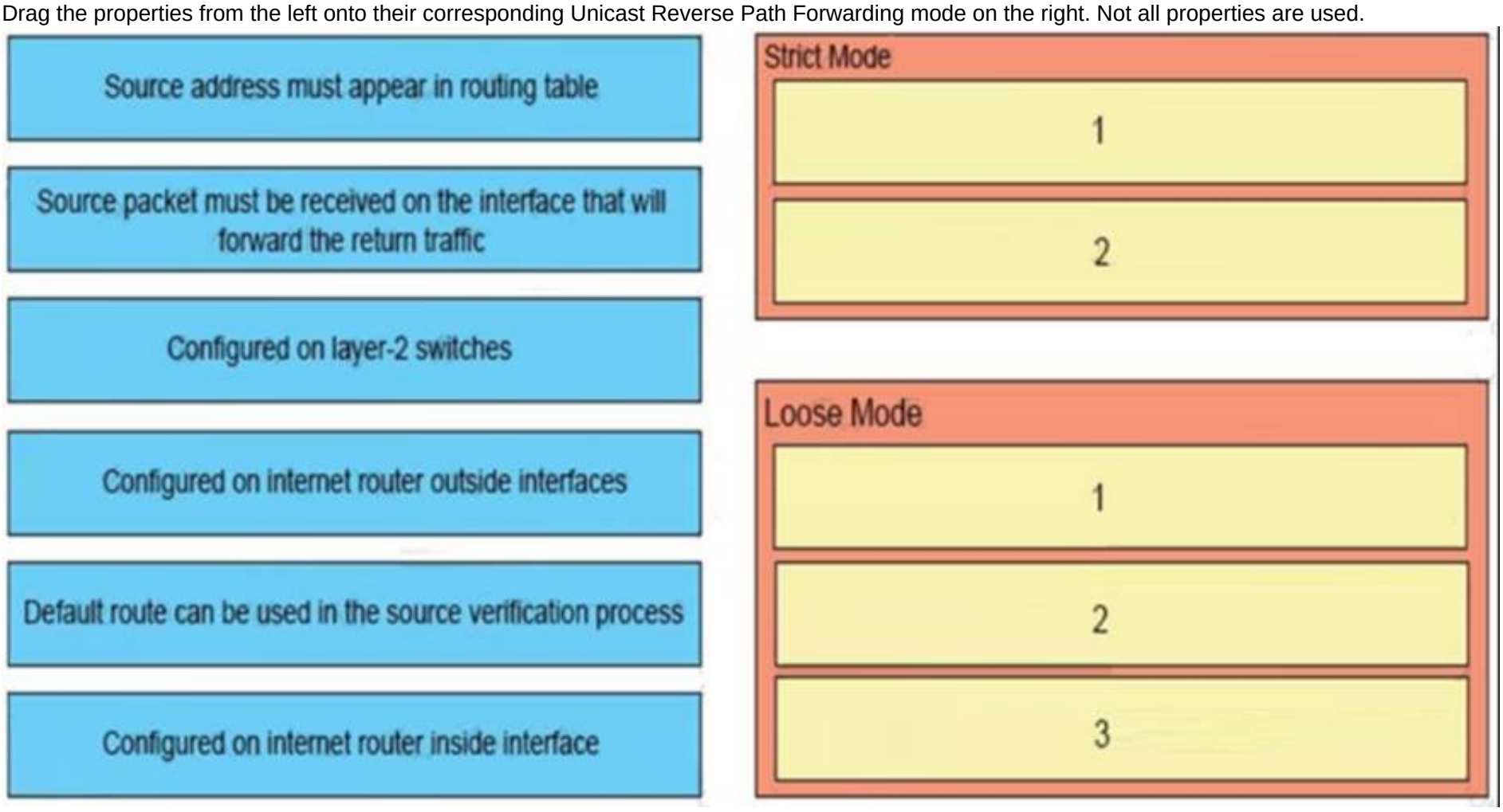
NEW QUESTION 234
Drag and drop the extended traceroute options from the left onto the troubleshooting they perform on the right.

max ttl	limits the number of hops a packet travels.
port number	limits the number of traceroute packets sent to a single destination.
probe count	troubleshoots connections geenrated from a specific interface.
source address	troubleshoots QoS issues
type of service	troubleshoots TCP and UDP port states

