Exam Questions 300-135

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

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

NEW QUESTION 1
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 2
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 3
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 4
Refer to the exhibit.

```
%TUN-5-RECURDOWN: Tunnel0 temporarily disabled... (output omitted)
```

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 5
Which two statements about GRE tunnels are true? (Choose two)

A. GRE encapsulates the original packet
B. GRE tunnels operate in GRE/IP mode by default
C. The IP header encapsulates the GRE header
D. The carrier protocol adds the delivery header
E. GRE tunnels operate in GRE/IPsec mode by default

Answer: AE

NEW QUESTION 6
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 7

```
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 8
Which three protocols or protocol combinations does Management Plane Protection (MPP) support? (Choose three.)

A. SFTP
B. SSH
C. Both HTTP and HTTPS
D. FTP
E. Only HTTP
F. OSPF

Answer: BCD

NEW QUESTION 9
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 10
On which plane of operation can you access and configure a router or switch?

A. forwarding
B. management
C. control
D. data

Answer: B

NEW QUESTION 10
What is the ping response to a transmitted echo that needed to be fragmented and fragmentation was not allowed?

A. U
B. M
C. ....
D. D

Answer: D

NEW QUESTION 13
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 16
Which protocol is used by traceroute and ping operations?

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

Answer: D

NEW QUESTION 19
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 23
On which two topologies can you deploy a point-to-point GRE over IPsec design? (Choose two.)

A. bus
B. partial-mesh
C. hub-and-spoke
D. ring
E. tree

Answer: BC

NEW QUESTION 24
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 25
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 28
Which three keywords are supported in the ip header option?

A. Timeout
B. Type of service
C. Validate
D. Timestamp
E. Record
F. Strict

Answer: DEF

NEW QUESTION 32
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 37
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.

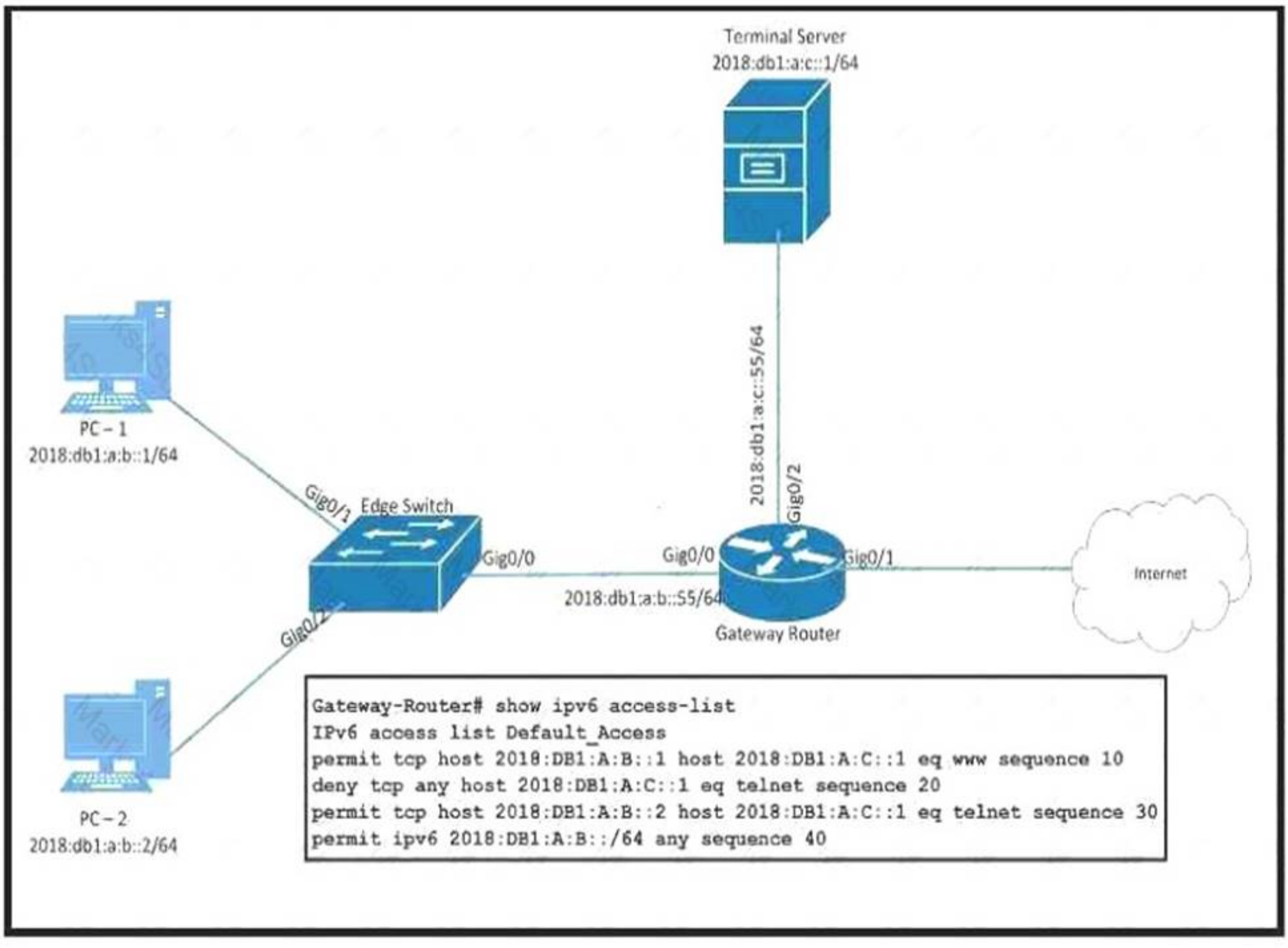
Answer: D

NEW QUESTION 39
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 40
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 42
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 44
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 49
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 54
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 57
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.

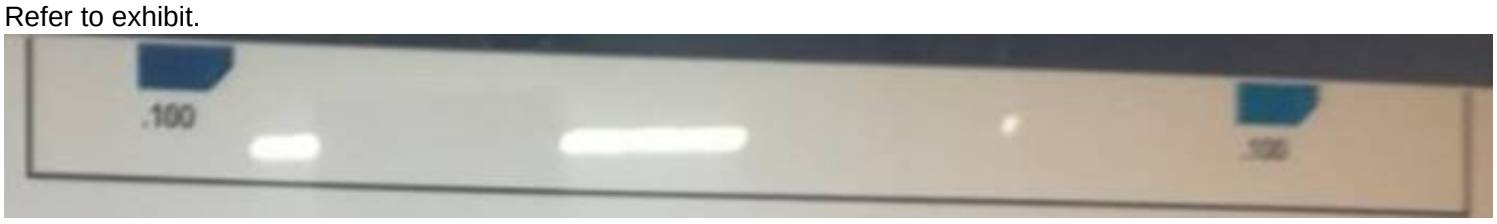
Answer: C

NEW QUESTION 58
If you are troubleshooting a spann.ng-tree loop on a VLAN, which standard troubleshooting approach is most appropriate for identifying the cause of the loop?

A. divide and conquer
B. top-down
C. bottom-up
D. follow-the-path

Answer: D

NEW QUESTION 59
Refer to exhibit.

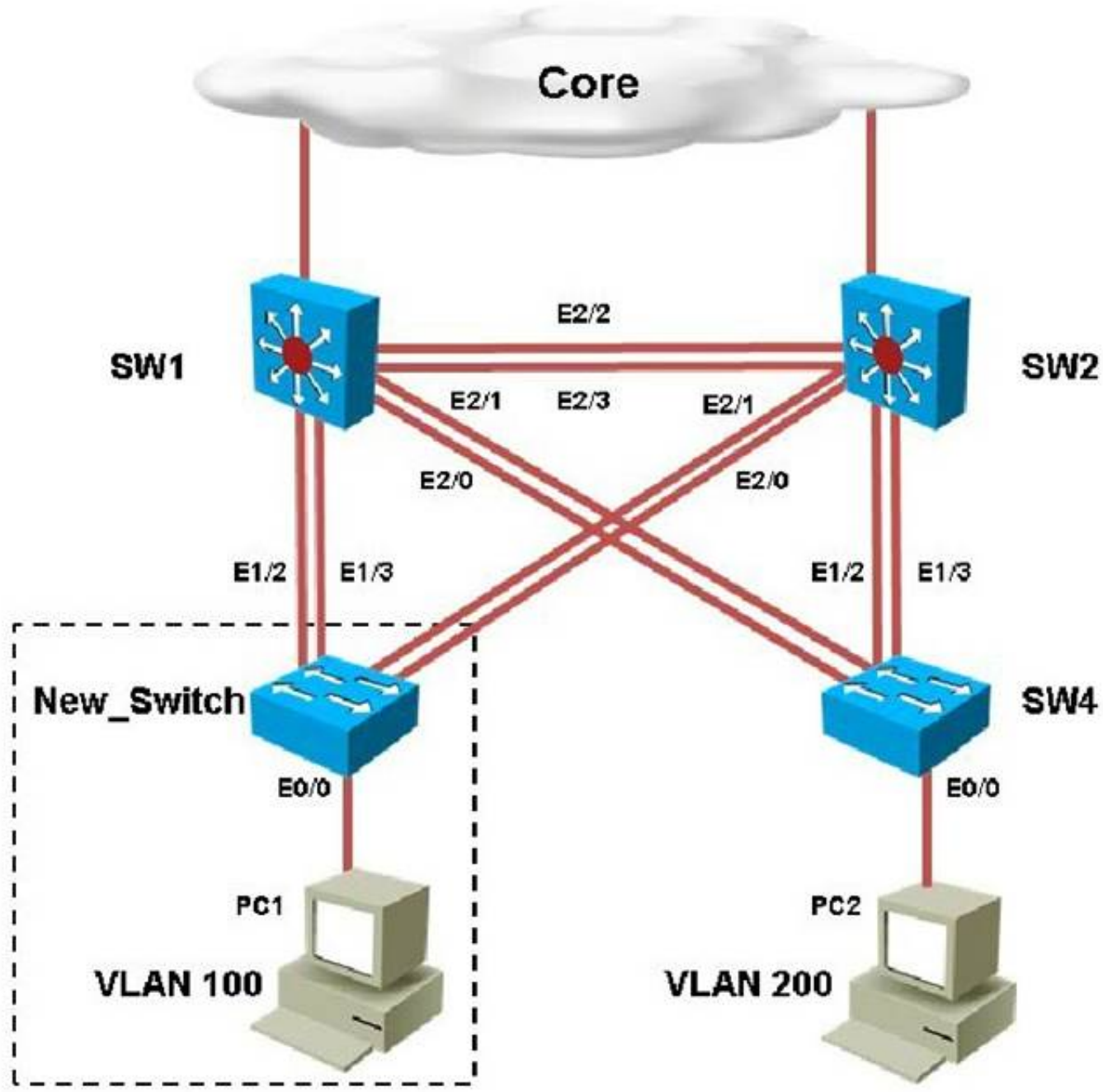


If all routers are sharing routes via OSPF area 0, which two configuration can you apply to R2 and R3 so that they can enable a GRE tunnel between them? (Choose two)

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

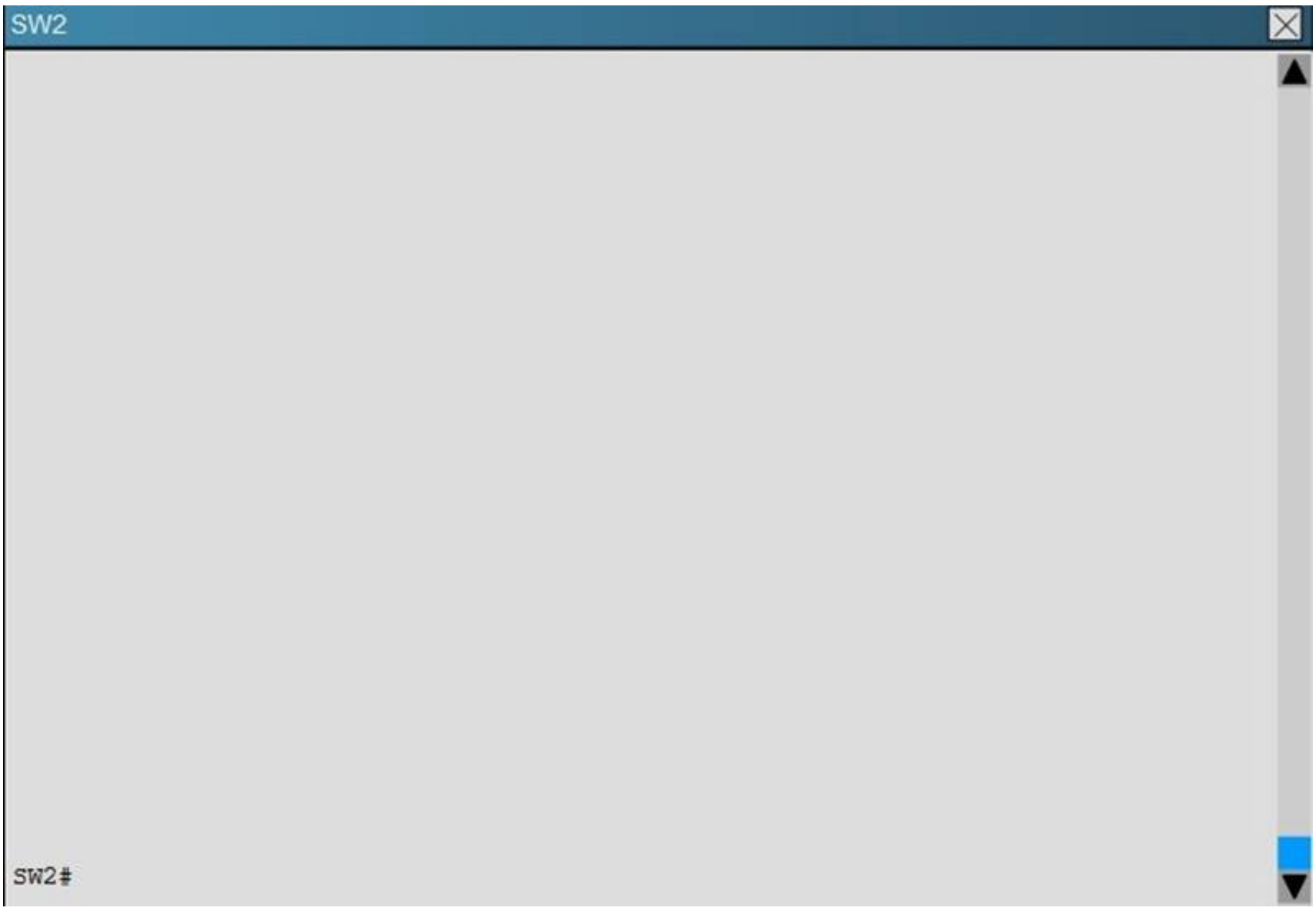
Answer: BD

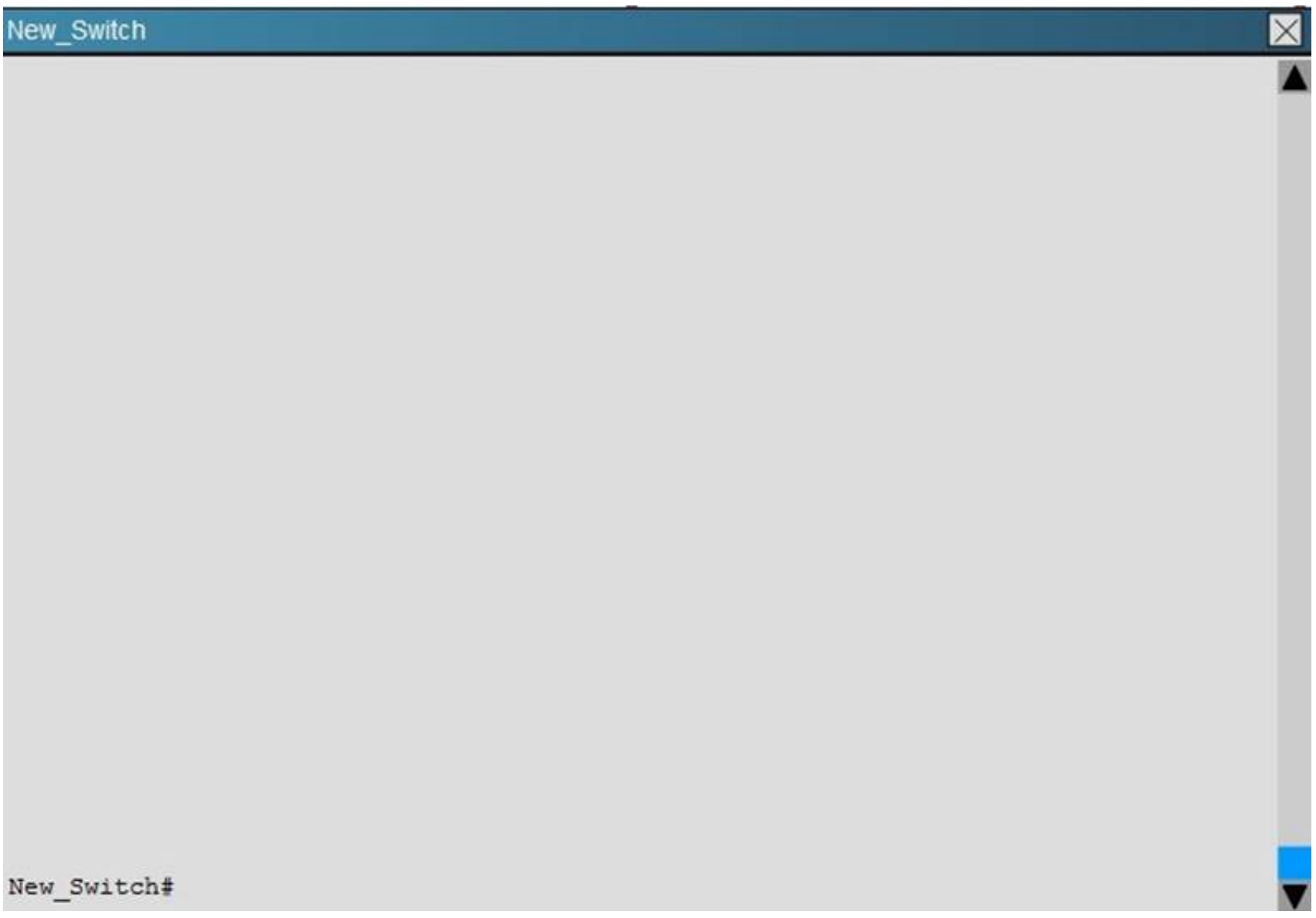
NEW QUESTION 62
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.

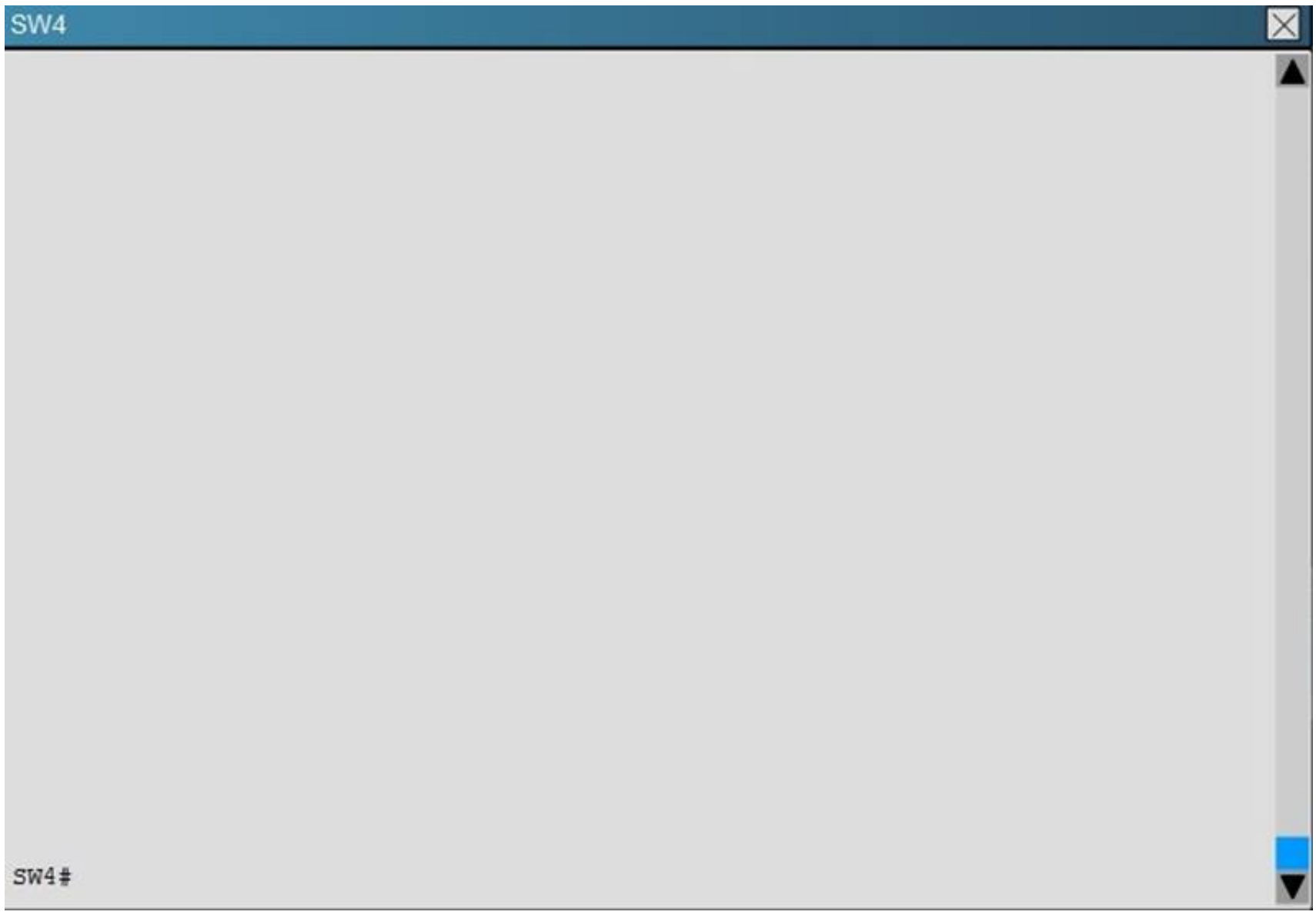

Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

SW1

```
SW1#
```


SW2
SW2#


New_Switch
New_Switch#



PC2 in VLAN 200 is unable to ping the gateway address 172.16.200.1; identify the issue.

A. VTP domain name mismatch on SW4
B. VLAN 200 not configured on SW1
C. VLAN 200 not configured on SW2
D. VLAN 200 not configured on SW4

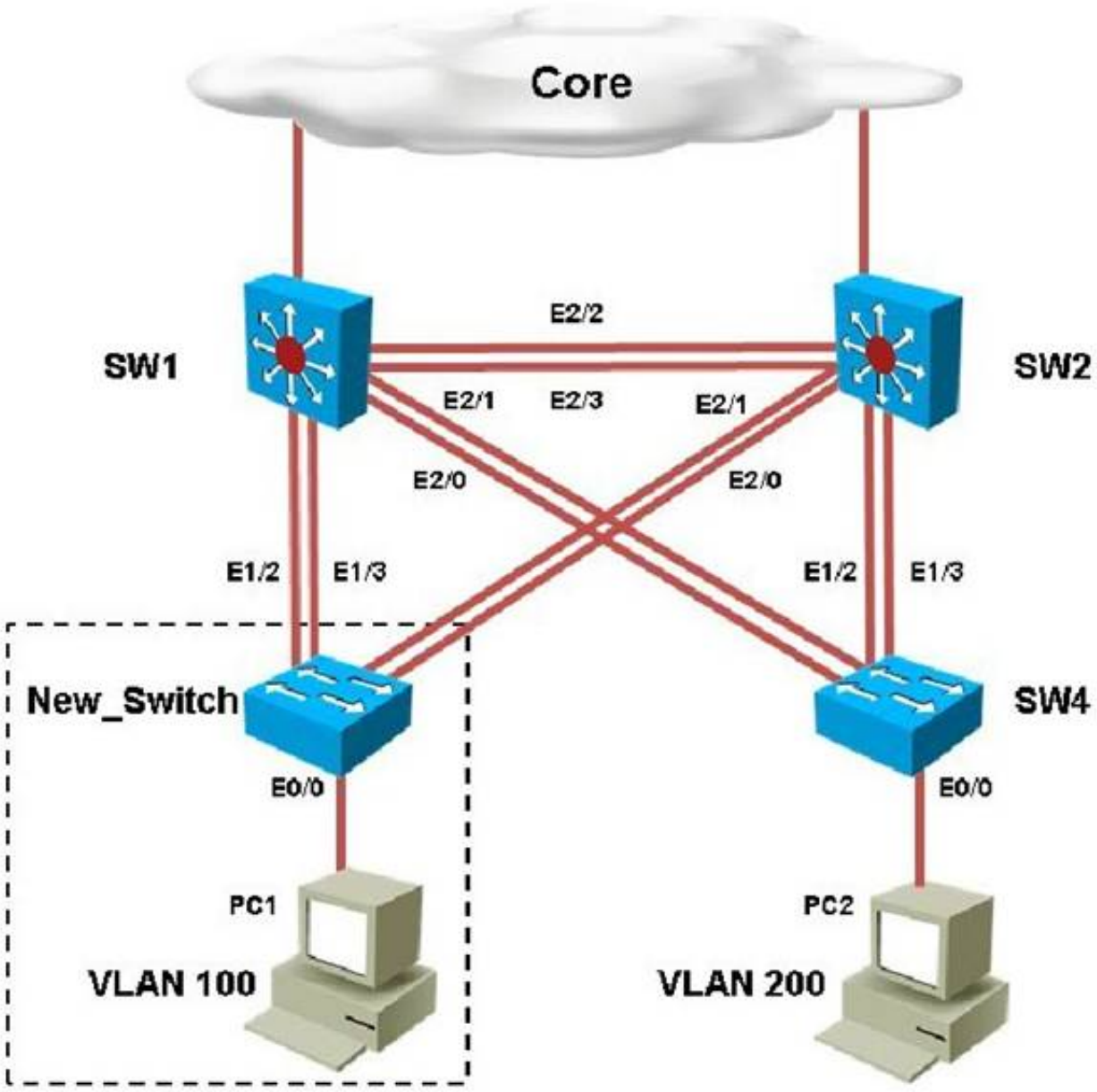
Answer: D

Explanation: By looking at the configuration for SW2, we see that it is missing VLAN 200, and the “switchport access vlan 200” command is missing under interface eth 0/0:

SW4

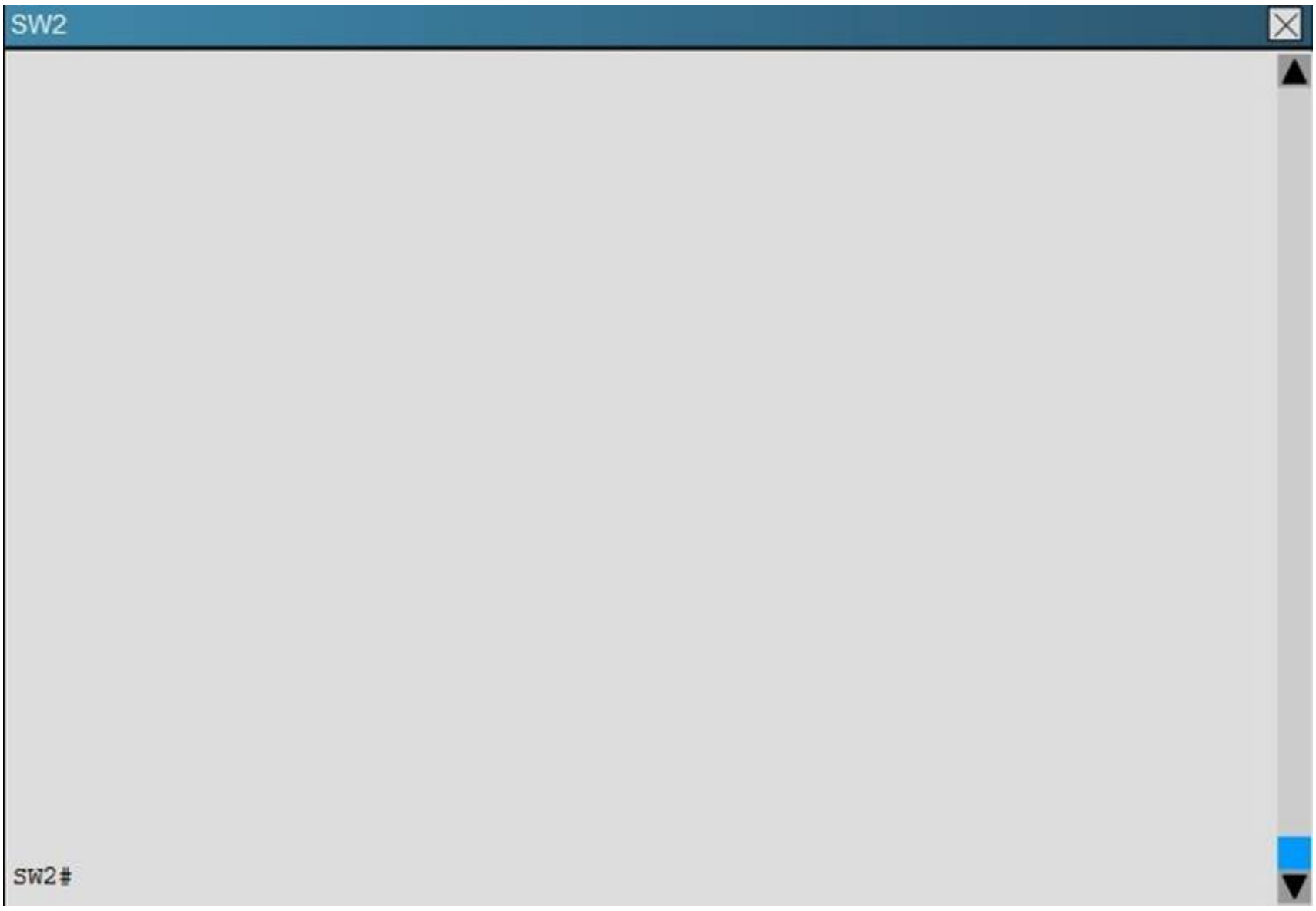
```
vlan internal allocation policy ascending
!
vlan 100
!
vlan 300
 name Management_VLAN
!
vlan 400
 name VLAN400
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 description Connected to PC2
 switchport mode access
 duplex auto
!
```

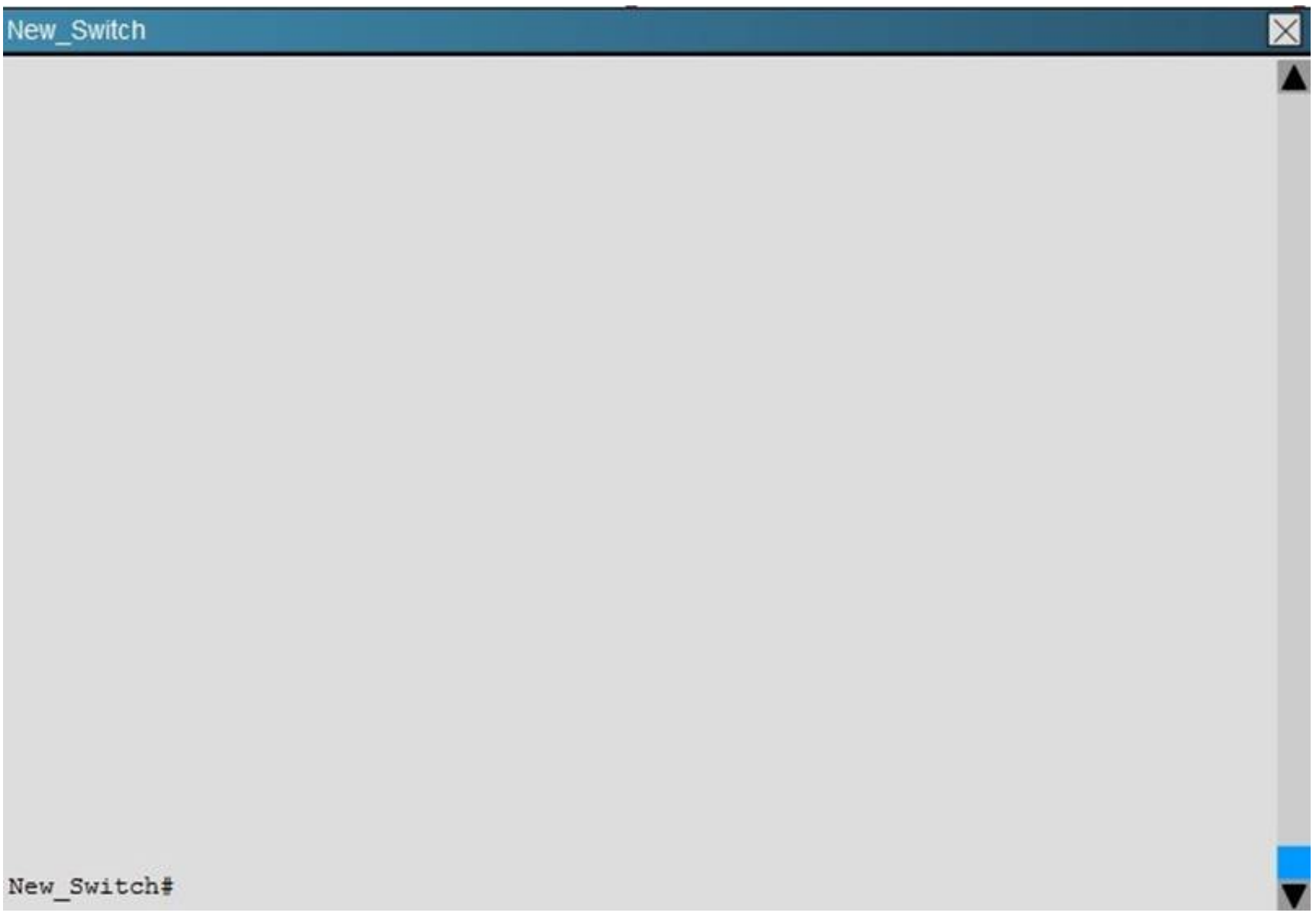
NEW QUESTION 66
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.

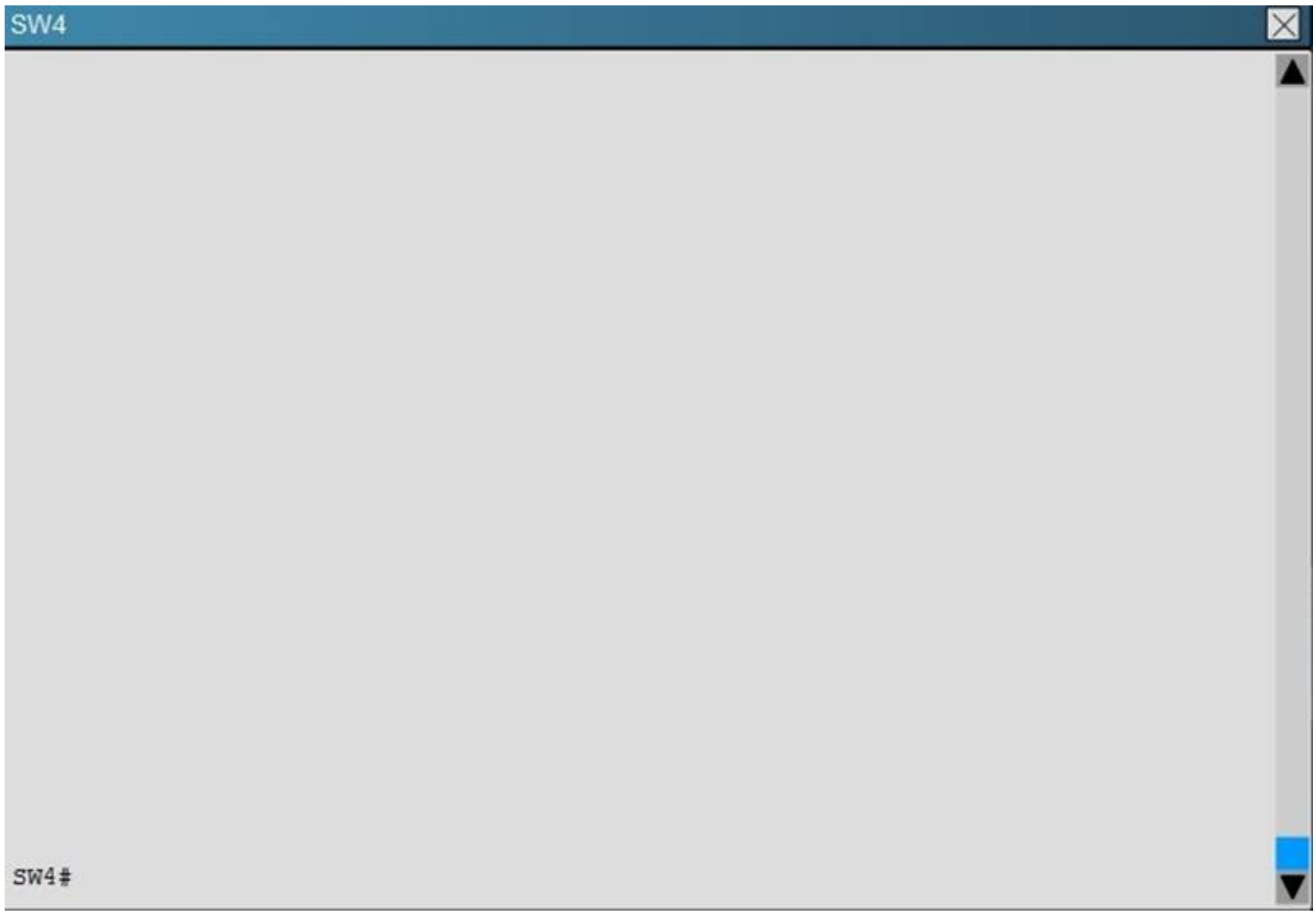


SW1

```
SW1#
```


SW2
SW2#


New_Switch
New_Switch#

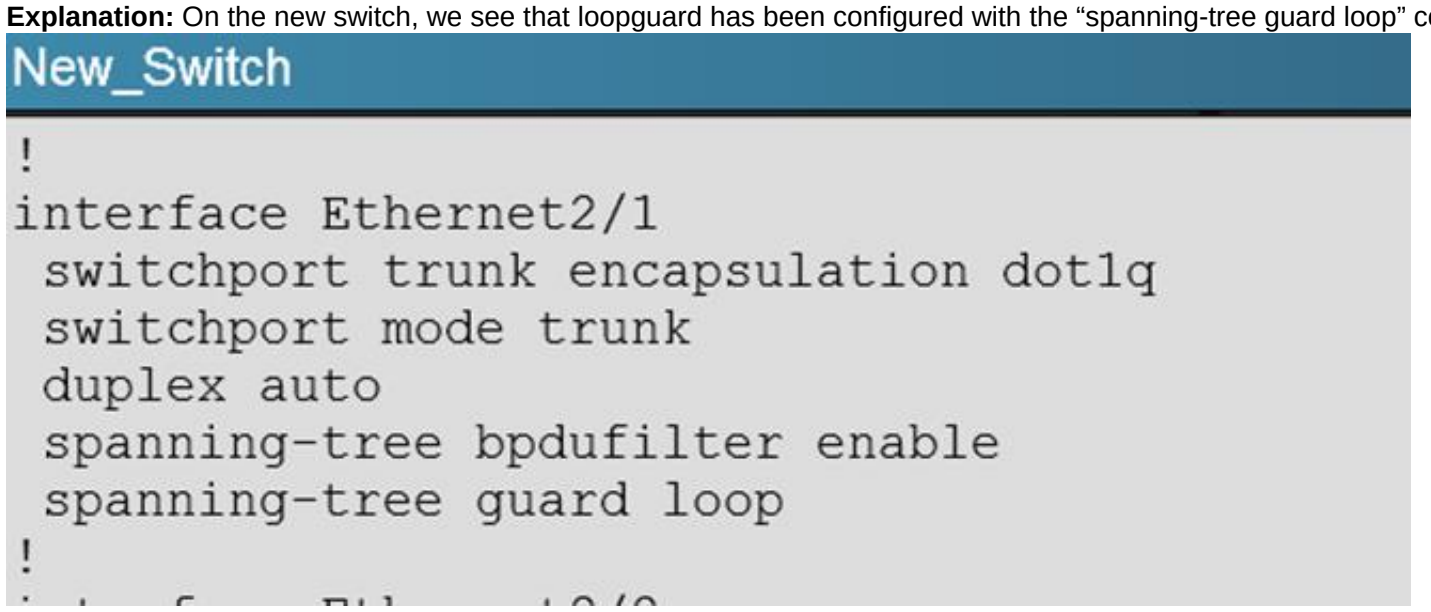


Which of statement is true regarding STP issue identified with switches in the given topology?