Answer:

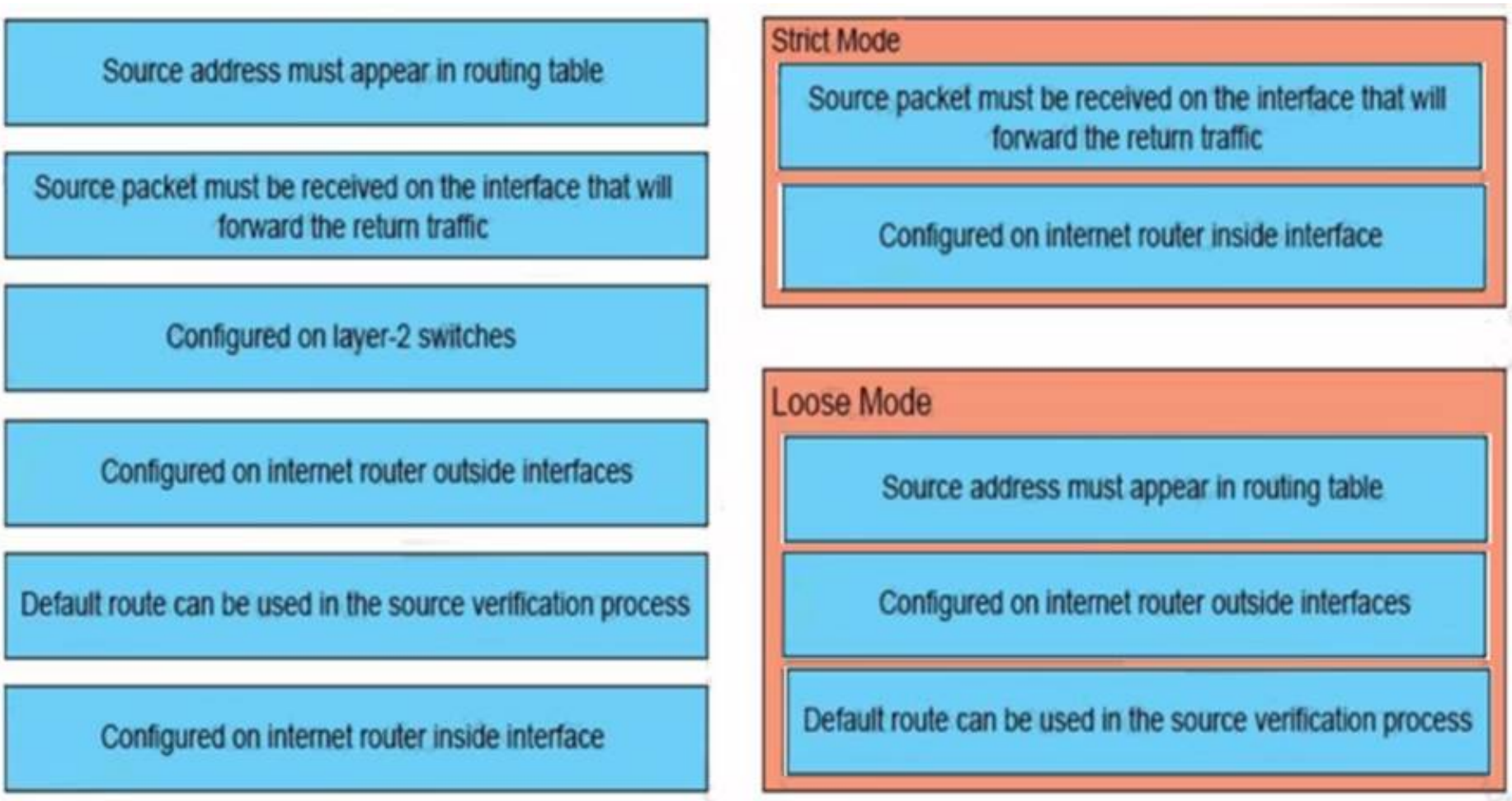
Explanation: Max TTL —> limits the number of hops a packet travel
Port number –> troubleshoot connections generated from specific interface Probe count –> limits the number of traceroute
Source address–> troubleshoot TCP and UDP port
Type of service –> troubleshoot QoS issues

NEW QUESTION 236
Drag the properties from the left onto their corresponding Unicast Reverse Path Forwarding mode on the right. Not all properties are used.