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

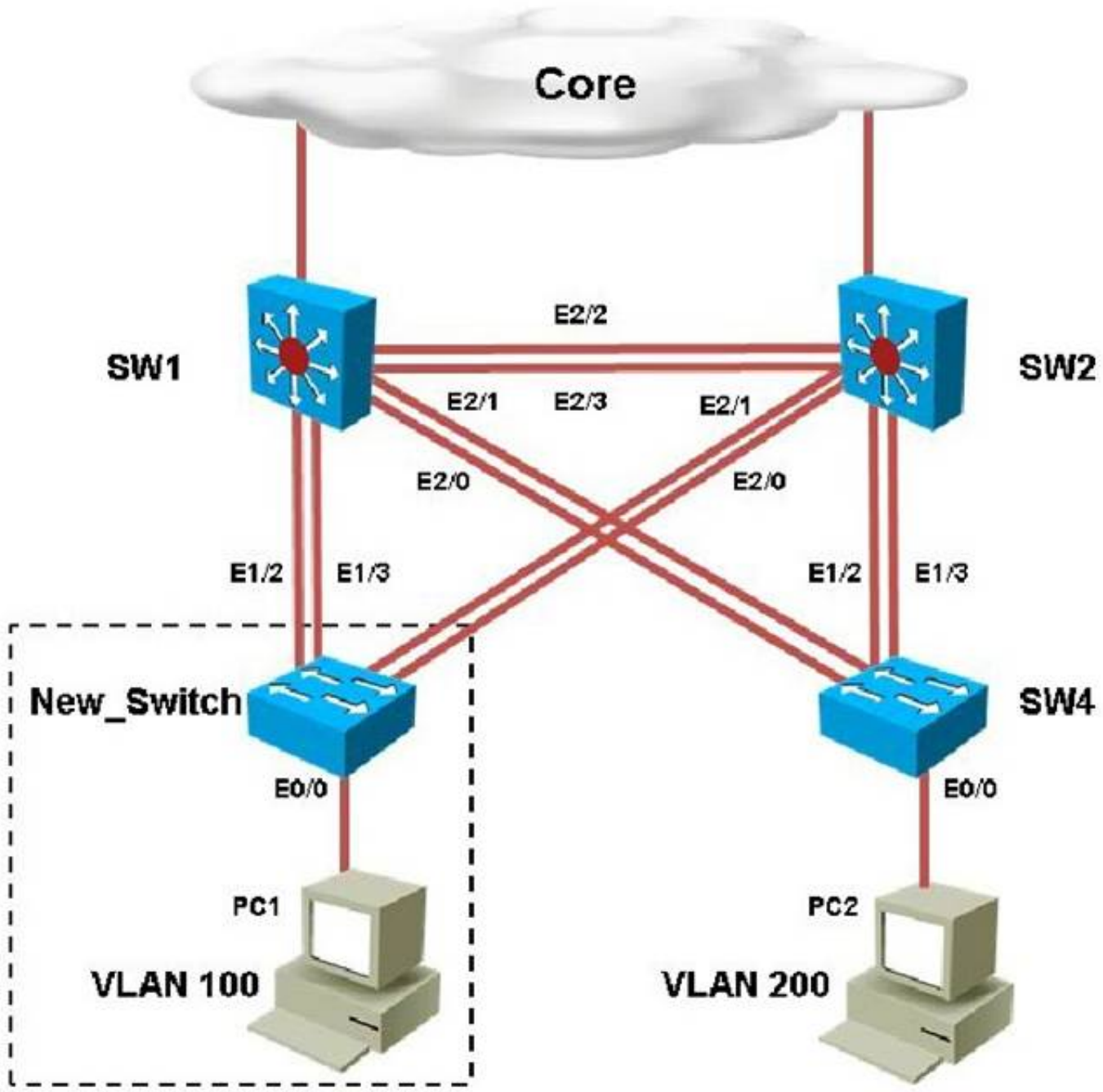
Answer: A

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

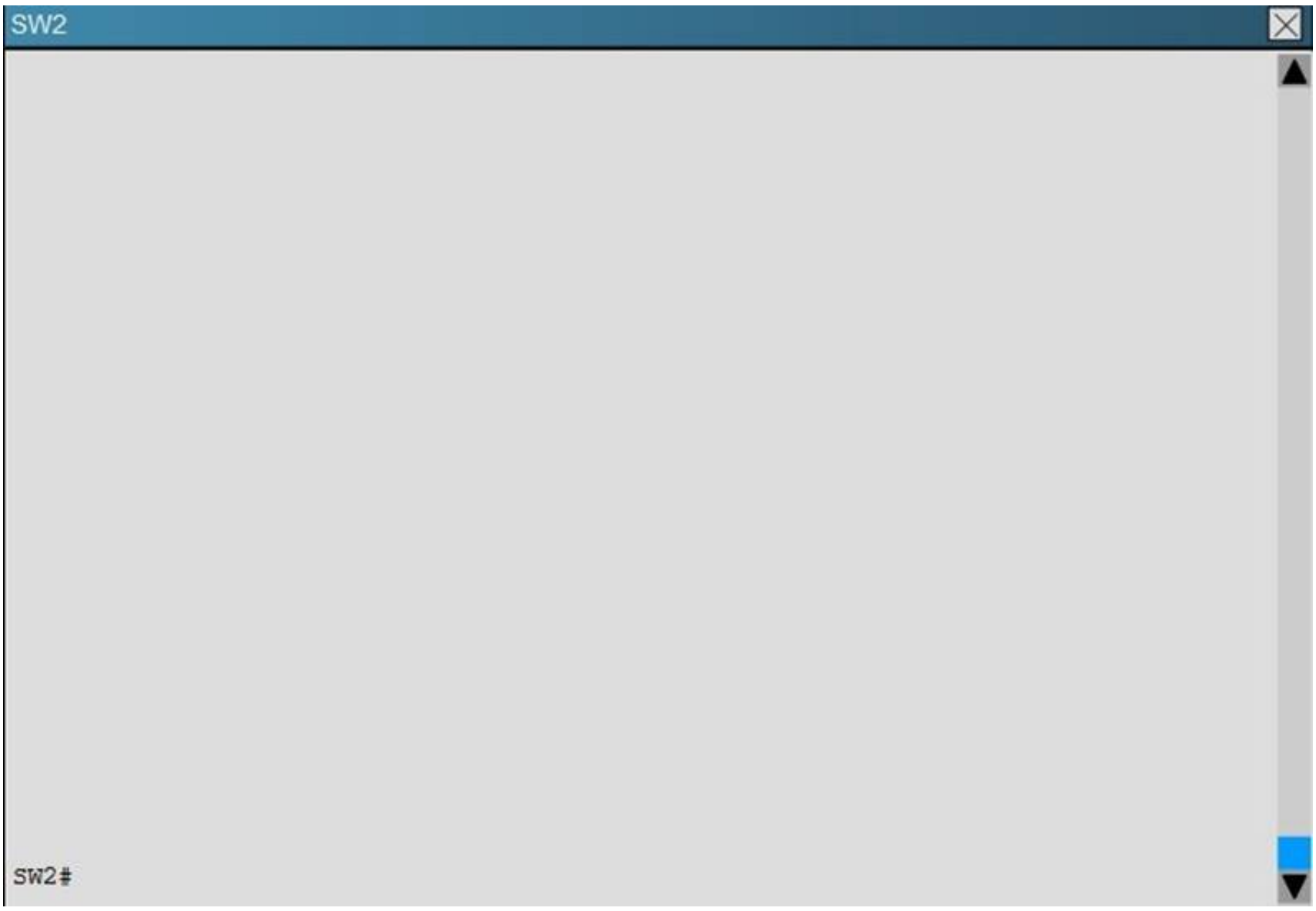


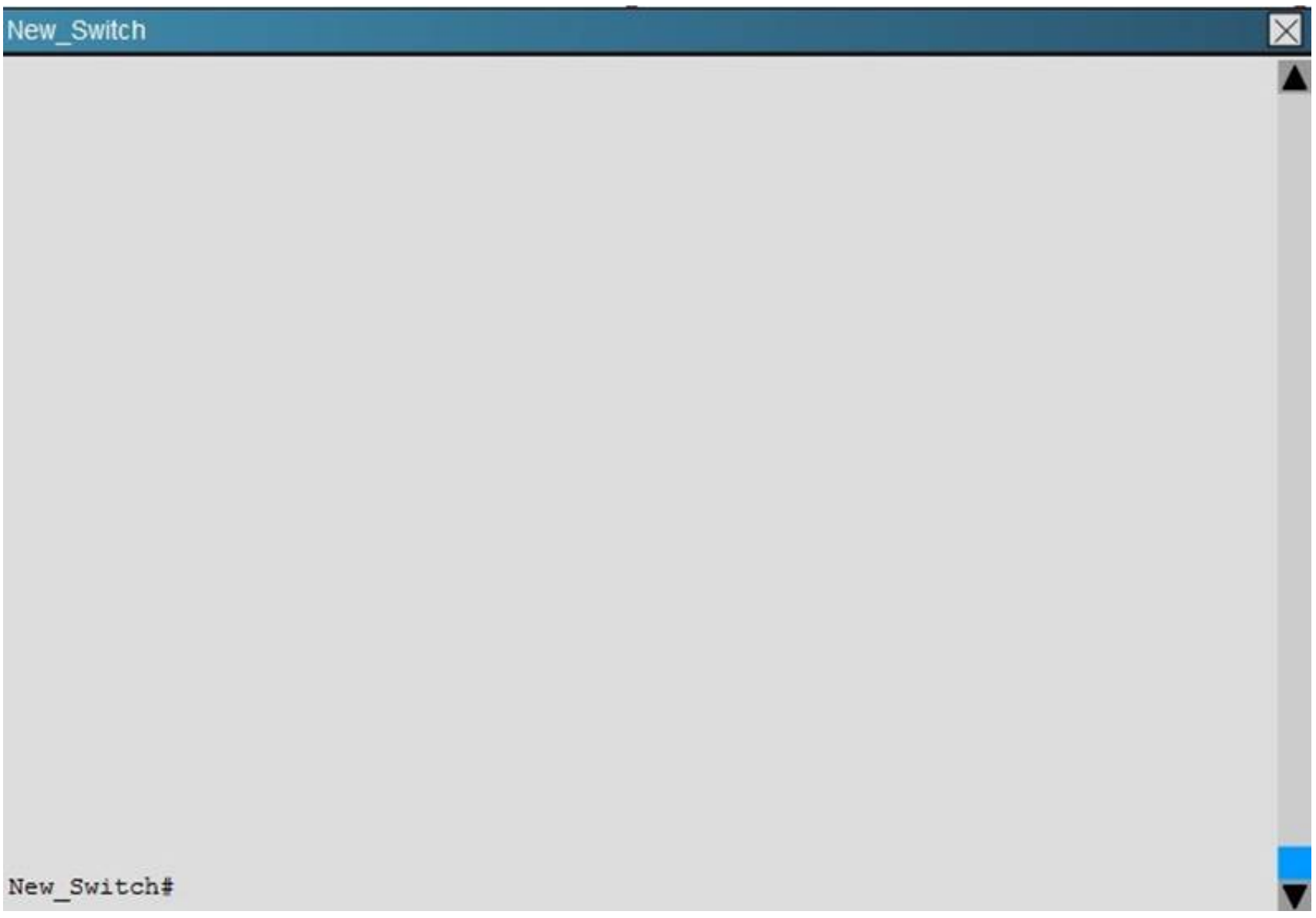
The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the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

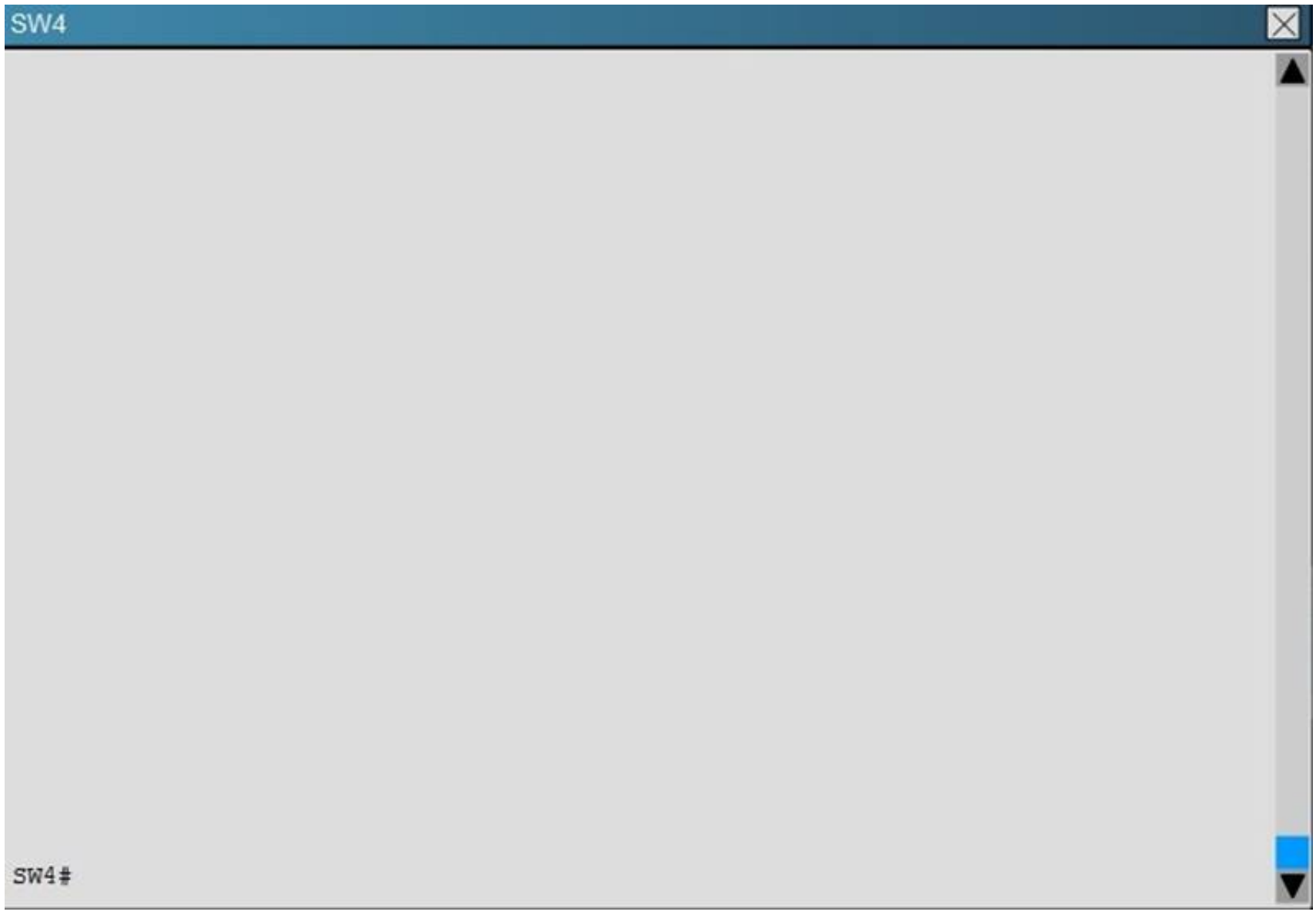
NEW QUESTION 68
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.


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

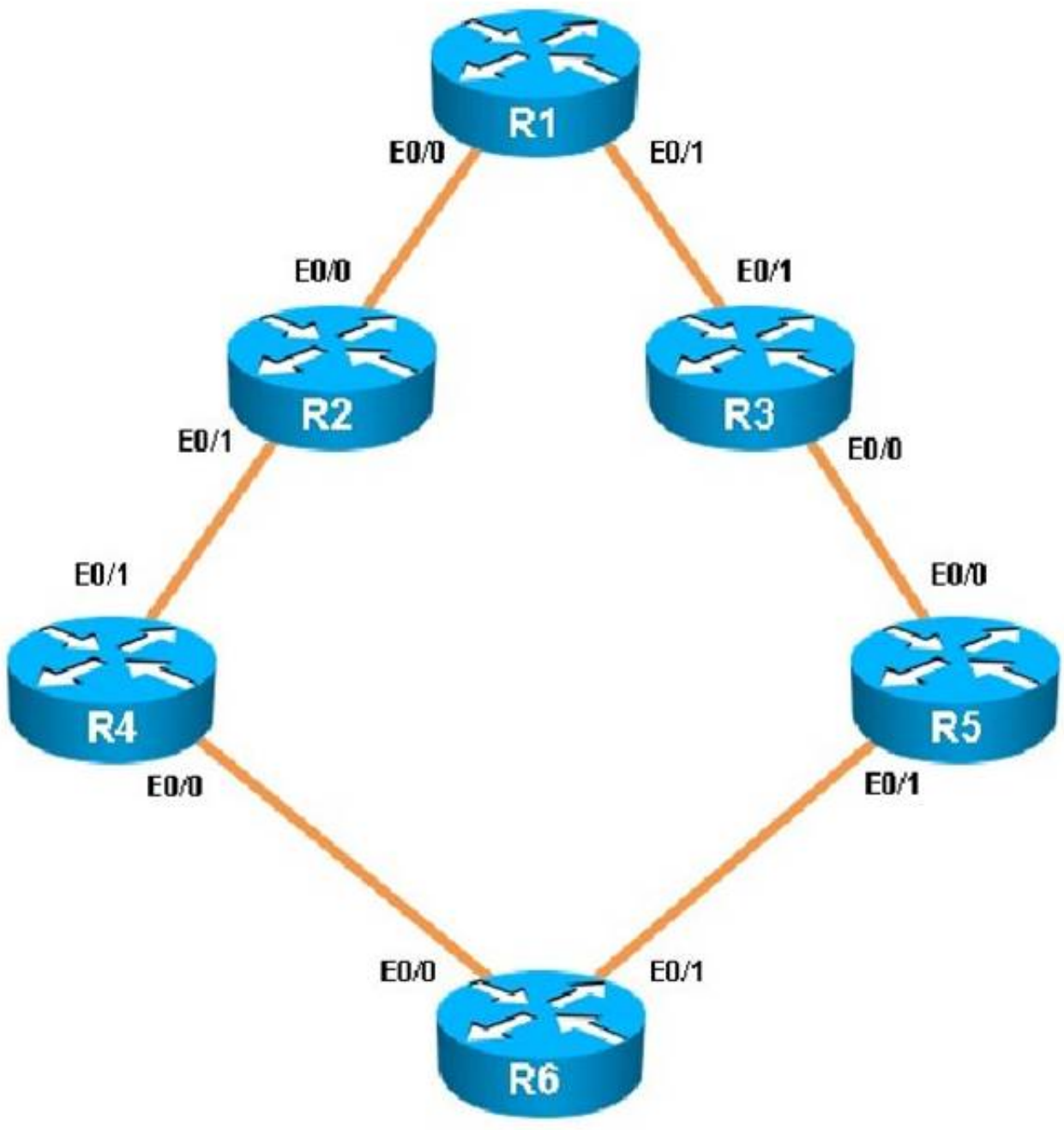
```
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 172.16.100.1 255.255.255.0
!
interface Vlan200
 ip address 172.16.200.1 255.255.255.0
!
interface Vlan300
 ip address 192.168.10.1 255.255.255.0
!
```

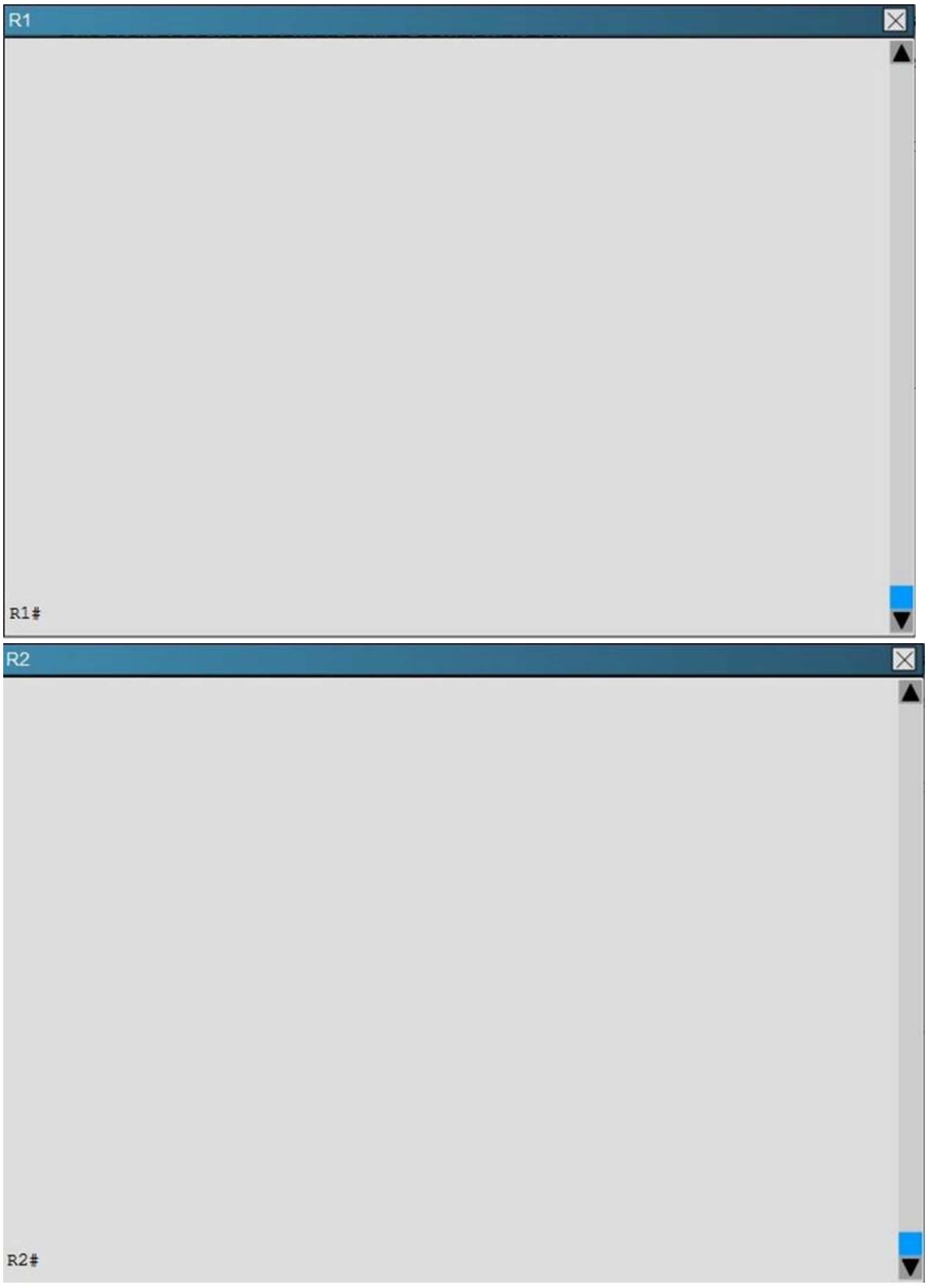
SW4

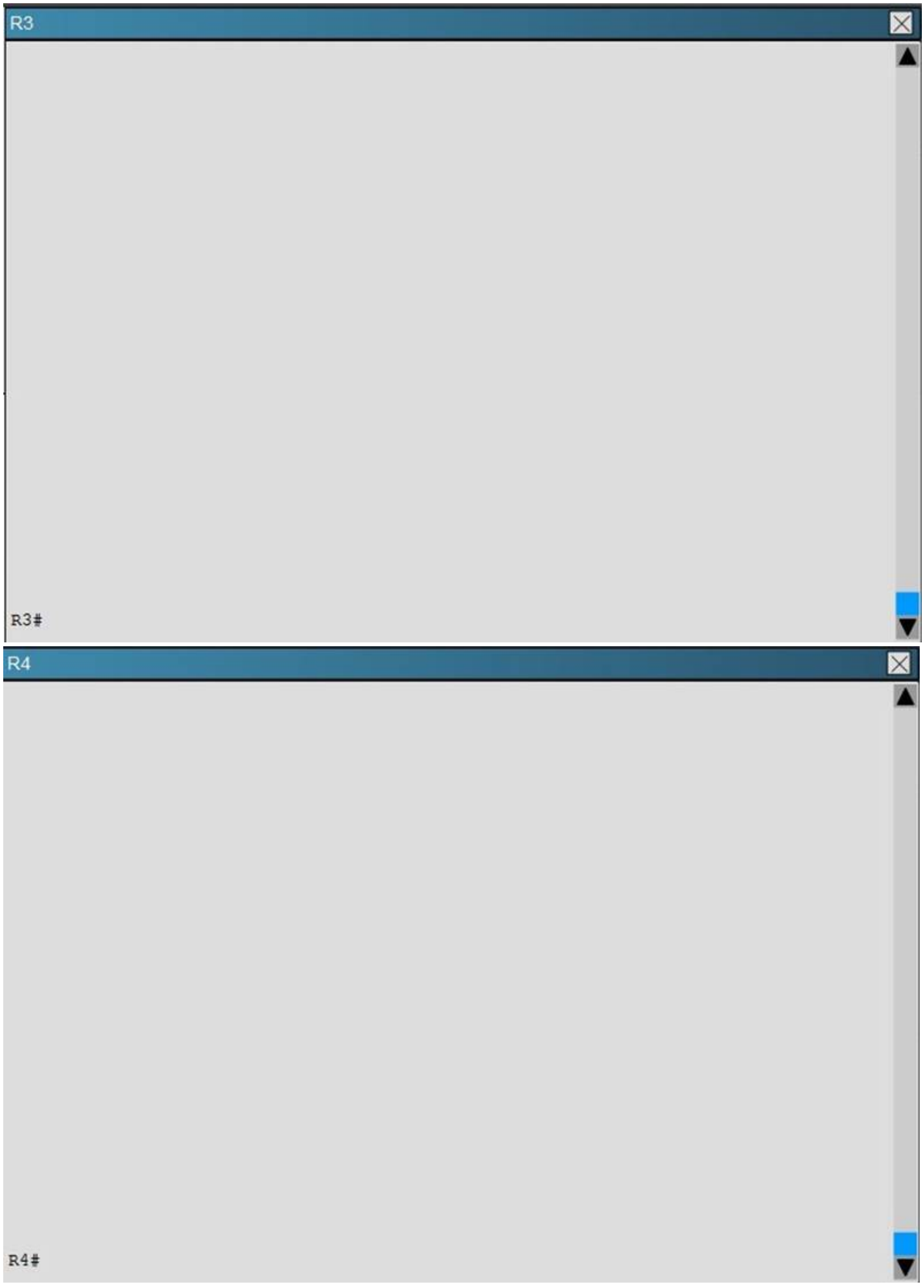
```
 switchport mode trunk
 duplex auto
!
interface Ethernet2/2
 shutdown
 duplex auto
!
interface Ethernet2/3
 shutdown
 duplex auto
!
interface Vlan1
 no ip address
!
interface Vlan300
 ip address 192.168.100.4 255.255.255.0
!
!