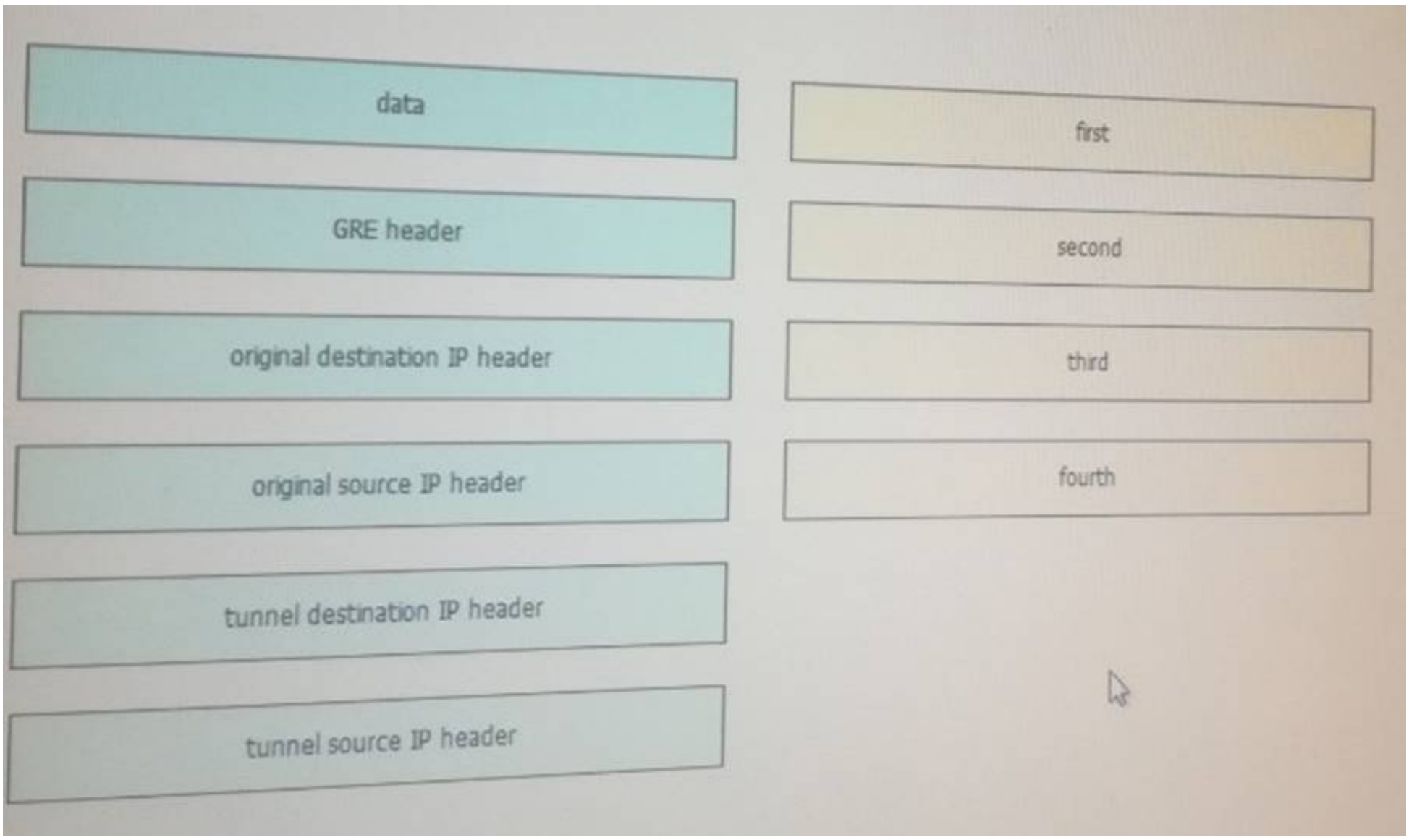


Answer:

Explanation:



NEW QUESTION 241
Drag and drop the components of a GRE tunnel from the left into the correct order on the right when monitoring a GRE encapsulated packet.



Answer:

Explanation: A. Source tunnel IP headerB. Destination tunnel IP headerC. GRE headerD. Original source IP header

NEW QUESTION 242
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).
The fault condition is related to which technology?

A. NTP
B. IP DHCP Server
C. IPv4 OSPF Routing
D. IPv4 EIGRP Routing
E. IPv4 Route Redistribution
F. IPv6 RIP Routing
G. IPv6 OSPF Routing
H. IPV4 and IPV6 Interoperability
I. IPv4 layer 3 security

Answer: G

Explanation: As explained earlier, the problem is with route redistribution on R4 of not redistributing RIP routes into OSPF for IPV6.

NEW QUESTION 244
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).
Use the supported commands to isolate the cause of this fault and answer the following question. On which device is the fault condition located?

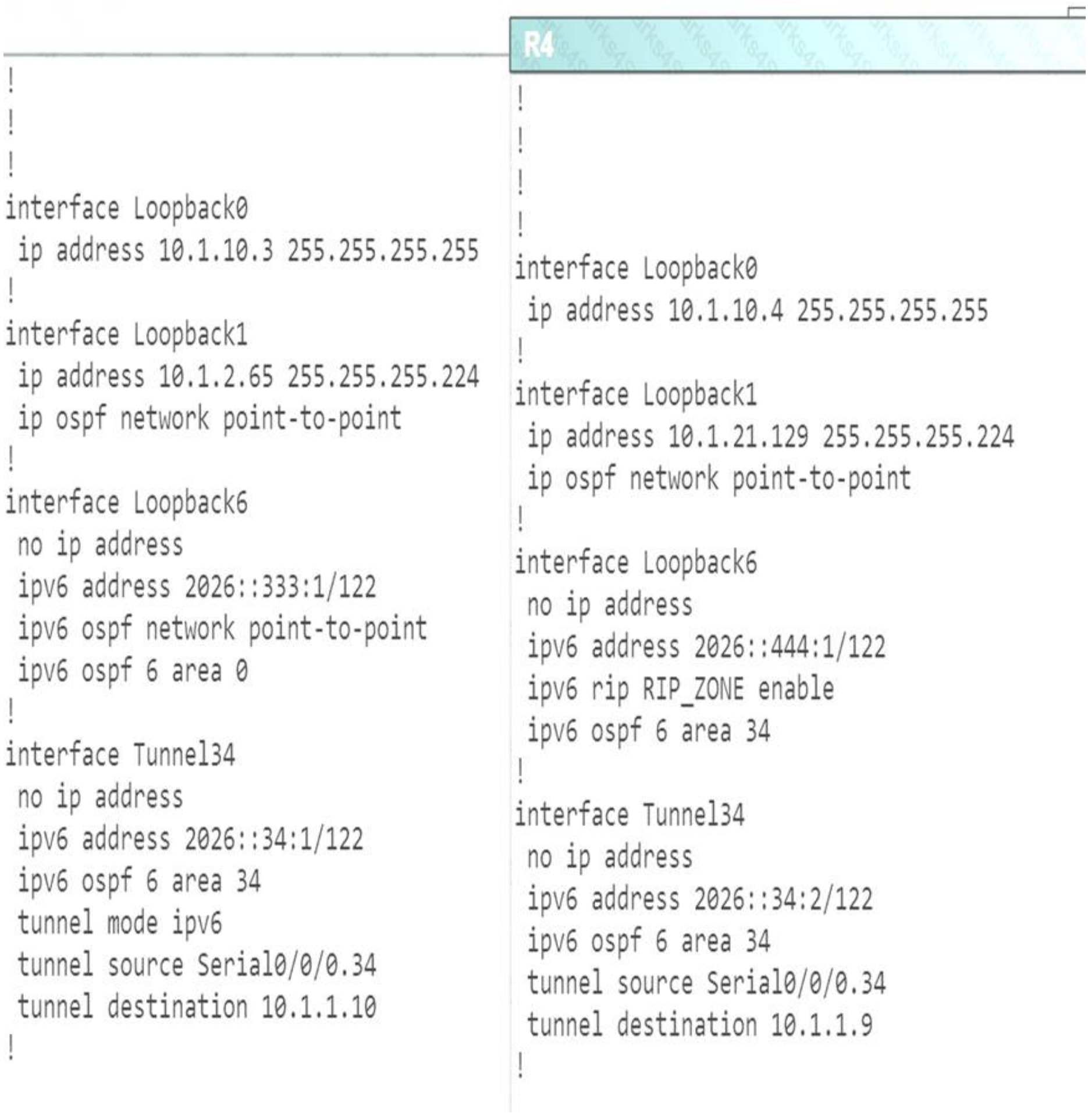
A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Answer: C