```

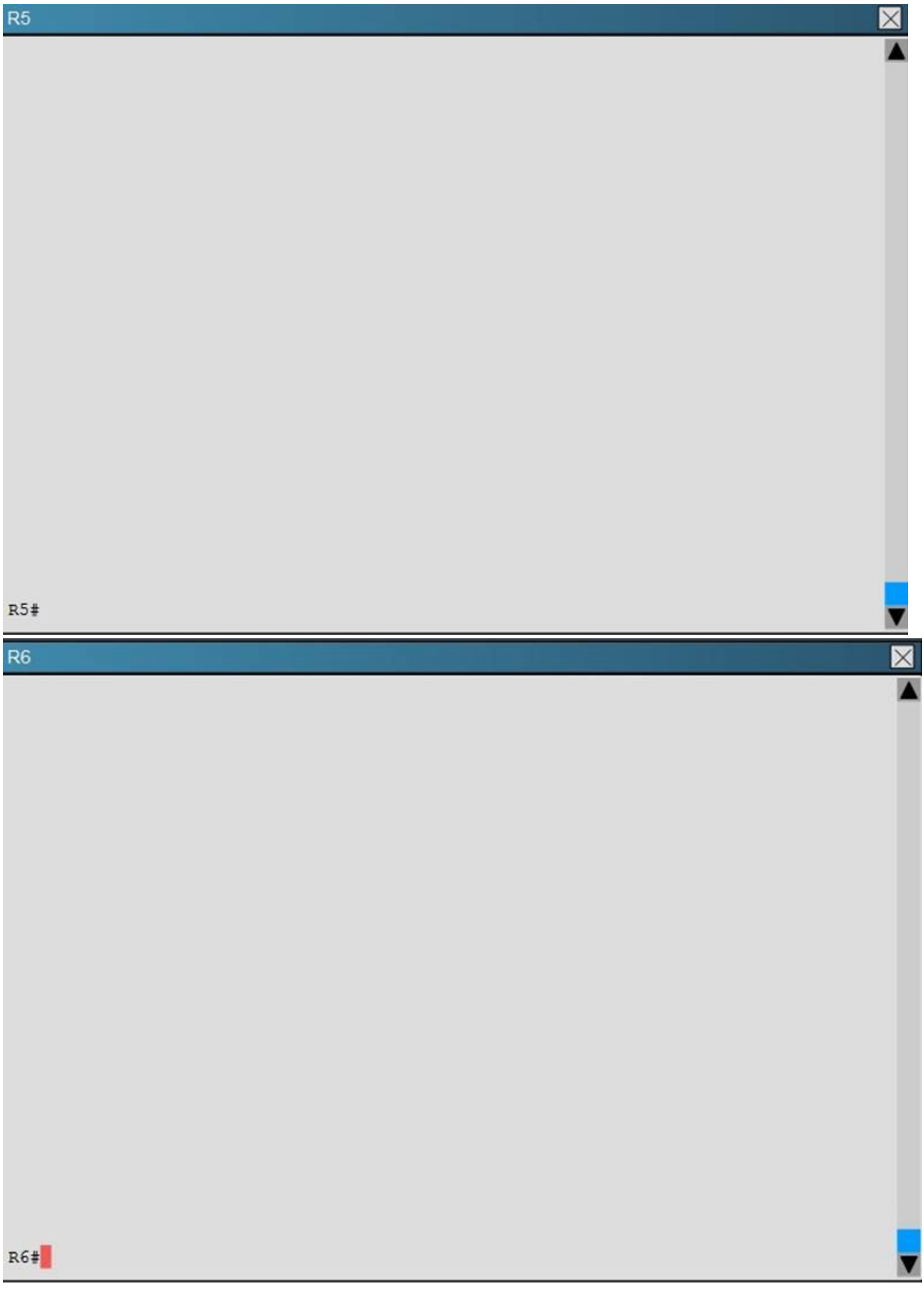
Topic 3, Troubleshooting EIGRP

NEW QUESTION 70
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

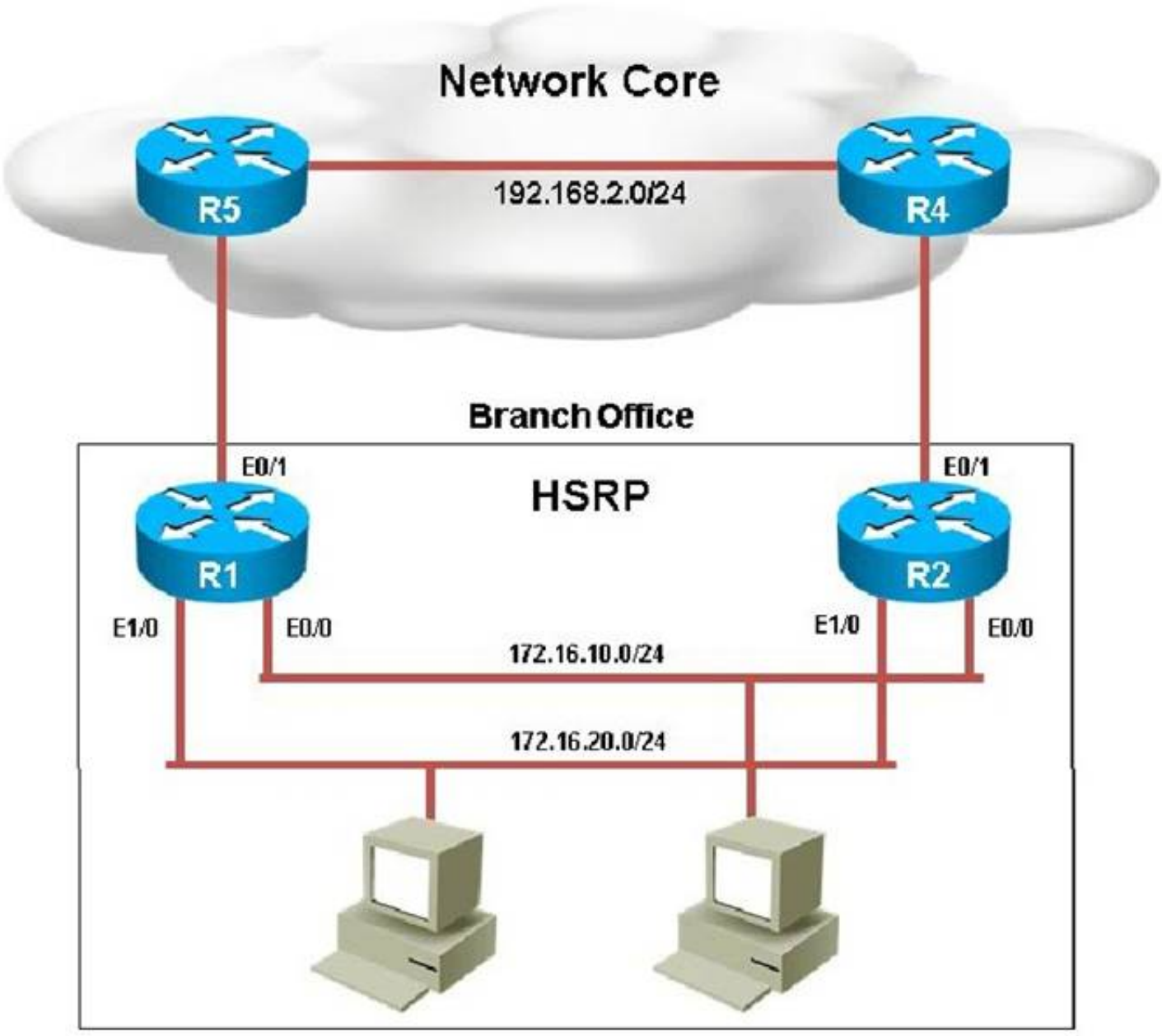
```
!
router eigrp 1
 distribute-list 3 in Ethernet0/0
 distribute-list 3 in Ethernet0/1
 network 192.168.35.0
 network 192.168.56.0
!
!
```

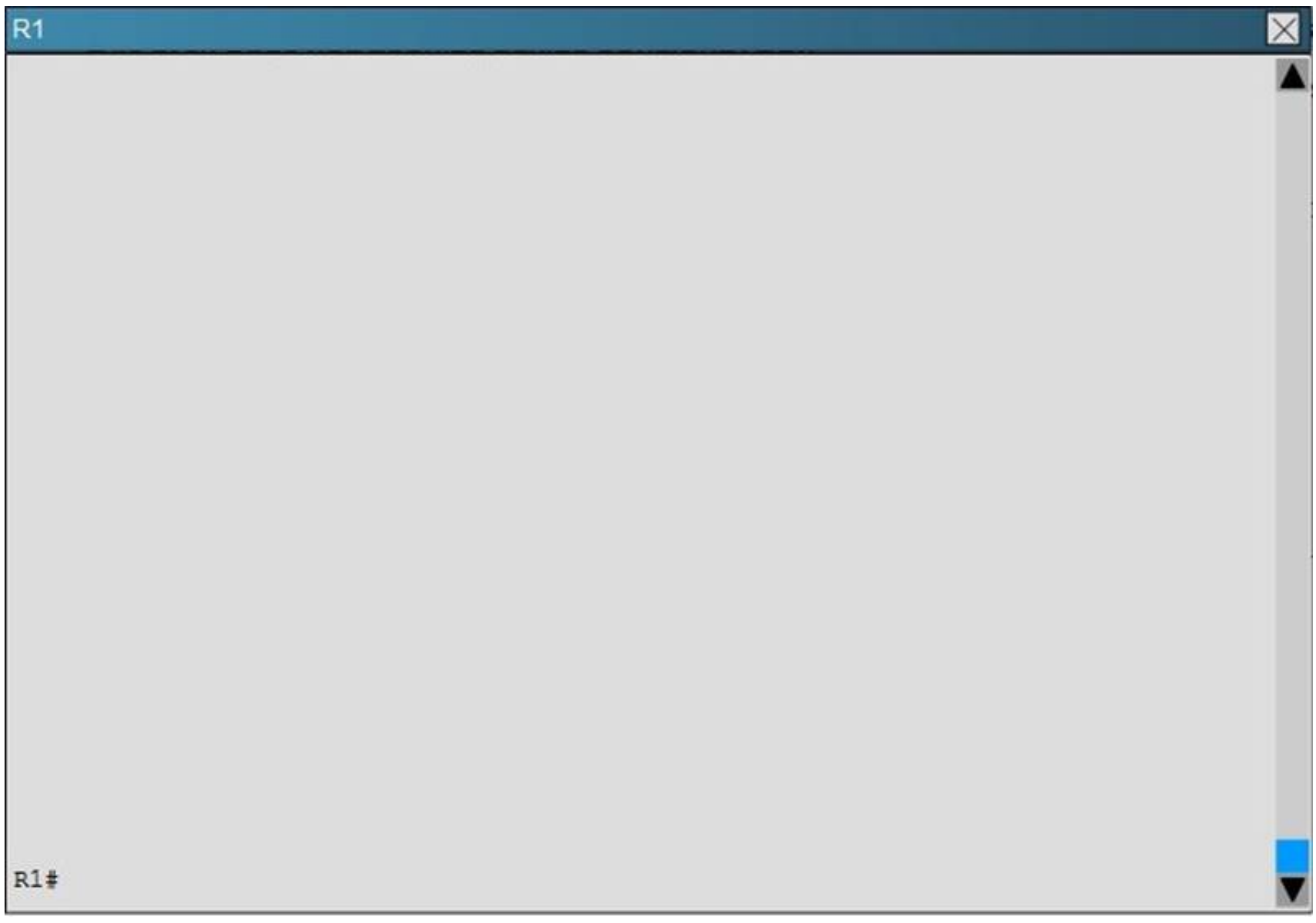
R5

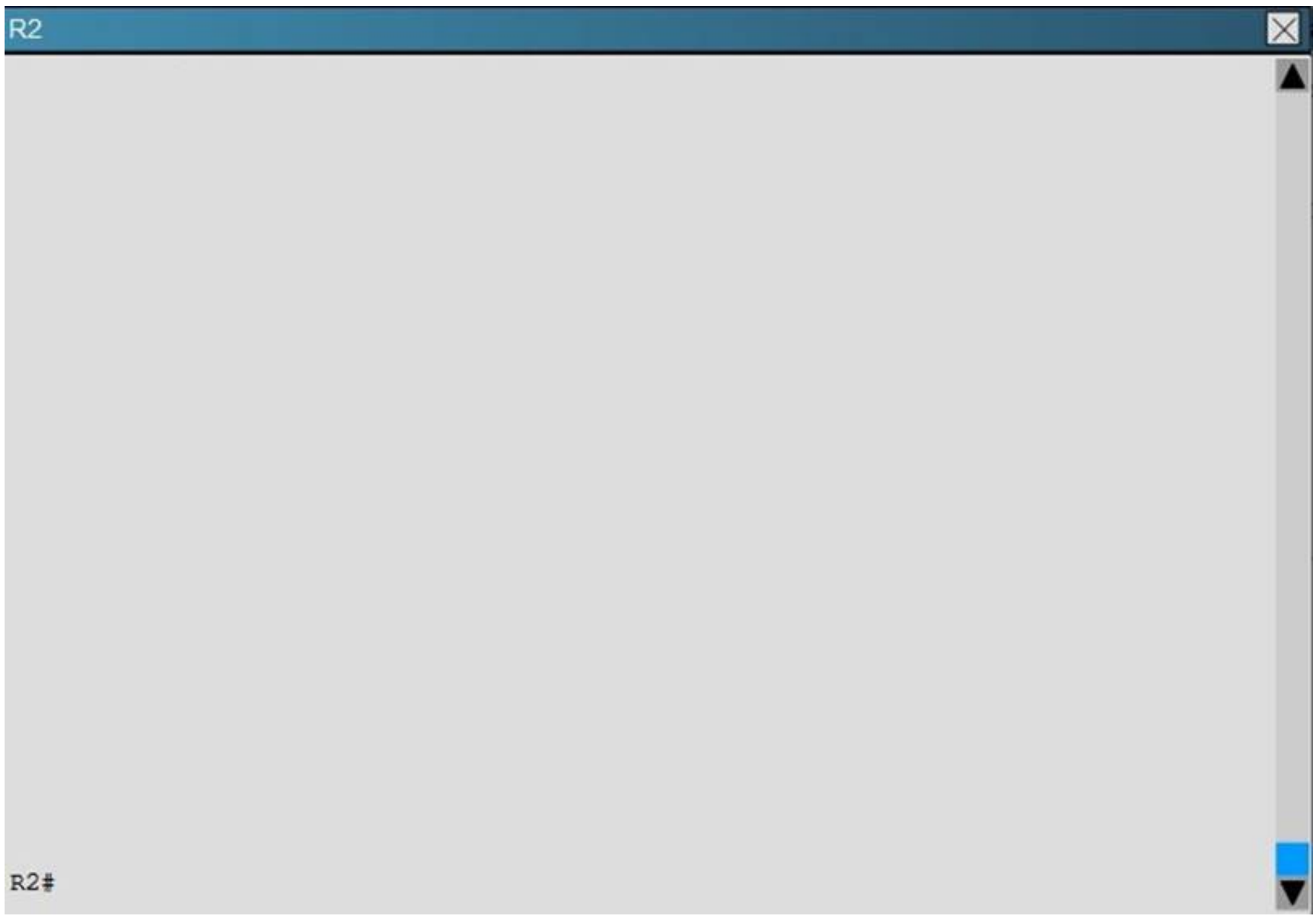
```
!
access-list 1 permit 192.168.1.15
access-list 1 permit 192.168.1.24
access-list 1 permit 192.168.1.17
access-list 1 permit 192.168.1.20
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny   150.1.1.1
access-list 3 deny   192.168.46.0 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#
```

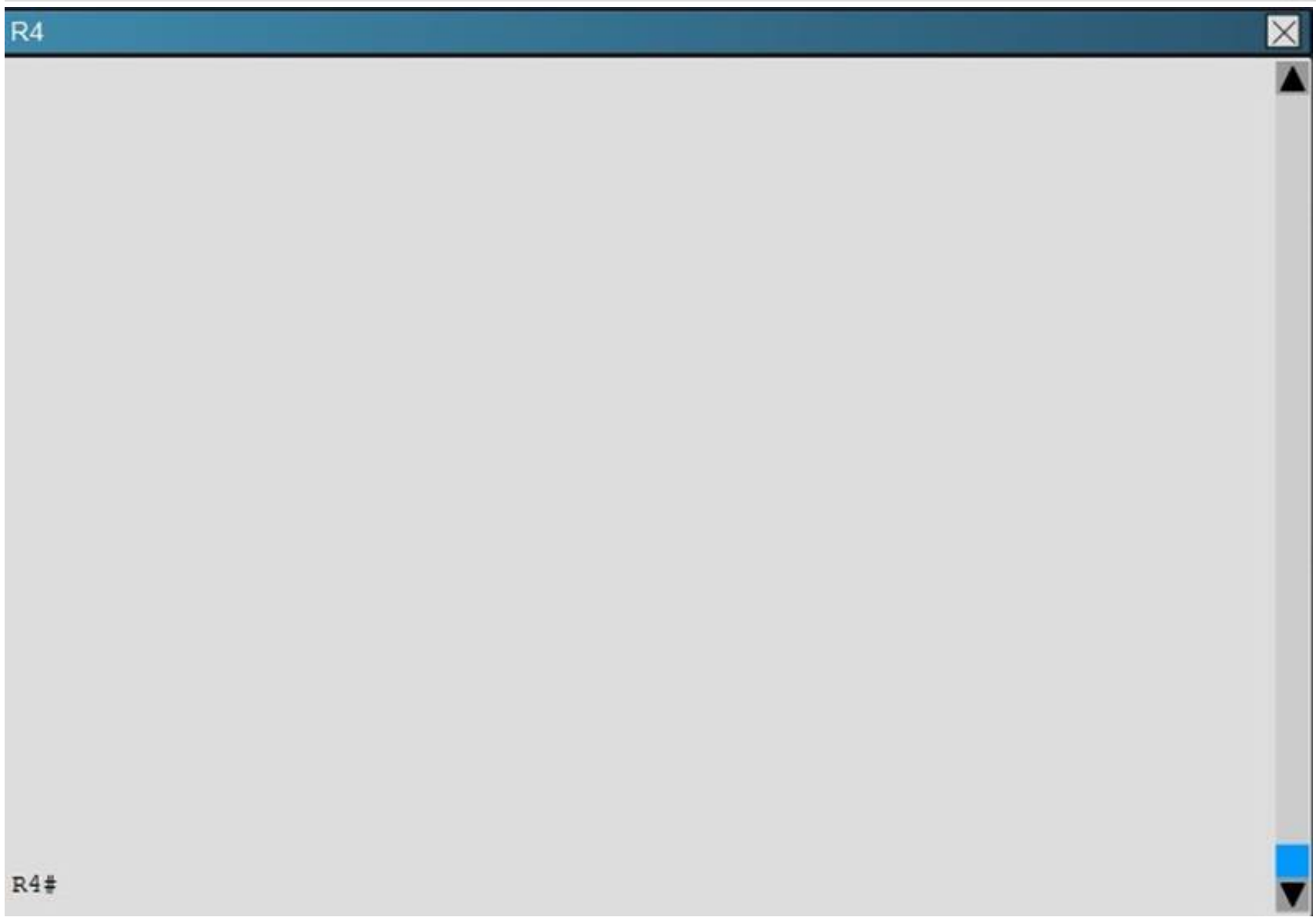
Topic 4, Troubleshooting HSRP

NEW QUESTION 73
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

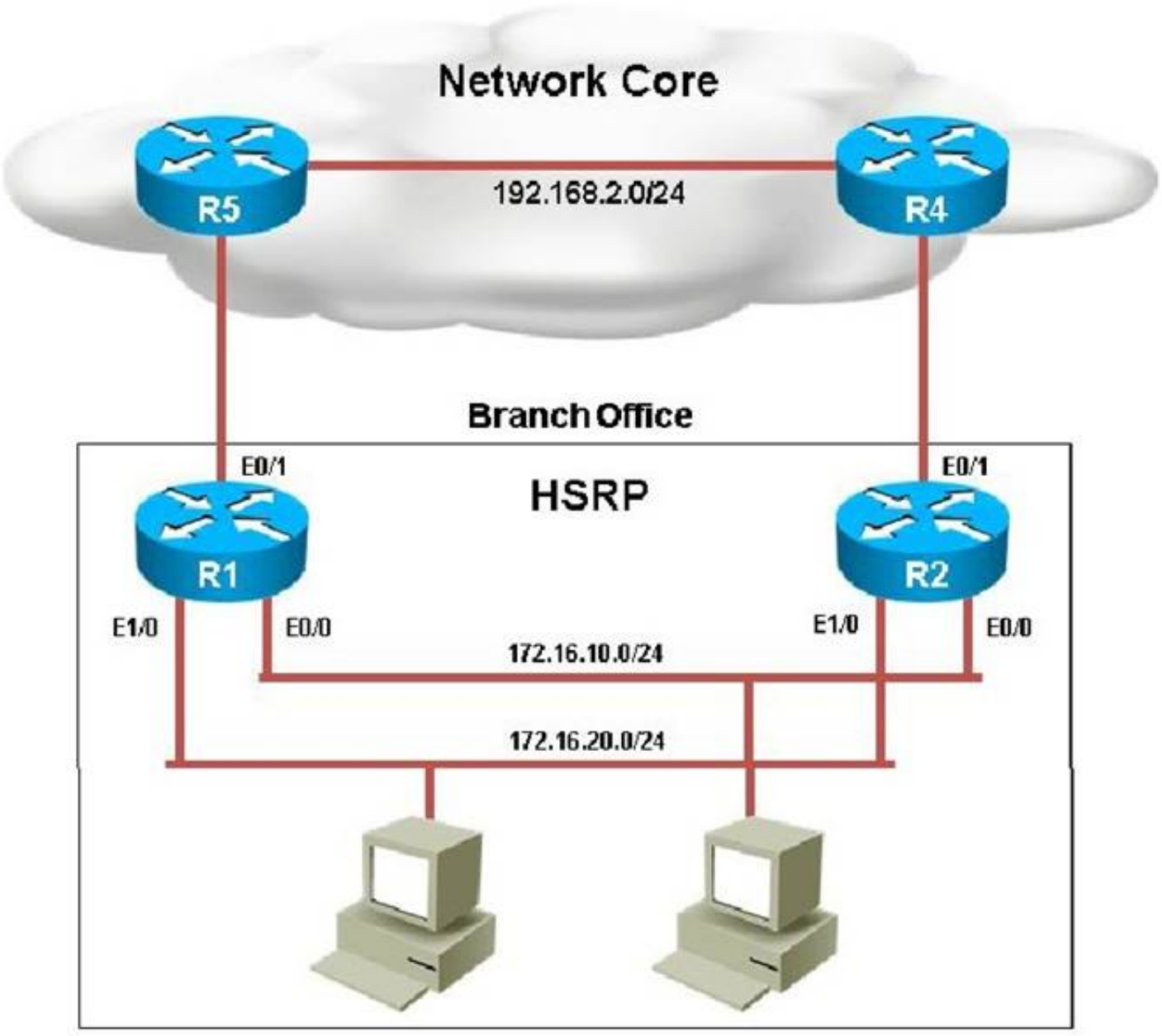
```
interface Ethernet1/0
 description connection to 172.16.20.0/24 network
 ip address 172.16.20.2 255.255.255.0
 ip access-group 102 in
 standby version 2
 standby 2 ip 172.16.20.254
 standby 2 authentication cisco123
!
```

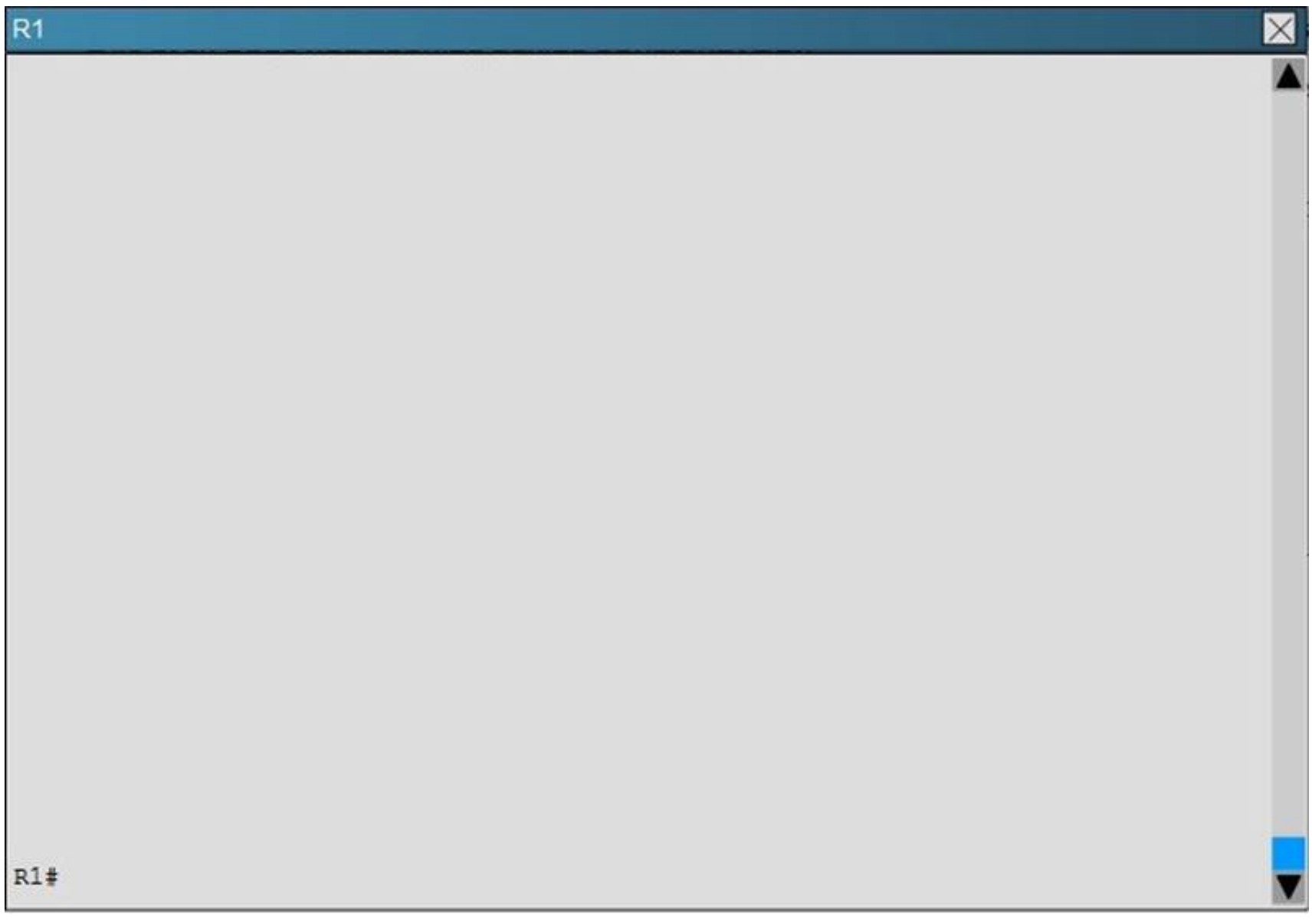
R1

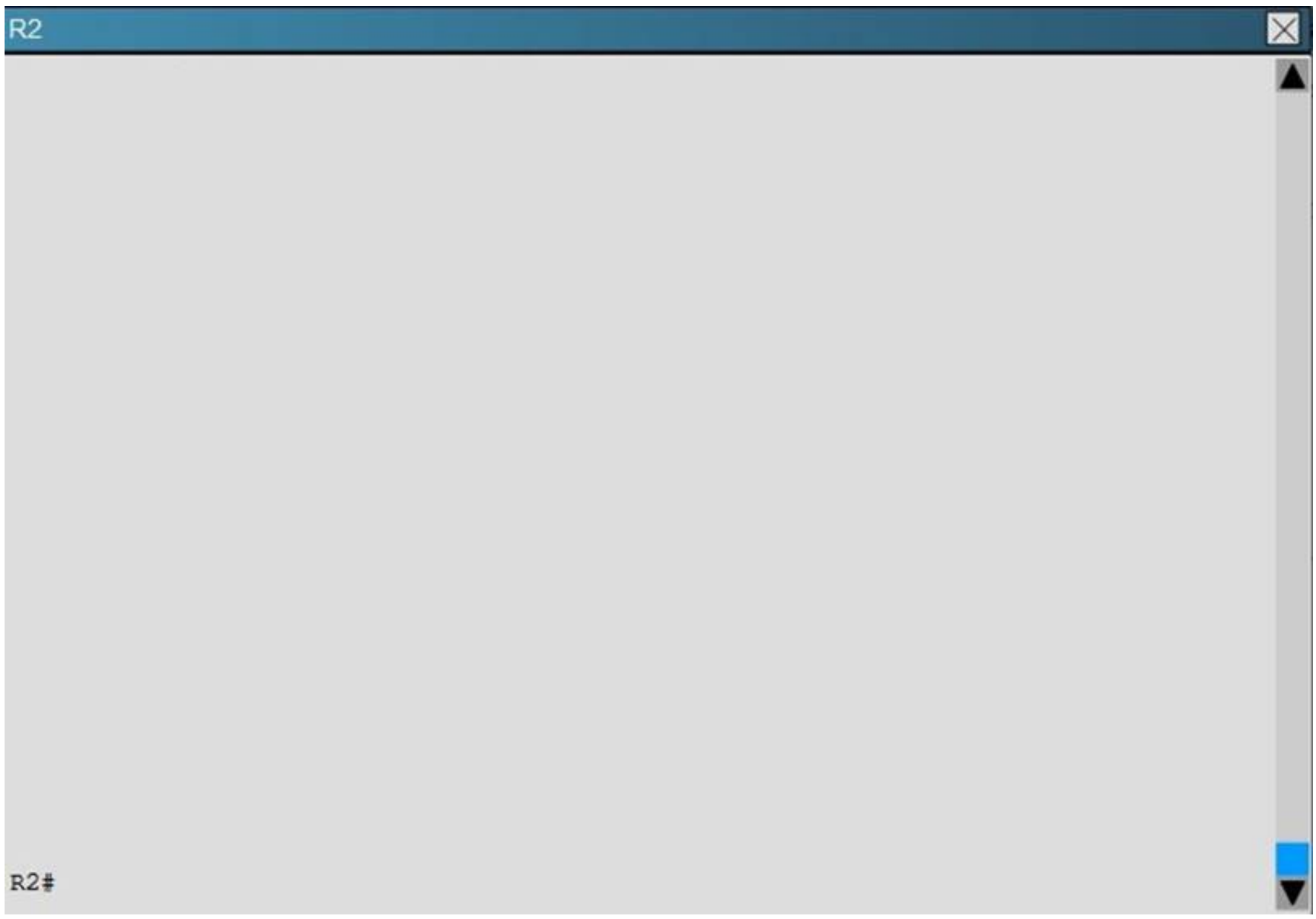
```
no ip http server
!