Explanation: Start to troubleshoot this by pinging the loopback IPv6 address of DSW2 (2026::102:1). This can be pinged from DSW1, and R4, but not R3 or any other devices past that point. If we look at the routing table of R3, we see that there is no OSPF neighbor to R4:
Screen Shot 2015-03-11 at 4

```
R3>ping 2026::102:1

Translating "2026::102:1"

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2026::102:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R3>show ipv6 ospf ne
R3>show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.1.10.2         1   FULL/  -        00:00:30    16              Serial0/0/0.23

R3>
```

This is due to mismatched tunnel modes between R3 and R4: Screen Shot 2015-03-11 at 4



Problem is with R3, and to resolve the issue we should delete the “tunnel mode ipv6” under interface Tunnel 34.

NEW QUESTION 246
Which of the following commands will display a router's crypto map IPsec security association settings?

A. show crypto map ipsec sa
B. show crypto map
C. show crypto engine connections active
D. show ipsec crypto map
E. show crypto map sa
F. show ipsec crypto map sa

Answer: A

NEW QUESTION 251
Which of the following management types can be used to deploy appropriate quality-of-service solutions to make the most efficient use of bandwidth?

A. Fault management
B. Accounting management
C. Operations management
D. Performance management
E. Security management
F. Configuration management

Answer: D

NEW QUESTION 255
Which of the following statements concerning IGMP are correct? (Choose all that apply.)

A. With IGMPvl, queries are sent to a specific group.
B. Hosts issuing IGMPvl requests will be correctly interpreted by IGMPv2 hosts due to backward compatibility.
C. An IGMPv2 router will ignore IGMPv2 leave messages when IGMFVl hosts are present.
D. With IGMFV2, a leave message is supported.
E. An IGMPv2 host will send an IGMFVl report on an IGMFVl router.
F. An IGMPv2 router can only allow IGMPv2 hosts to execute a join request.

Answer: CDE

NEW QUESTION 259
Which of the following characteristics describe the BPDU Guard feature? (Choose all that apply.)

A. ABPDU Guard port should only be configured on ports with PortFast enabled.
B. BPDU Guard and PortFast should not be enabled on the same port.
C. BPDU Guard is used to ensure that superior BPDUs are not received on a switch port.
D. ABPDU Guard port receiving a BPDU will go into err-disable state.
E. ABPDU Guard port receiving a BPDU will be disabled.
F. BPDU Guard can be enabled on any switch port.

Answer: ADE

Explanation: Option A is, obviously, valid, since BPDUGuard is a enhancement of thePortFast feature. Reference: Spanning Tree PortFast BPDU Guard Enhancement
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a008009482f.shtml

NEW QUESTION 261
Which of the following is an unlikely reason for the ARP process to fail?

A. CEF switching is disabled on the switch
B. The source device and destination device are in different VLANs
C. The VLAN is excluded from the trunk
D. The host is connected to the switch through an IP phone
E. A faulty cable from host to switch or between switches
F. The trunking encapsulation type is inconsistent on the two ends of the link

Answer: AD

NEW QUESTION 266
Which of the following are byproducts of a structured maintenance plan? (Choose all that apply.)

A. Predictable security vulnerabilities
B. Economies of scale
C. Improved expenditure forecasts
D. Increased downtime
E. Predictable equipment obsolescence
F. Consumption of fewer resources

Answer: ABCEF

NEW QUESTION 269
Which of the following are shared distribution tree characteristics? (Choose all that apply.)

A. Memory requirements are higher for shared distribution tree than for source distribution tree.
B. Creates a tree from a central RP to all last-hop routers.
C. Uses a rendezvous point.
D. An optimal path is created between each source router and each last-hop router.
E. Place (S,G) entry in each router's multicast routing table.
F. Place (*,G) entry in a router's multicast routing to table.

Answer: CF

NEW QUESTION 273
Given the multicast IP address of 224.193.5.10, what would the corresponding multicast MAC address be?