access-list 102 deny   ip any host 224.0.0.102
access-list 102 permit ip any any
!
!
```

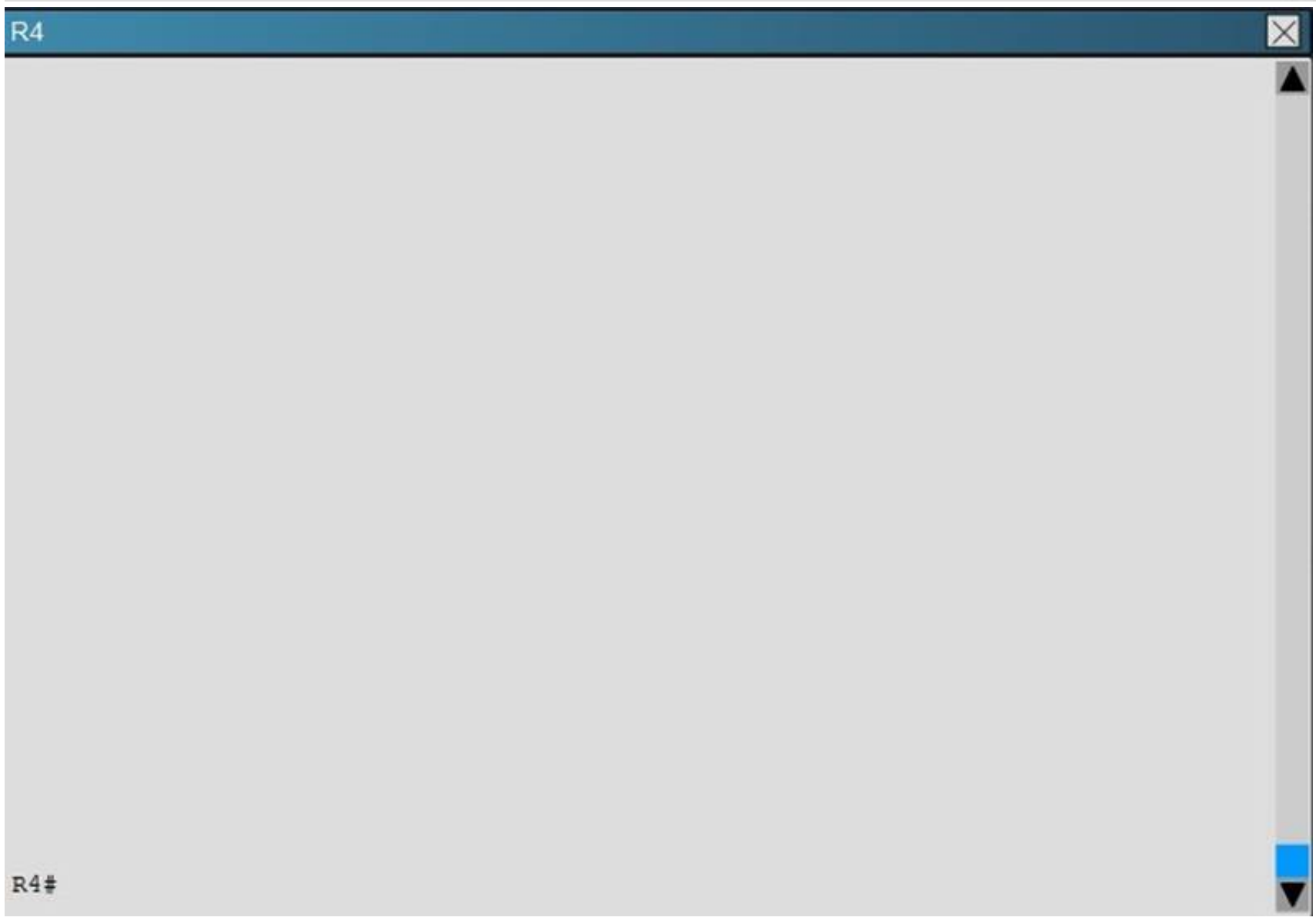
This access list is blocking all traffic to the 224.0.0.102 IP address, which is the multicast address used by HSRP.

NEW QUESTION 76
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#

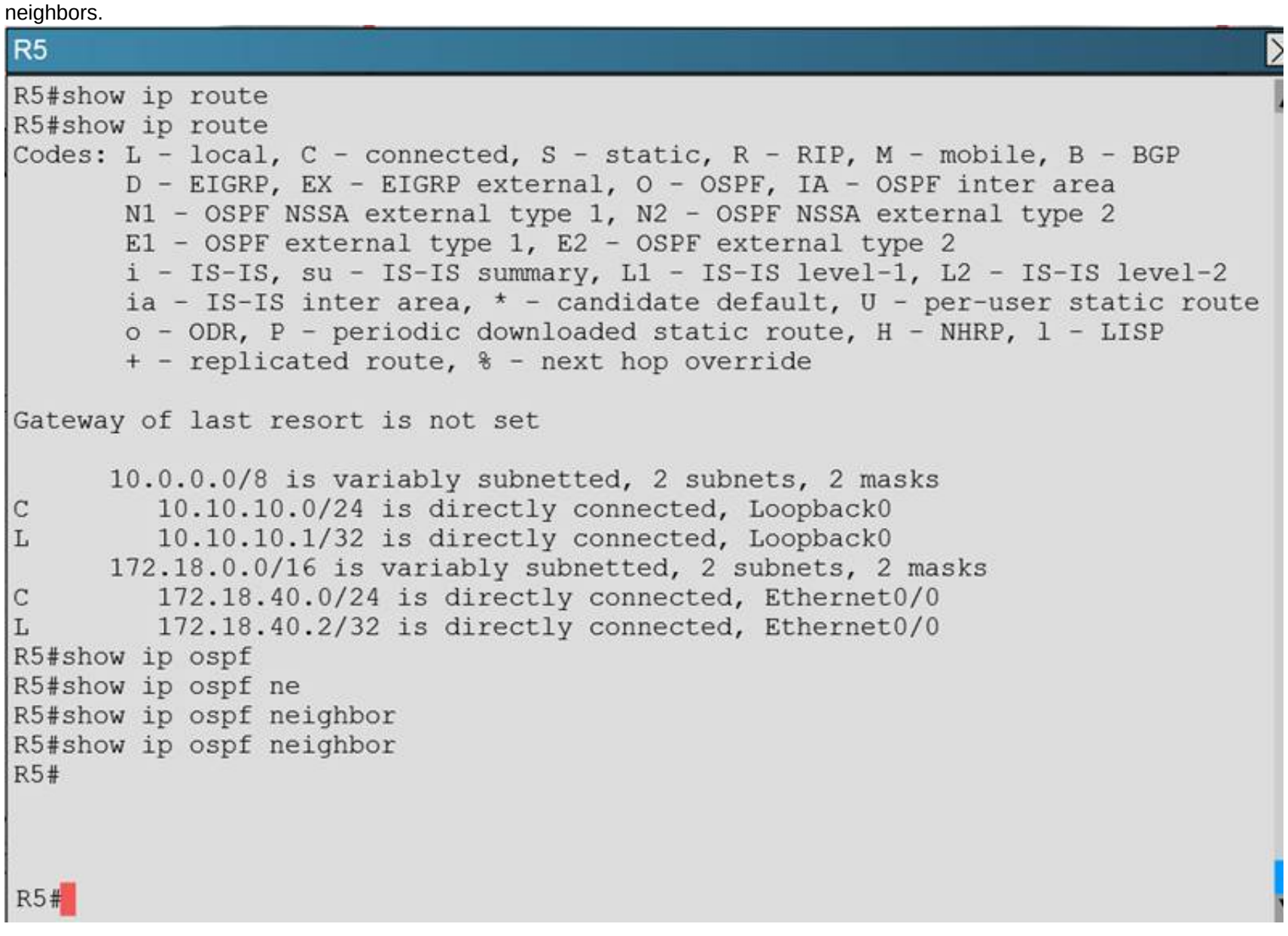

R4
R4#

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

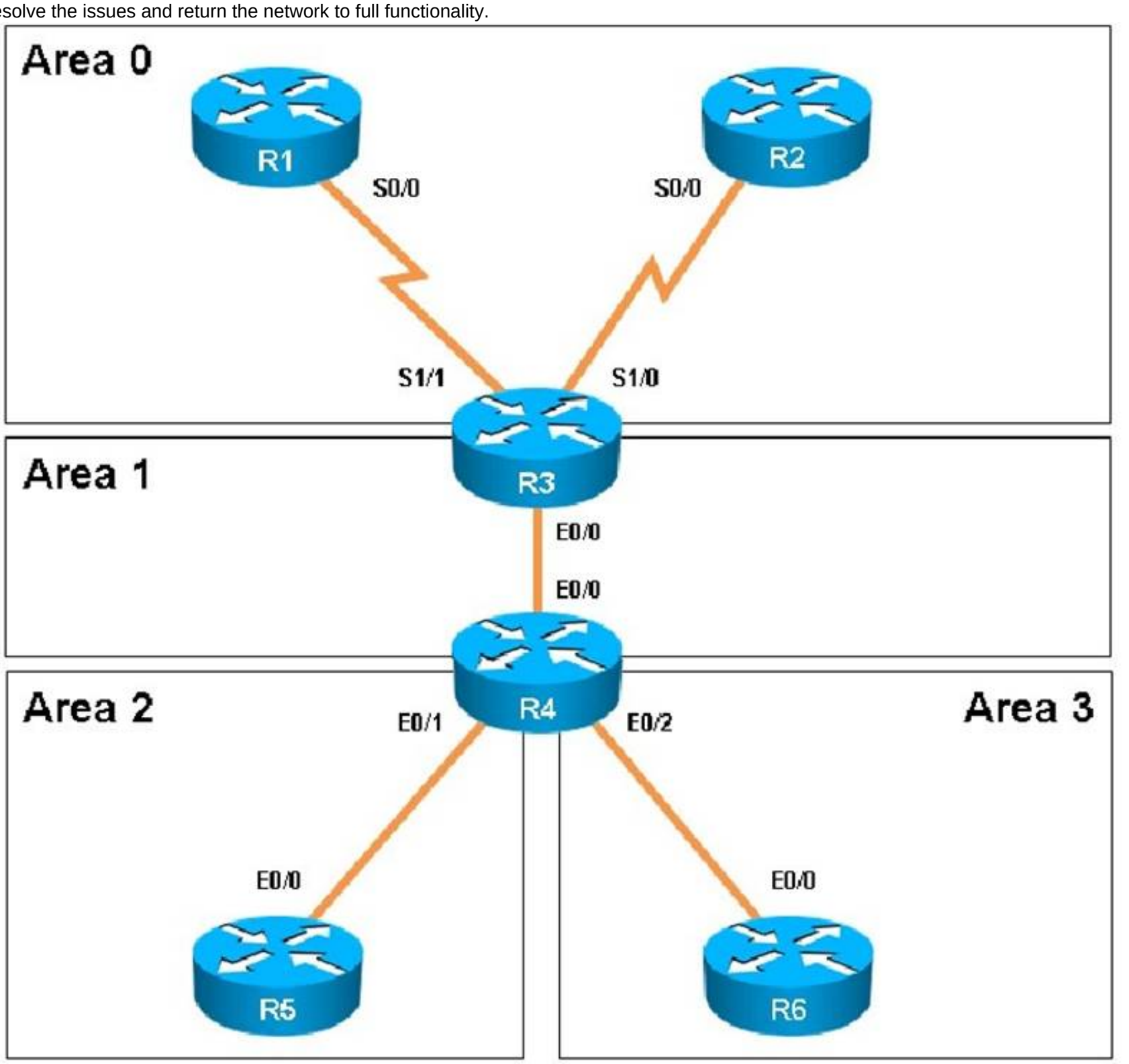
A. HSRP issue between R5 and R4
B. There is an OSPF issue between R5and R4
C. There is a DHCP issue between R5 and R4
D. The distribute-list configured on R5 is blocking route entries
E. The ACL configured on R5 is blocking traffic for the subnets advertised from R4.

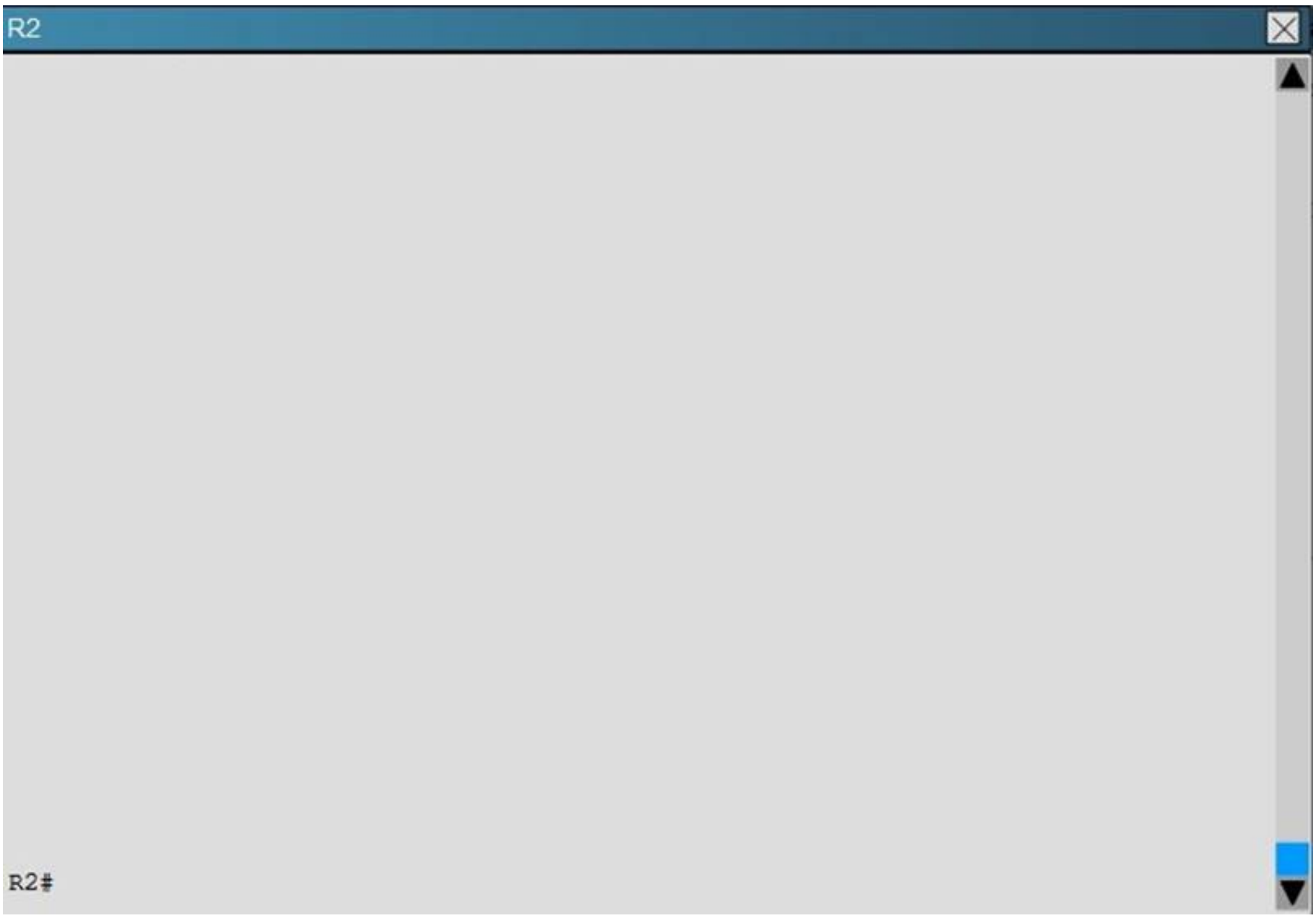
Answer: B

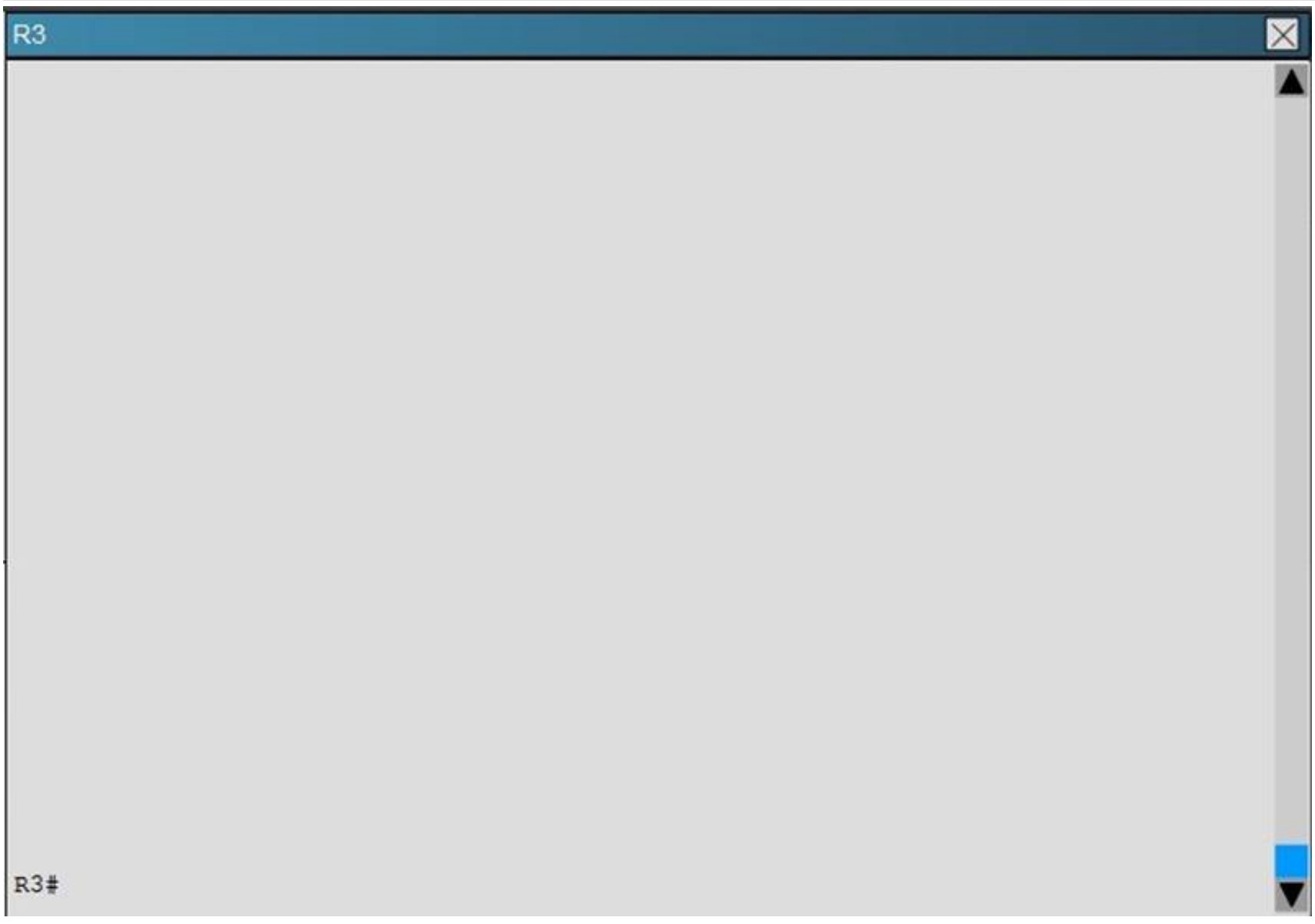
Explanation: If we issue the “show ip route” and “show ip ospf neighbor” commands on R5, we see that there are no learned OSPF routes and he has no OSPF neighbors.

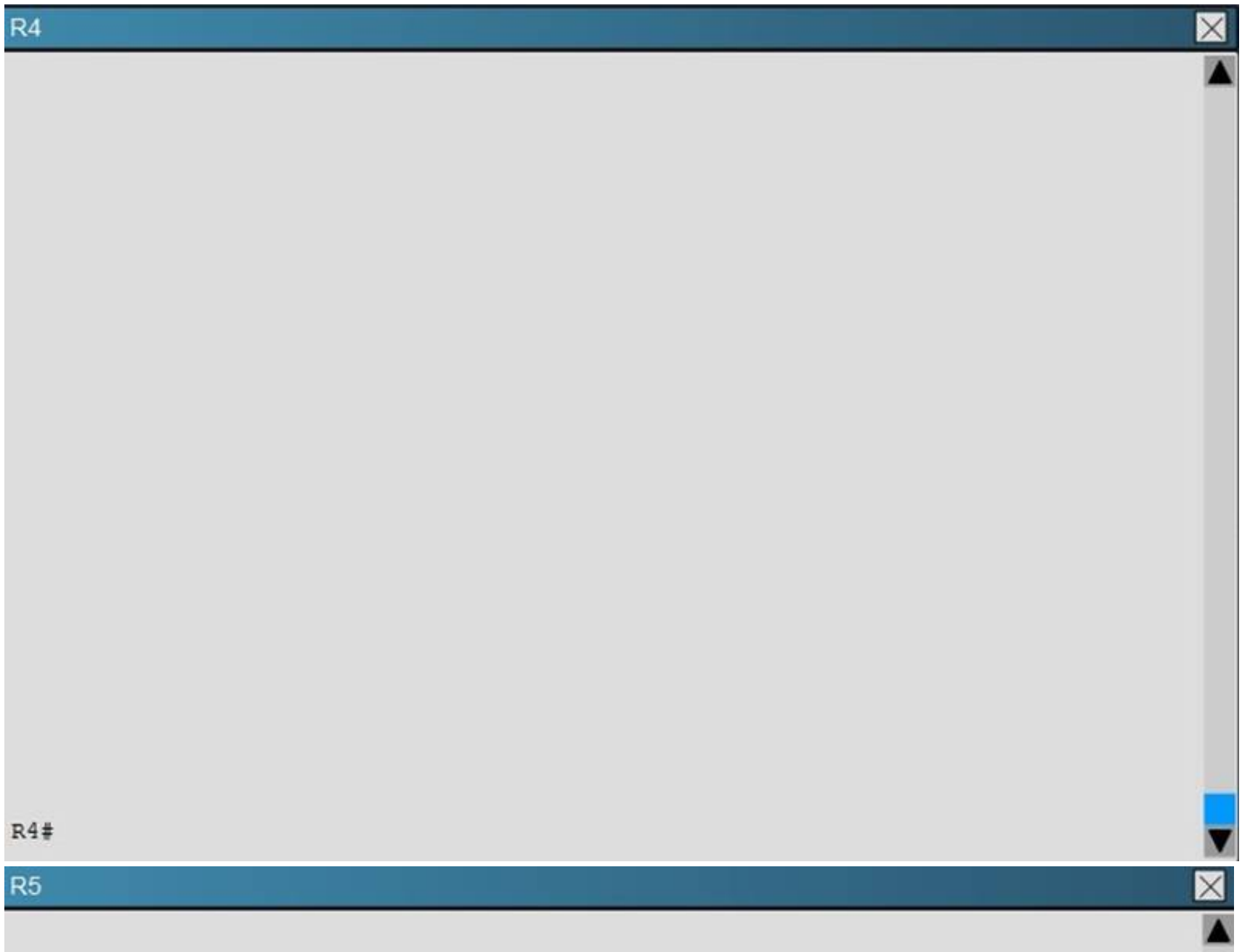


NEW QUESTION 77
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.




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

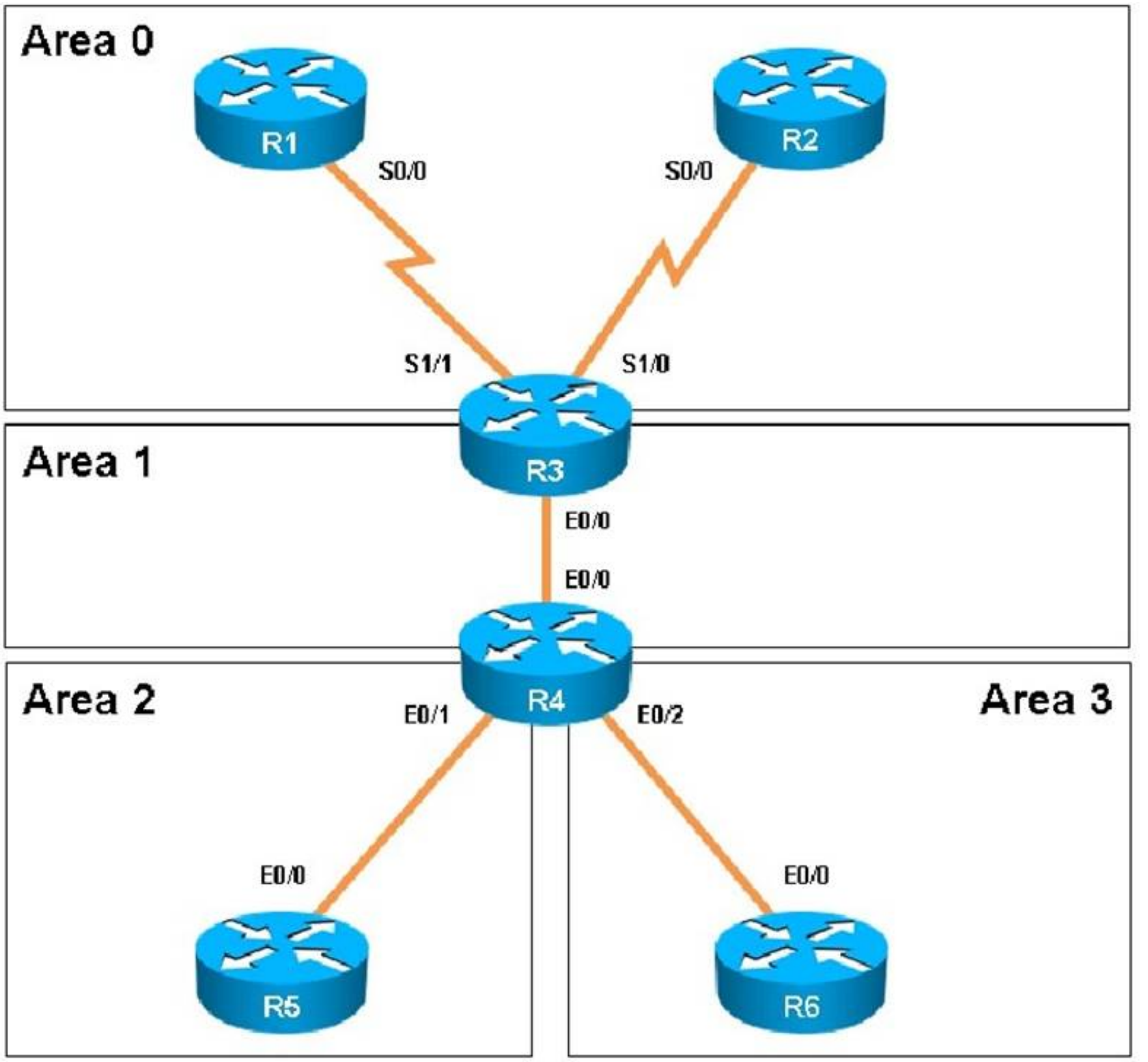
```
interface Ethernet0/0
 ip address 192.168.45.5 255.255.255.0
 ip ospf authentication-key CISCO
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
router ospf 100
 router-id 5.5.5.5
 auto-cost reference-bandwidth 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
```

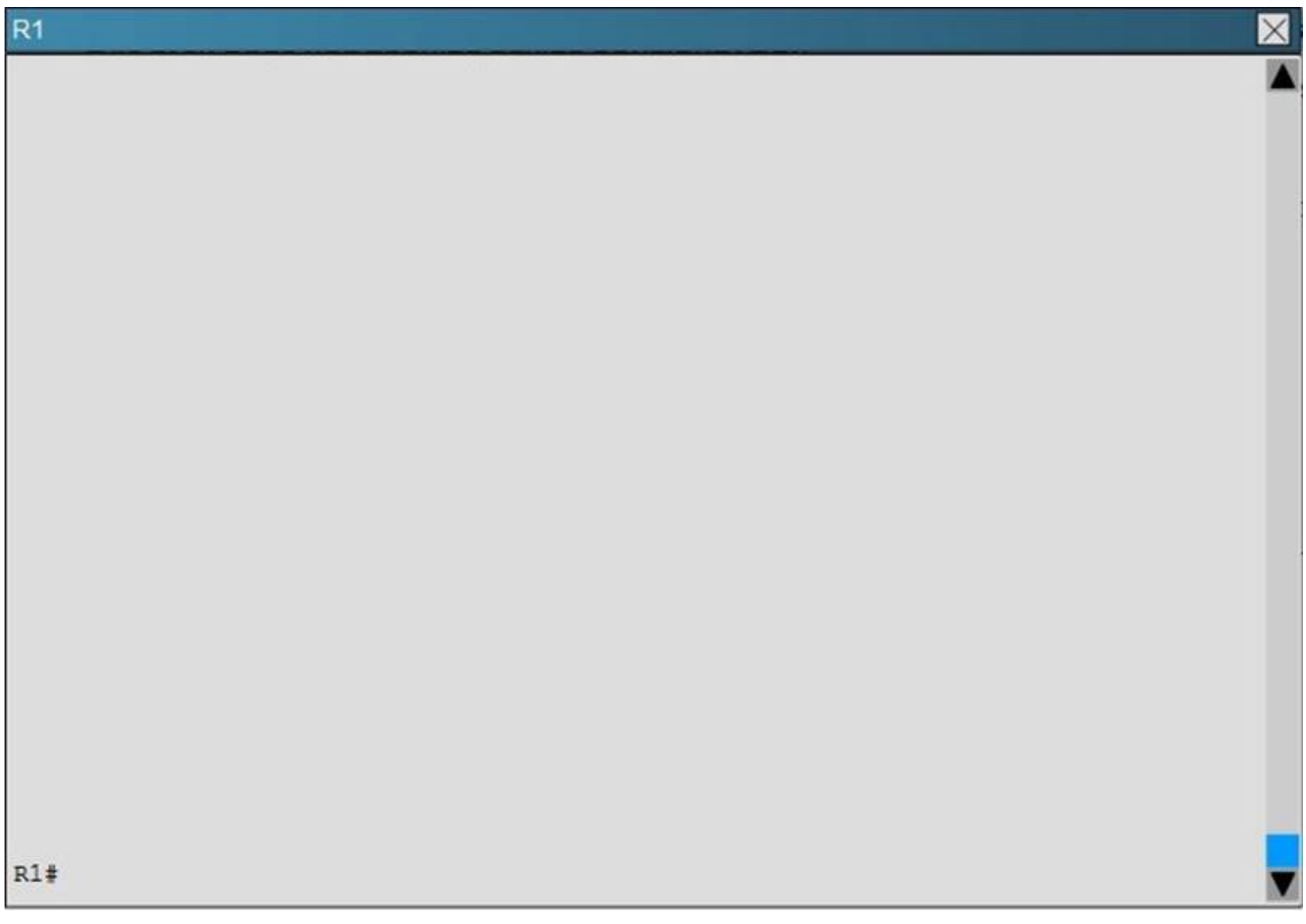
However, this has not been done on the link to R5 on R4:

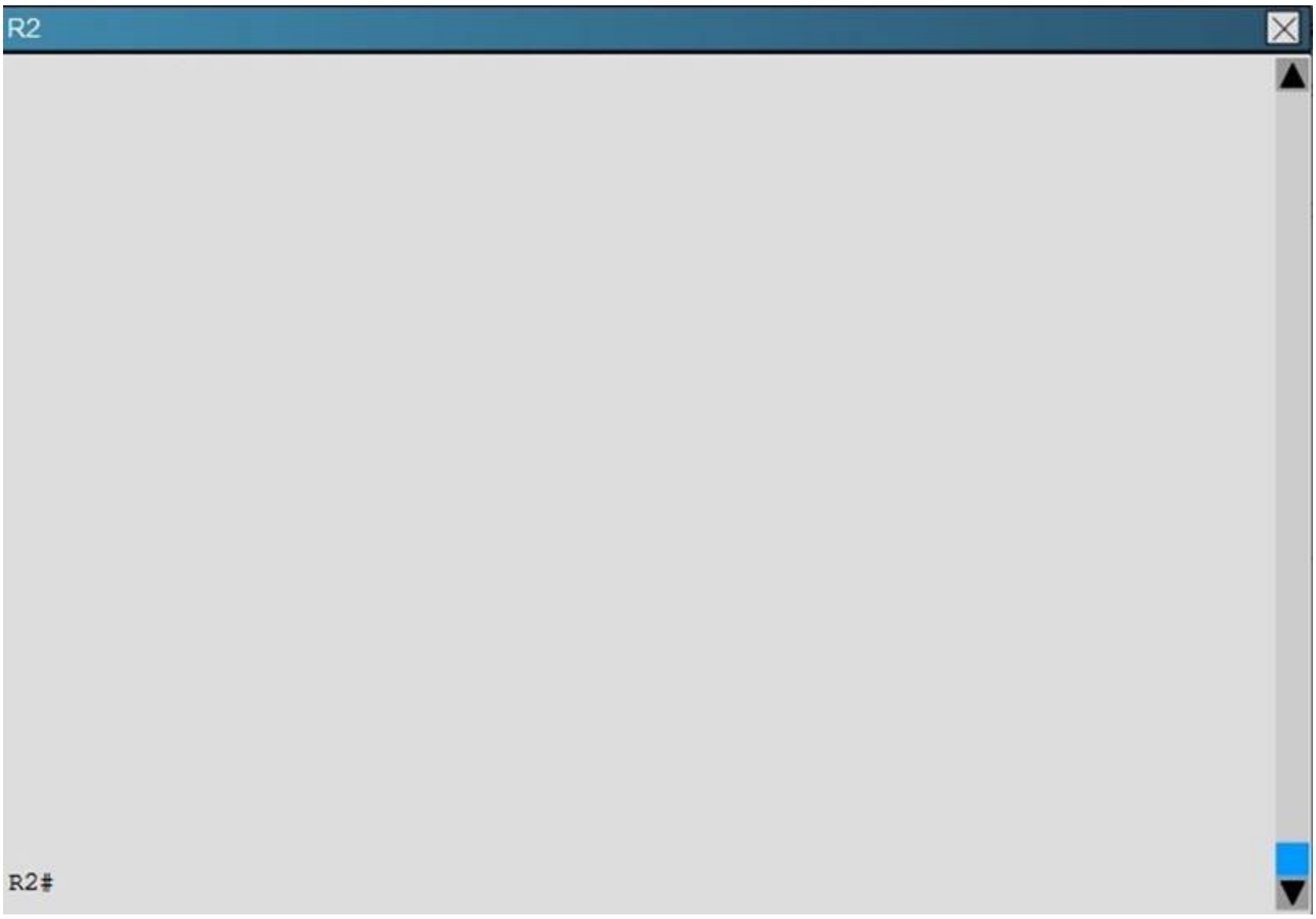
R4

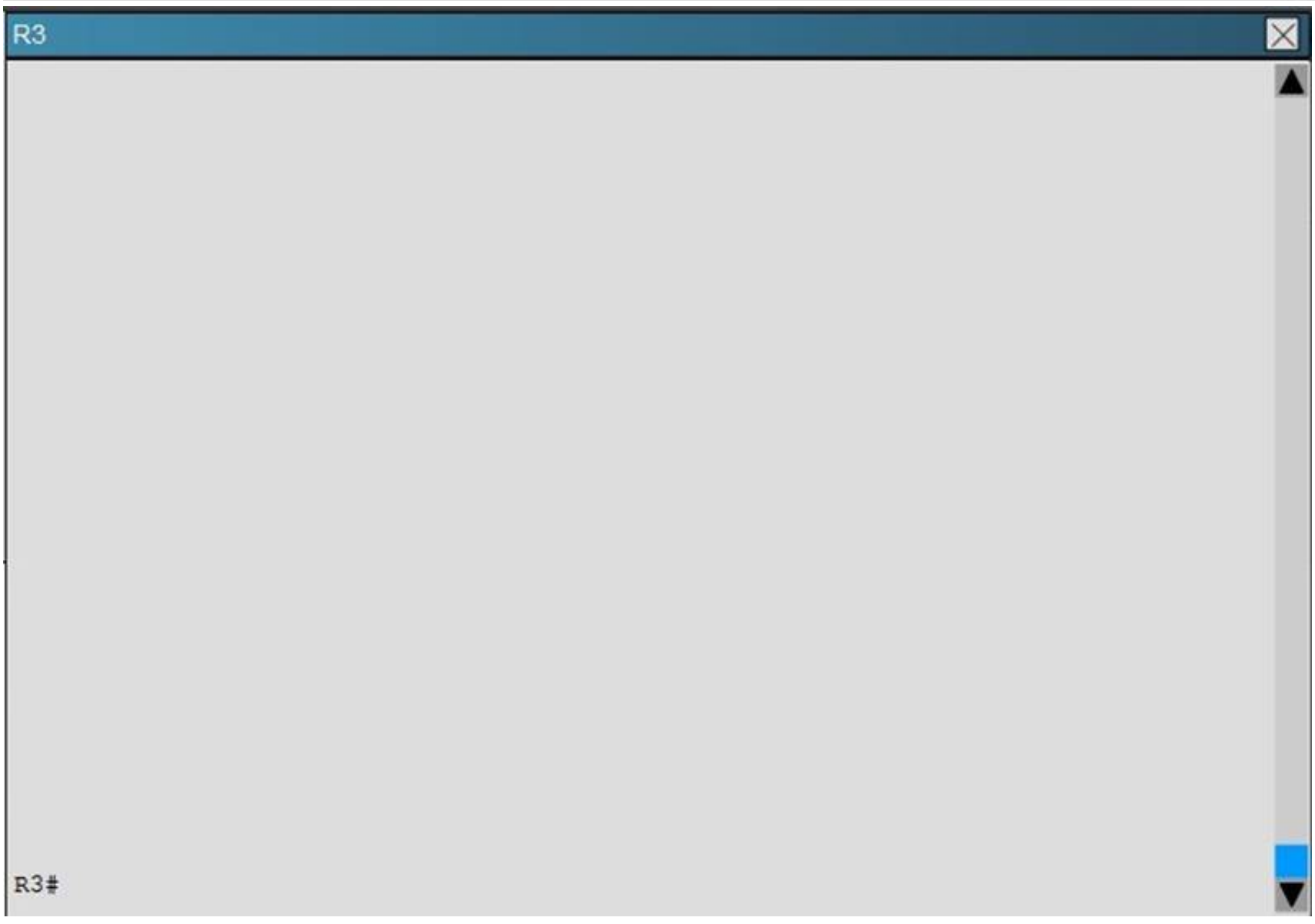
```
interface Ethernet0/1
 ip address 192.168.45.4 255.255.255.0
!
interface Ethernet0/2
 ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router ospf 100
 router-id 4.4.4.4
 auto-cost reference-bandwidth 3000
 area 1 virtual-link 3.3.3.3
 area 2 nssa
 area 2 range 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
!
```

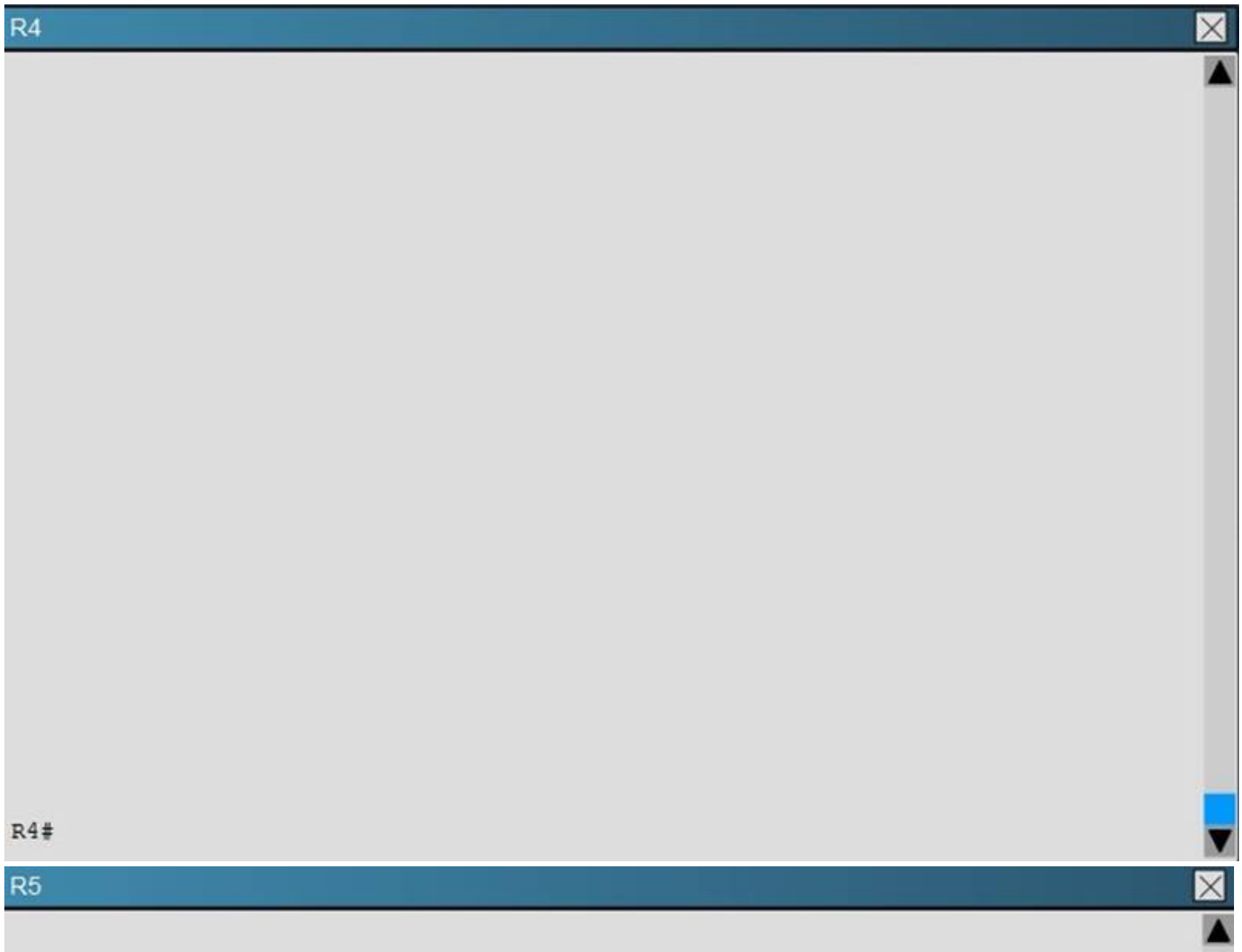
NEW QUESTION 81
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.