A. 00-00-0c-c0-05-0a
B. 00-00-0c-cl-05-0a
C. 01-00-5e-00-00-0c
D. 01-00-5e-41-05-0a
E. 00-00-0c-01-00-5e
F. 01-00-5e-cl-05-0a

Answer: F

Explanation: First three octets are 01-00-05e for every single multicast address.Las three octets are the hexadecimal version of the las three octets of the IP address, in this case 193.5.10 is translated to c1-05-0a.
Reference:

NEW QUESTION 278
Which of the following statements regarding documentation would not be considered a helpful step in the troubleshooting process?

A. Use the Cisco Auto Configuration tool.
B. Use the Cisco Rollback feature.
C. Automate documentation.
D. Schedule documentation checks.
E. Use the Cisco Configuration Archive tool.
F. Require documentation prior to a ticket being closed out.

Answer: A

NEW QUESTION 280
Which of the following topology situations would be a qood candidate for configuring DMVPN?

A. Extranet VPN
B. Managed overlay VPN topology
C. Hub-and-spoke VPN topology
D. Central-site VPN topology
E. Full mesh VPN topology
F. Remote-access VPN topology

Answer: E

NEW QUESTION 285
You enabled CDP on two Cisco Routers which are connected to each other. The Line and Protocol status for the interfaces on both routers show as UP but the routers do not see each other a CDP neighbors. Which layer of the OSI model does the problem most likely exist?

A. Physical
B. Session
C. Application
D. Data-Link
E. Network

Answer: D

Explanation: CDP is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices. In this case, the line protocol is up which means that the physical layer is operational (layer 1) but the data link layer is not.
Reference: “Configuring CDP”
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/cdp.html

NEW QUESTION 290
You have the followings commands on your Cisco Router: ip ftp username admin
ip ftp password backup
You have been asked to switch from FTP to HTTP. Which two commands will you use to replace the existing commands?

A. ip http username admin
B. ip http client username admin
C. ip http password backup
D. ip http client password backup
E. ip http server username admin
F. ip http server password backup

Answer: BD

Explanation: Configuring the HTTP Client
Perform this task to enable the HTTP client and configure optional client characteristics.
The standard HTTP 1.1 client and the secure HTTP client are always enabled. No commands exist to disable the HTTP client. For information about configuring optional characteristics for the HTTPS client, see the HTTPS-HTTP Server and Client with SSL 3.0, Release 12.2(15)T, feature module.
SUMMARY STEPS
1. http://www.cisco.com/en/US/i/templates/blank.gifenable
2. http://www.cisco.com/en/US/i/templates/blank.gifconfigure terminal
3. http://www.cisco.com/en/US/i/templates/blank.gifip http client cache {ager interval minutes | memory {file file-size-limit | pool pool-size-limit}
4. http://www.cisco.com/en/US/i/templates/blank.gifip http client connection {forceclose | idle timeout seconds | retry count | timeout seconds}
5. http://www.cisco.com/en/US/i/templates/blank.gifip http client password password
6. http://www.cisco.com/en/US/i/templates/blank.gifip http client proxy-server proxy-name proxy-port port-number
7. http://www.cisco.com/en/US/i/templates/blank.gifip http client response timeout seconds

8. http://www.cisco.com/en/US/i/templates/blank.gifip http client source-interface type number
9. http://www.cisco.com/en/US/i/templates/blank.gifip http client username username

Reference: HTTP 1.1 Web Server and Client.
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_web.html

NEW QUESTION 291
You examine the port statistics on a Cisco Catalyst switch and notice an excessive number of frames are being dropped. Which of the following are possible reasons for the drops?

A. Unknown destination MAC address
B. Bad cabling
C. MAC forwarding table is full
D. Port configured for half duplex
E. Port configured for full duplex
F. Network congestion

Answer: BF

NEW QUESTION 293
Which of the following are valid modes of accessing the management plane? (Choose all that apply.)

A. Serial connection
B. Secure Shell
C. RADIUS
D. Simple Network Management Protocol
E. HTTP
F. Telnet

Answer: ABDEF

NEW QUESTION 298
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-135 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-135 Product From:

https://www.2passeasy.com/dumps/300-135/

Money Back Guarantee

300-135 Practice Exam Features:

* 300-135 Questions and Answers Updated Frequently

* 300-135 Practice Questions Verified by Expert Senior Certified Staff

* 300-135 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-135 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year