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 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 86
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 91
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 93
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

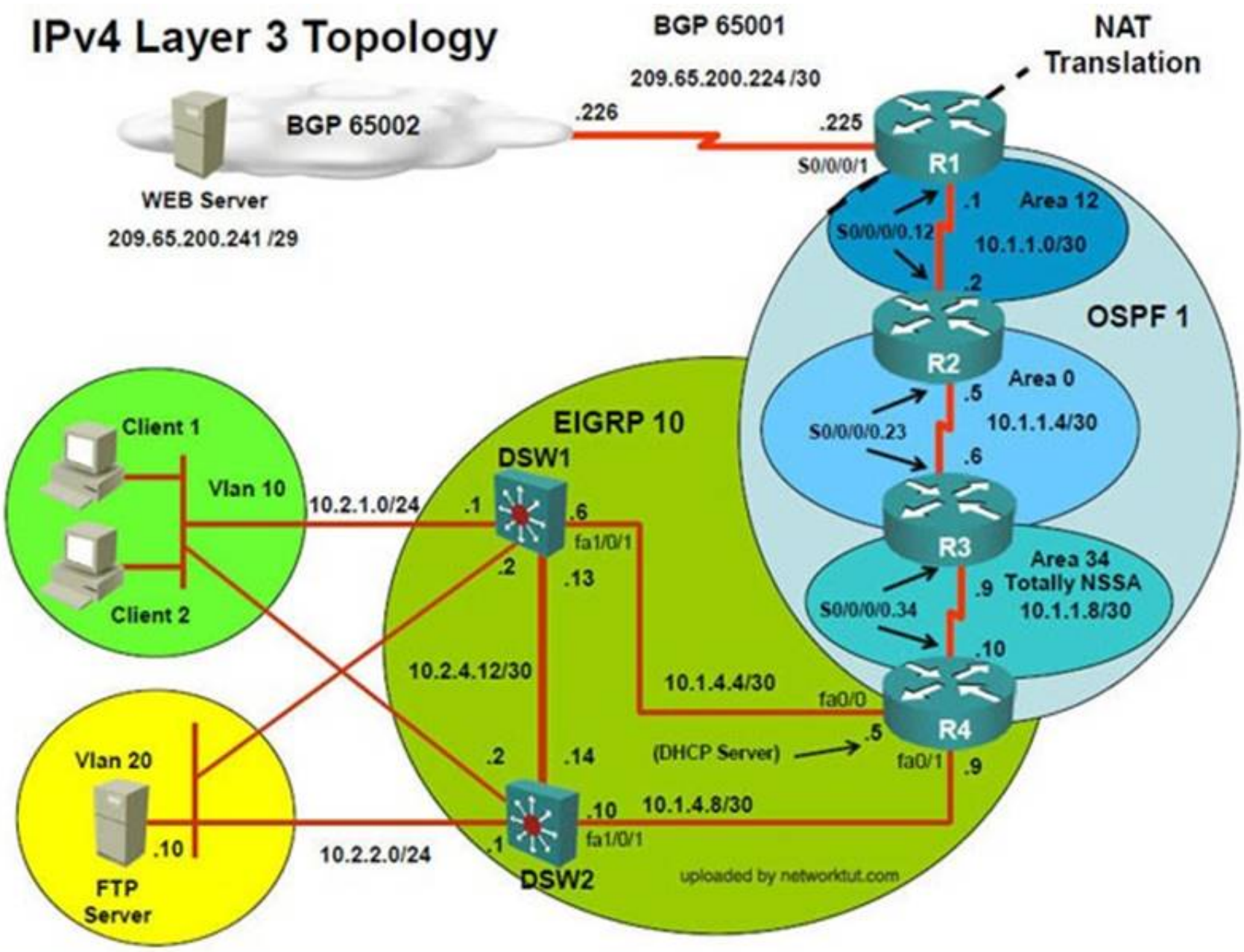
NEW QUESTION 97
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP 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?

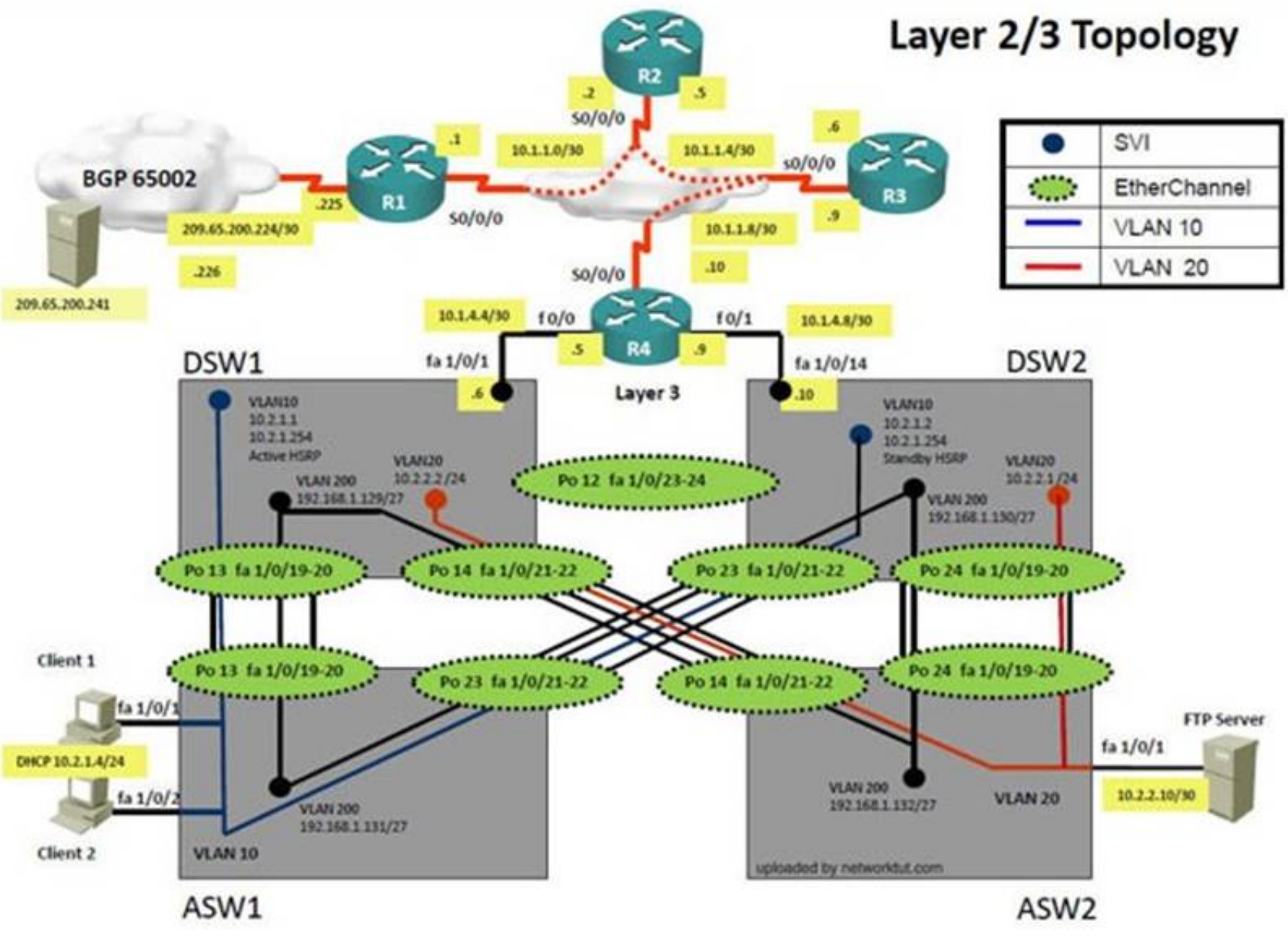
A. Enable OSPF authentication on the s0/0/0 interface using the ip ospf authentication message-digest command
B. Enable OSPF routing on the s0/0/0 interface using the network 10.1.1.0 0.0.0.255 area 12 command.
C. Enable OSPF routing on the s0/0/0 interface using the network 209.65.200.0 0.0.0.255 area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

Answer: A

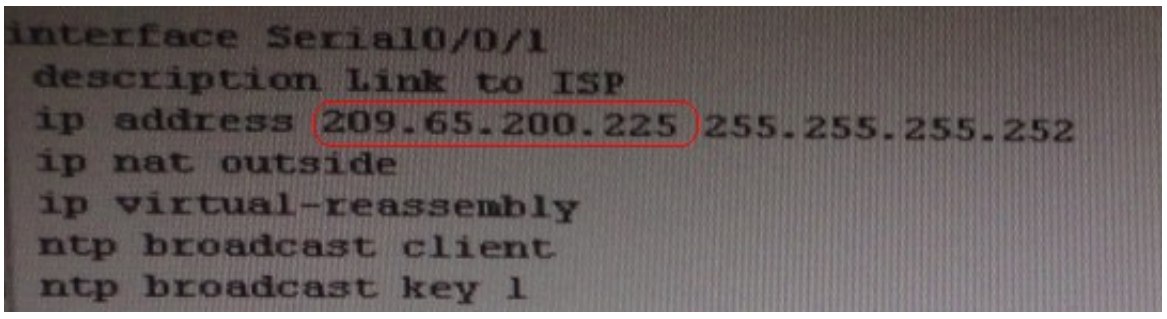
Explanation: On R1, for IPV4 authentication of OSPF the command is missing and required to configure------ ip ospf authentication message-digest

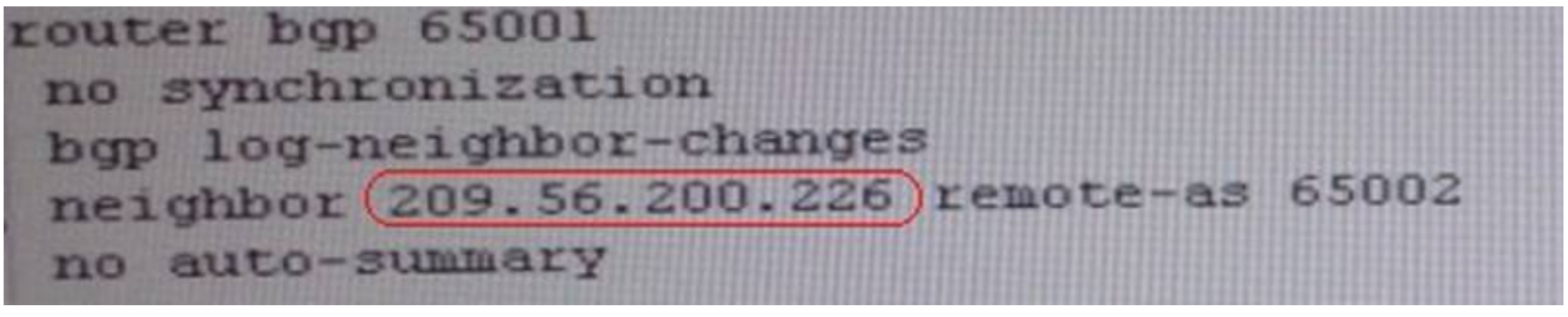
Topic 9, Ticket 4 : BGP Neighbor
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is 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





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 101
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 106
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 108
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?

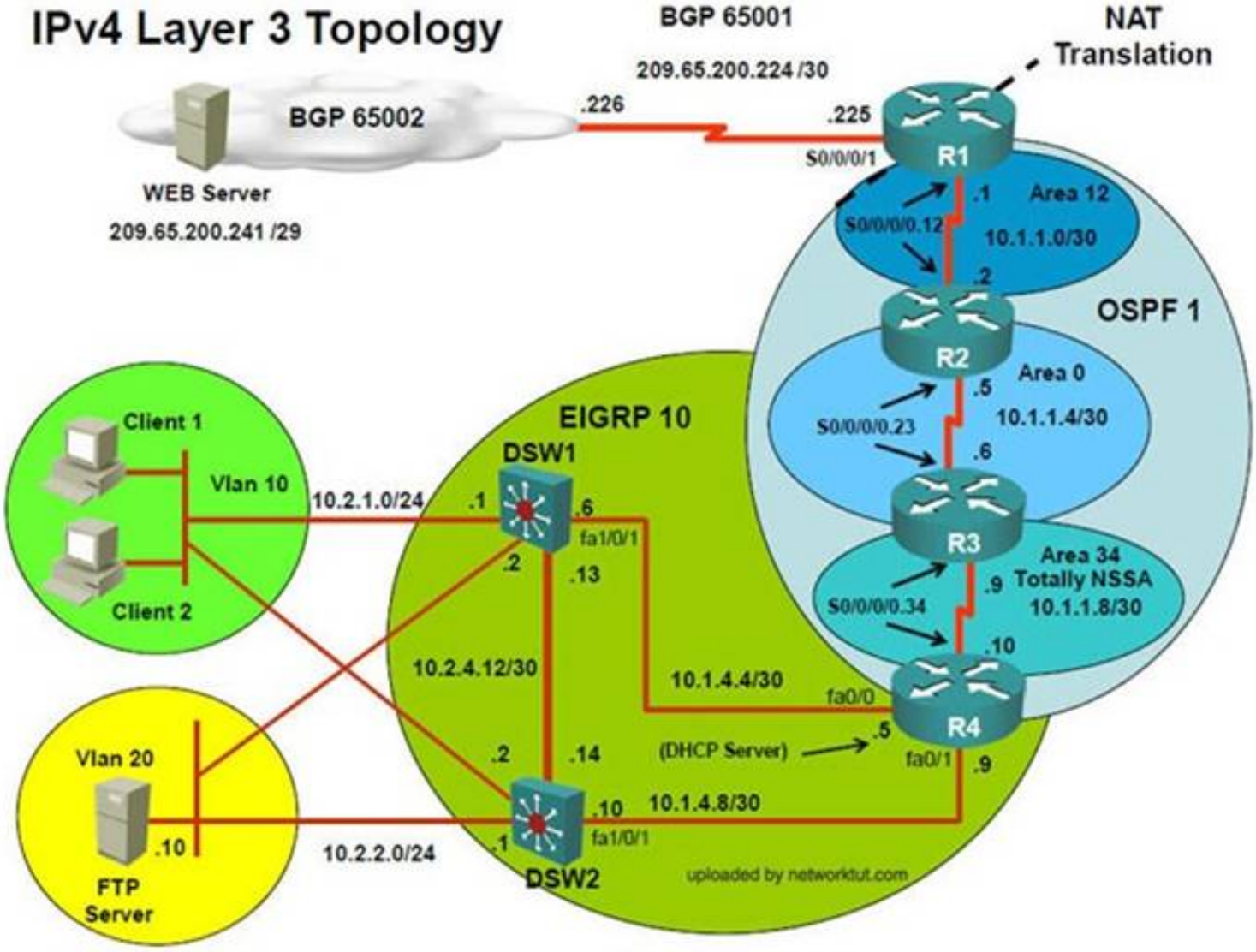
A. Under the interface Serial0/0/0 configuration enter the ip nat inside command.
B. Under the interface Serial0/0/0 configuration enter the ip nat outside command.
C. Under the ip access-list standard nat_trafic configuration enter the permit 10.2.0.0 0.0.255.255 command.
D. Under the ip access-list standard nat_trafic configuration enter the permit 209.65.200.0 0.0.0.255 command.

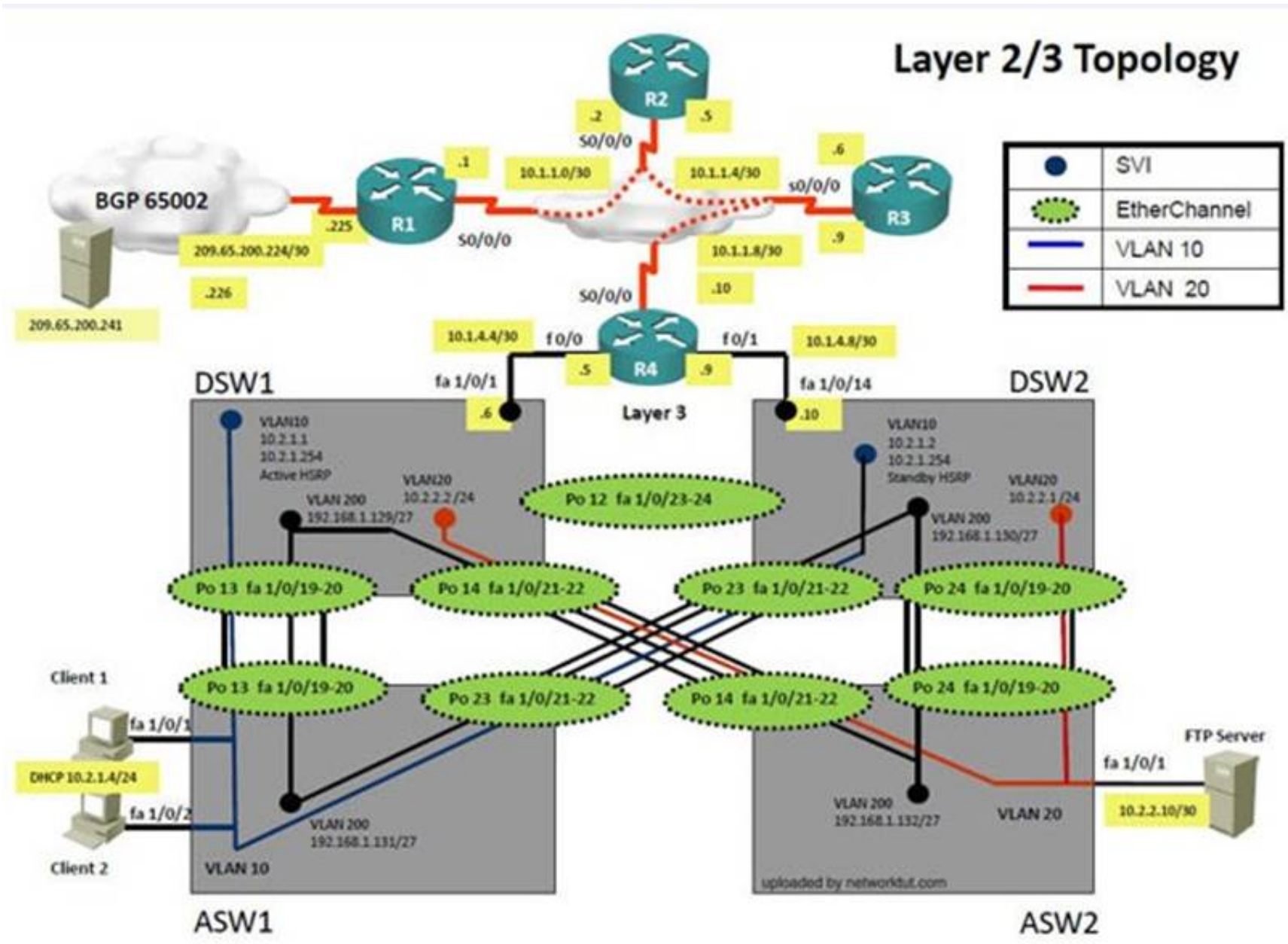
Answer: C

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.

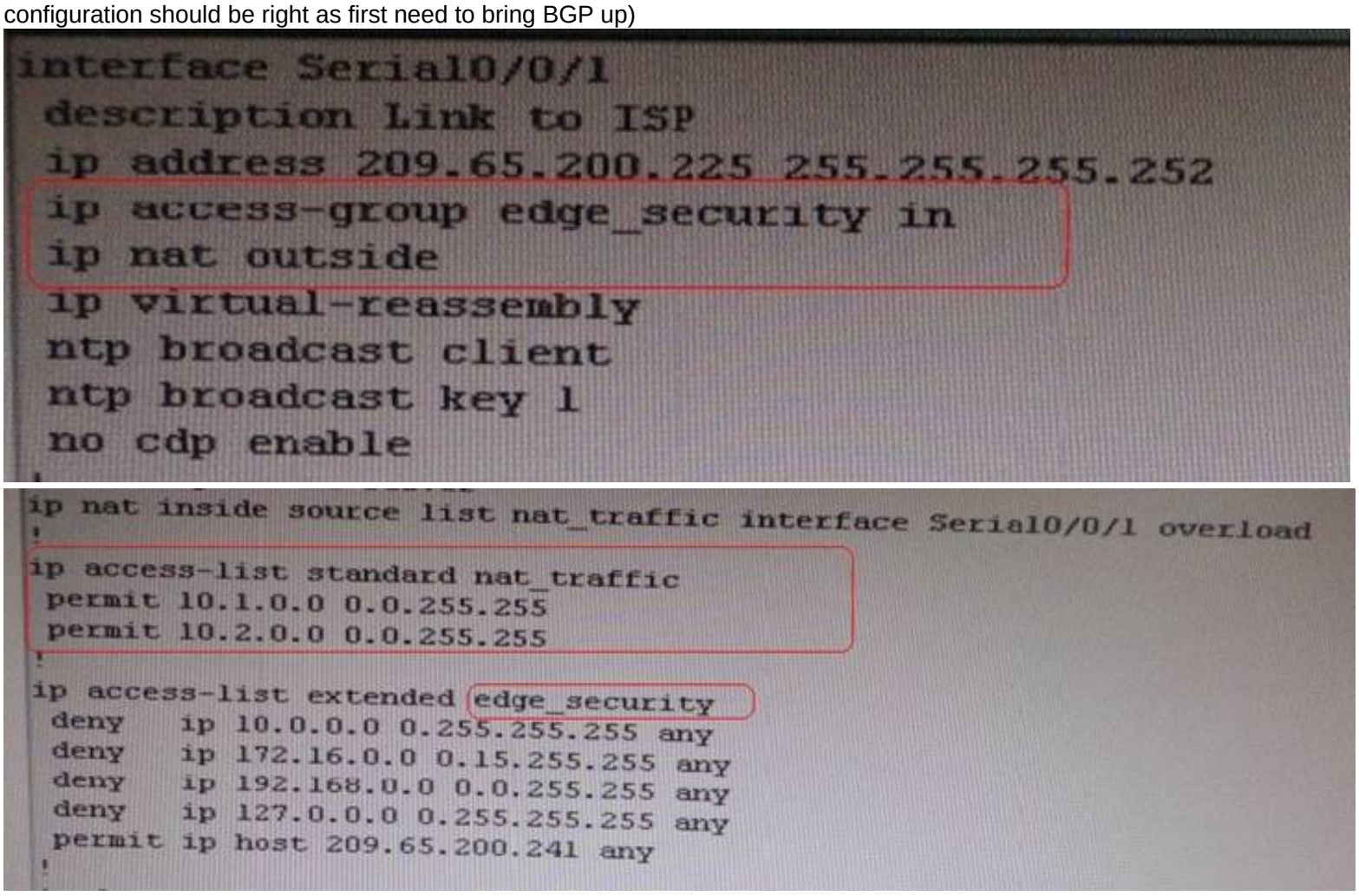
Topic 11, Ticket 6 : R1 ACL
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 is configured 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. Redistribution 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 ----- State of BGP will be in active state. This means connectivity issue between serial
Check for running config. i.e sh run --- over here check for access-list configured on interface as BGP is down (No need to check for NAT configuration as its configuration should be right as first need to bring BGP up)



In above snapshot we can see that access-list of edge_security on R1 is not allowing wan IP network
Change required: On R1, we need to permit IP 209.65.200.222/30 under the access list.

NEW QUESTION 109
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 111
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

Answer: A

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

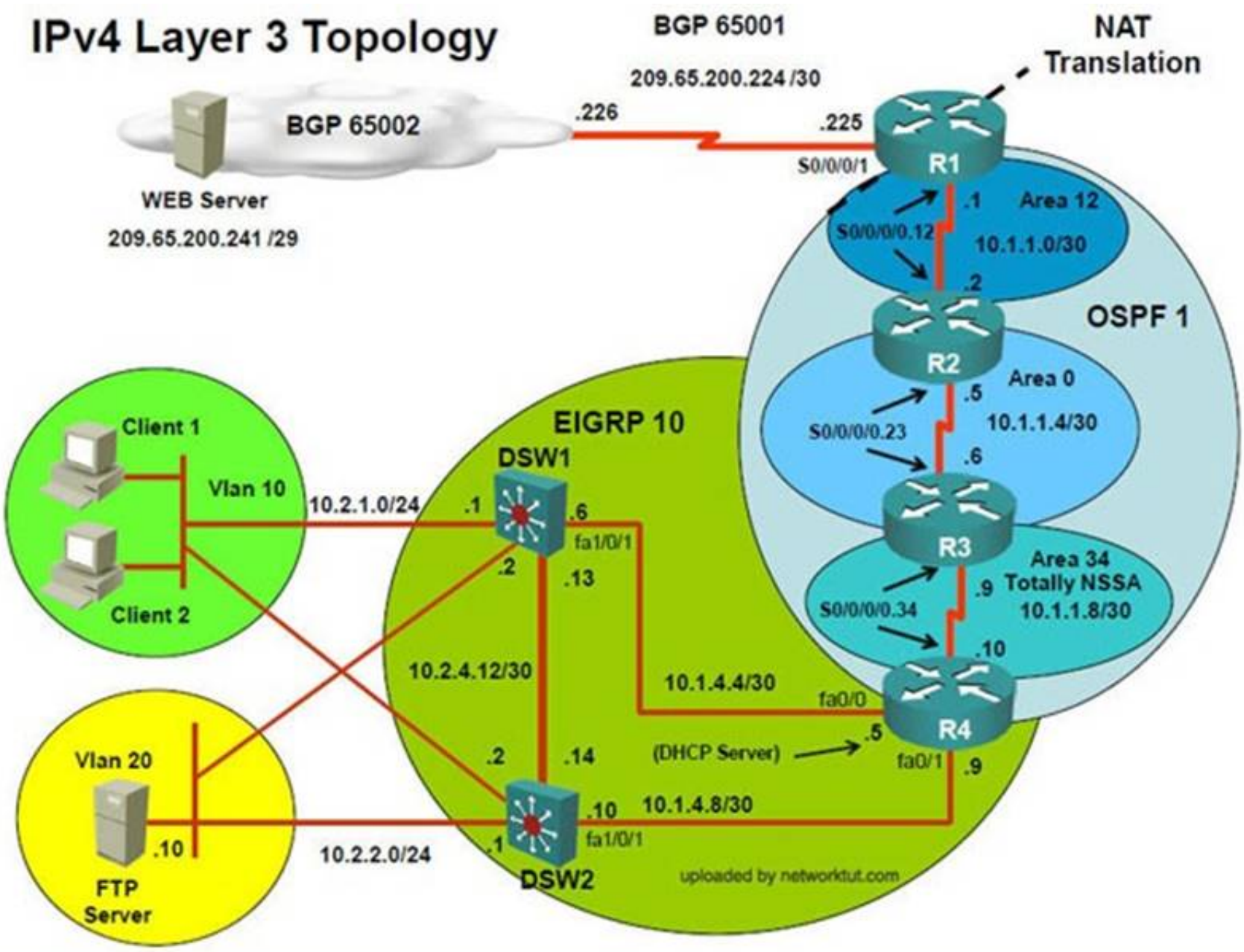
NEW QUESTION 115
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP 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?

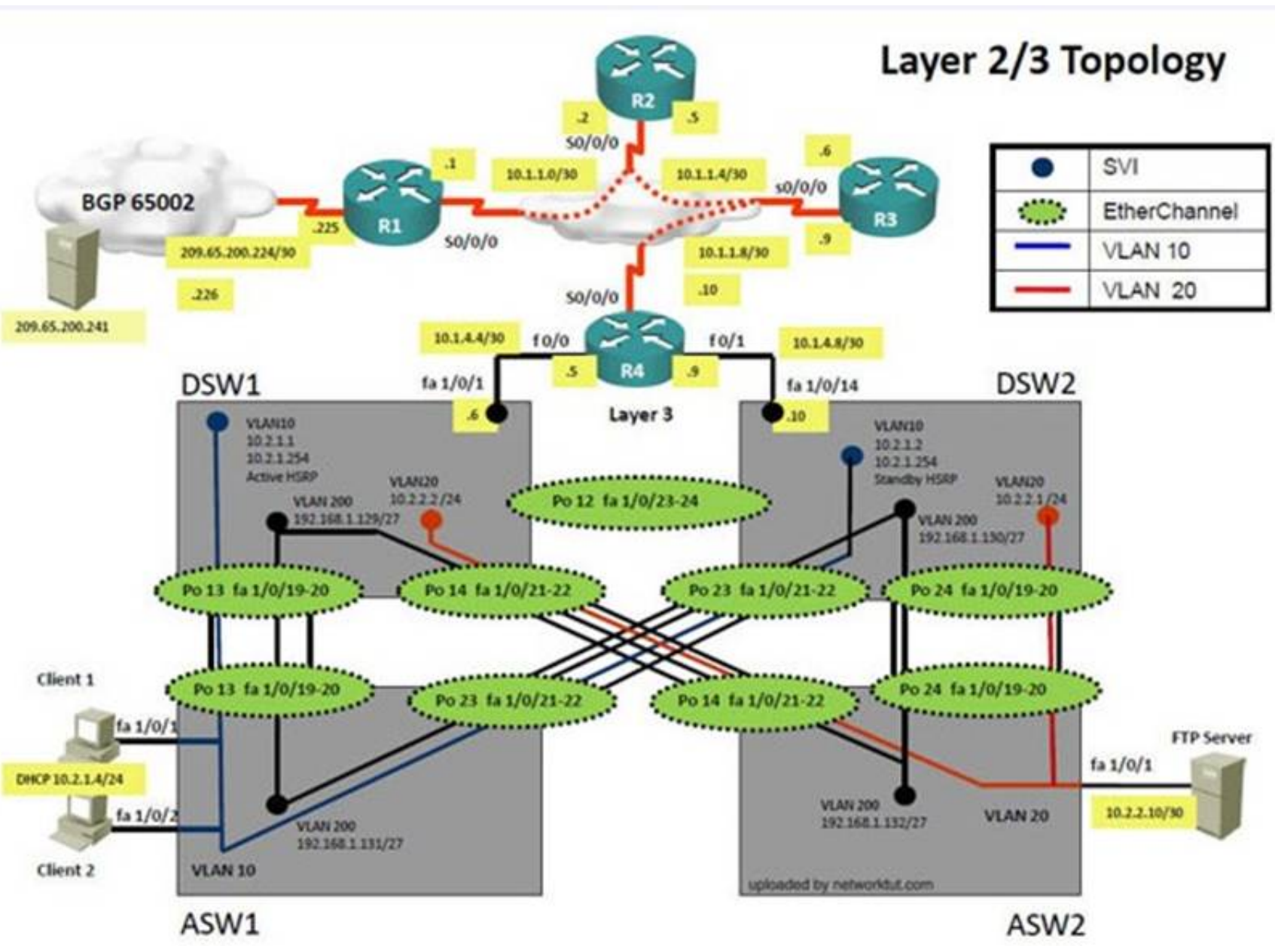
A. Under the interface Serial0/0/1 enter the ip access-group edge_security out command.
B. Under the ip access-list extended edge_security configuration add the permit ip 209.65.200.224 0.0.0.3 any command.
C. Under the ip access-list extended edge_security configuration delete the deny ip 10.0.0.0.0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

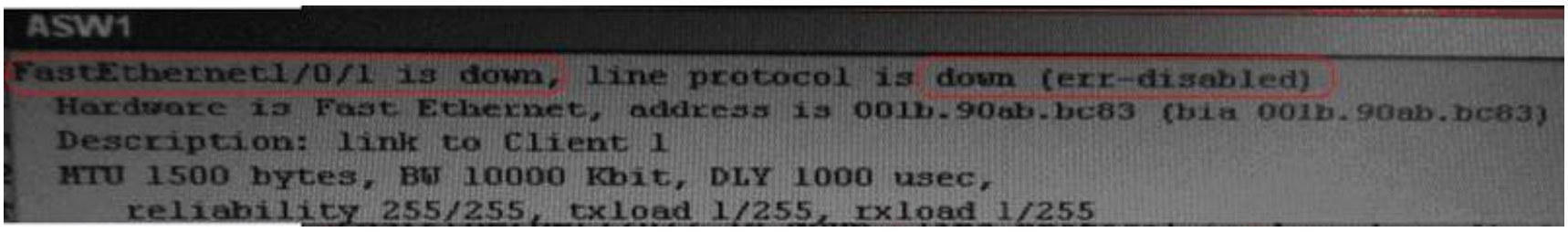
Explanation: On R1, we need to permit IP 209.65.200.222/30 under the access list.

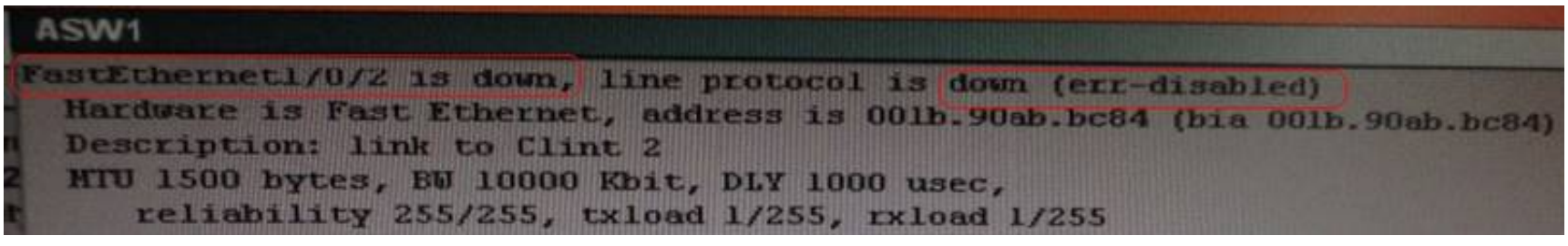
Topic 12, Ticket 7 : Port Security
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 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 116
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 121
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?

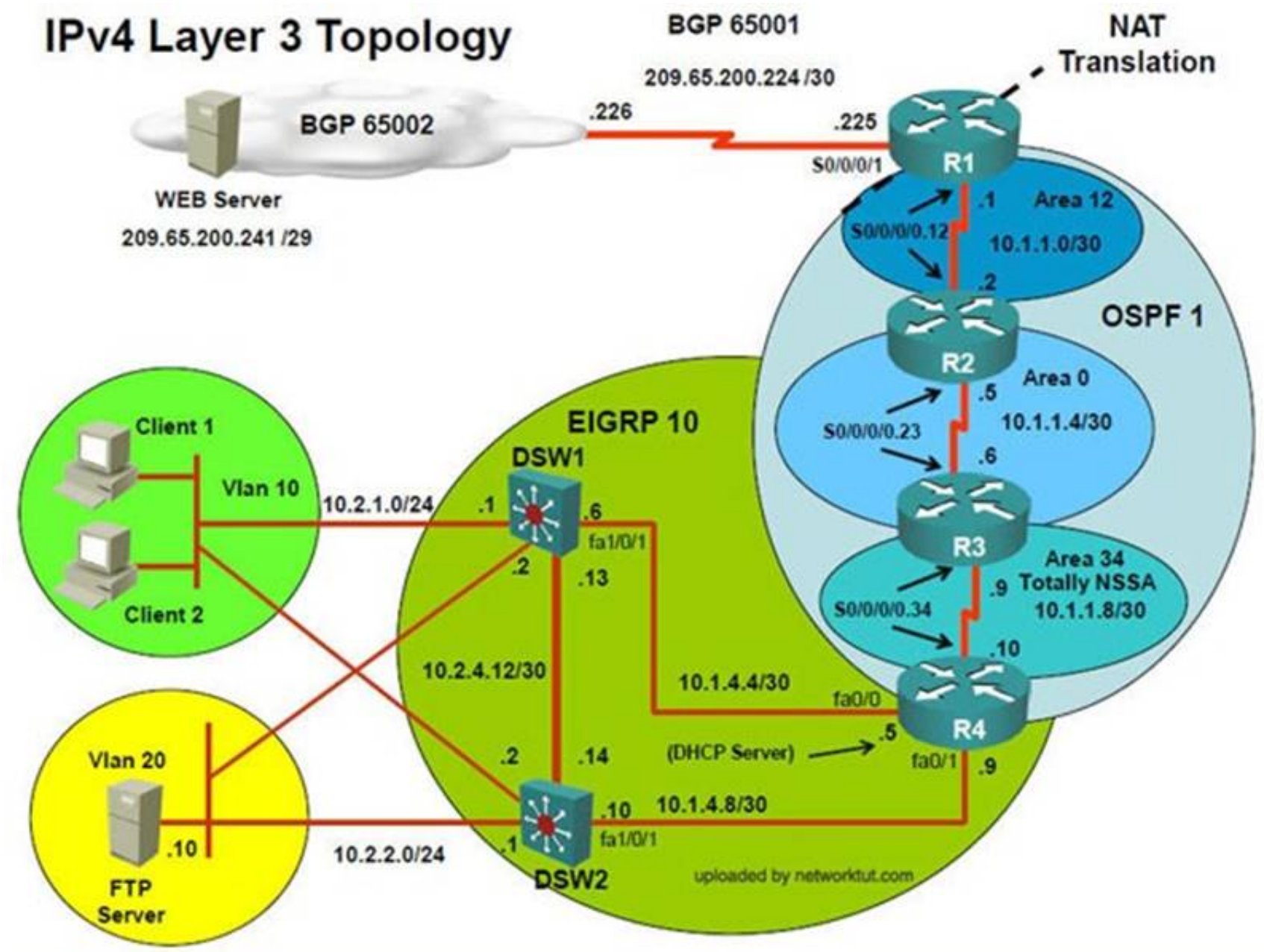
A. NTP
B. Switch-to-Switch Connectivity
C. Access Vlans
D. Port Security
E. VLAN ACL / Port ACL
F. Switch Virtual Interface

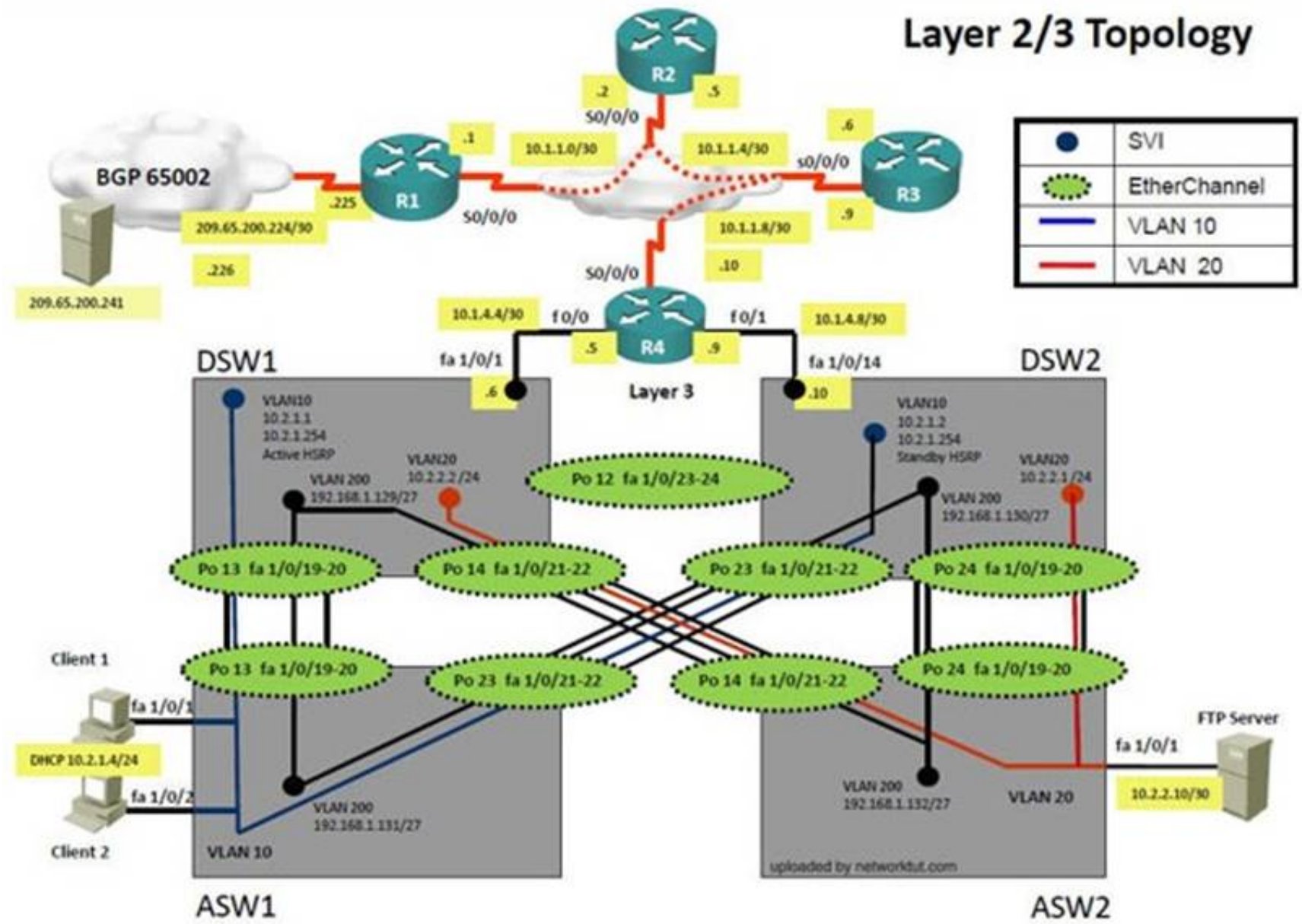
Answer: D

Explanation: Port security is causing the connectivity issues. On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2.

Topic 13, Ticket 8 : Redistribution of EIGRP to OSPF
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

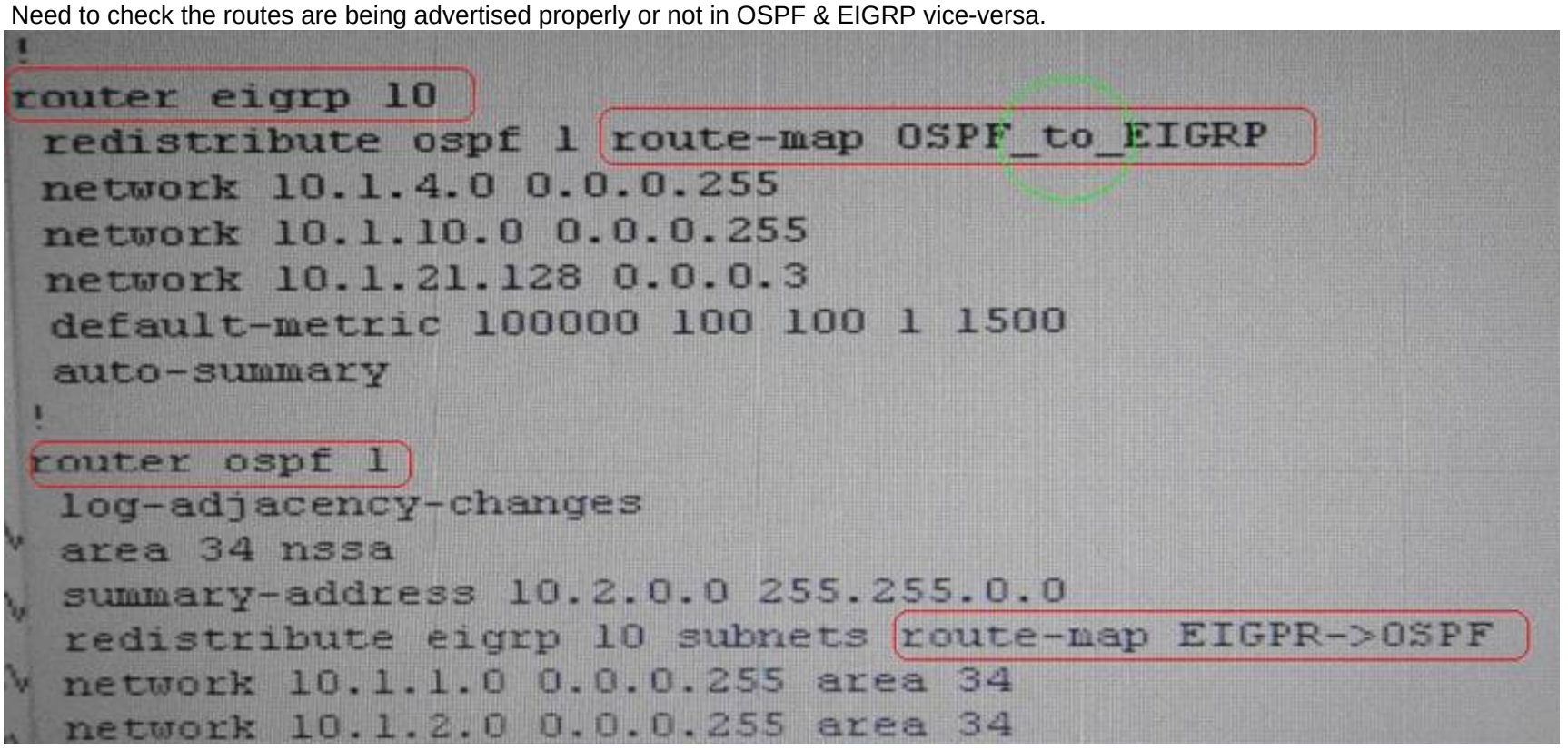
necessary.
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.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

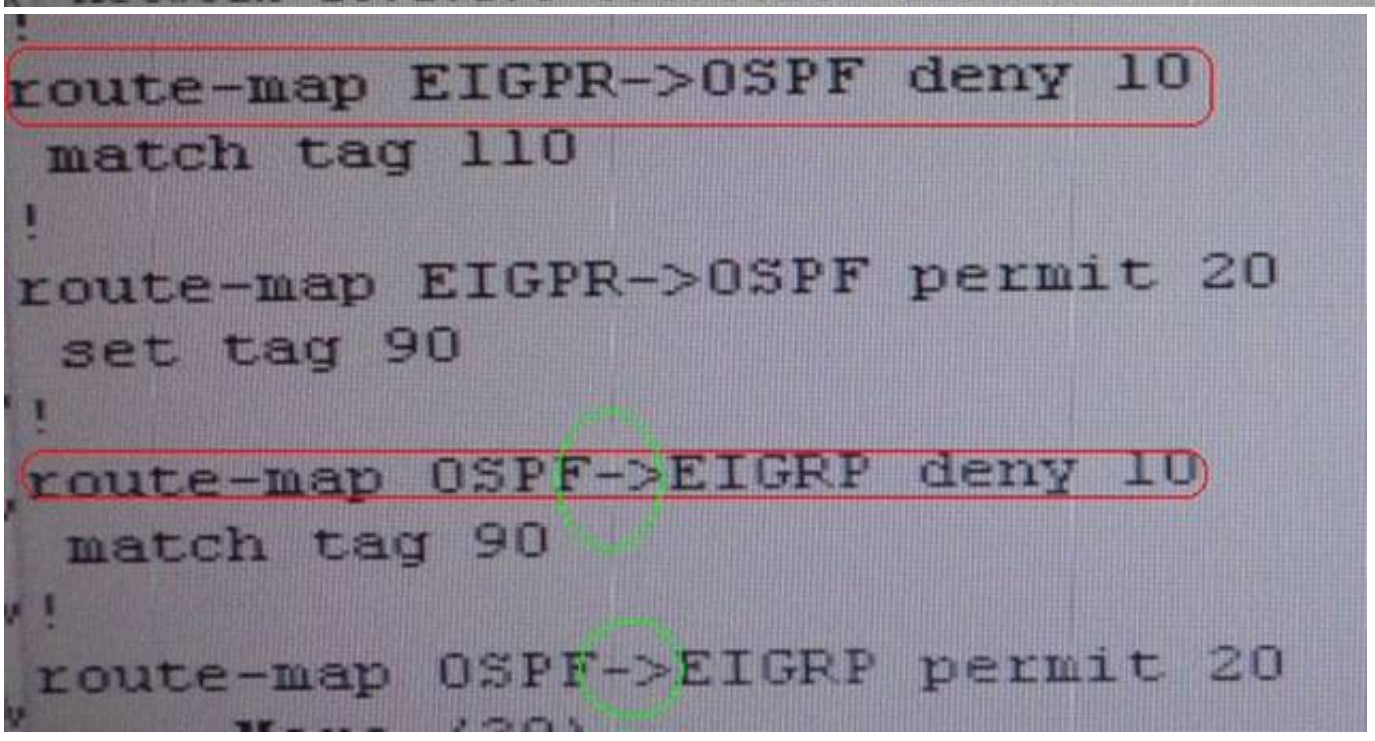




Client is unable to ping IP 209.65.200.241

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 , but cannot ping from R3, R2, R1
This clearly shows problem at R4 since EIGRP is between DSW1, DSW2 & R4 and OSPF protocol is running between R4, R3, R2, R1 so routes from R4 are not propagated to R3, R2, R1
Since R4 is able to ping 10.2.1.3 it means that routes are received in EIGRP & same needs to be advertised in OSPF to ping from R3, R2, R1.
Need to check the routes are being advertised properly or not in OSPF & EIGRP vice-versa.





From above snap shot it clearly indicates that redistribution done in EIGRP is having problem & by default all routes are denied from ospf to EIGRP… so need to change route-map name.
Change required: 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 125
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 127
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

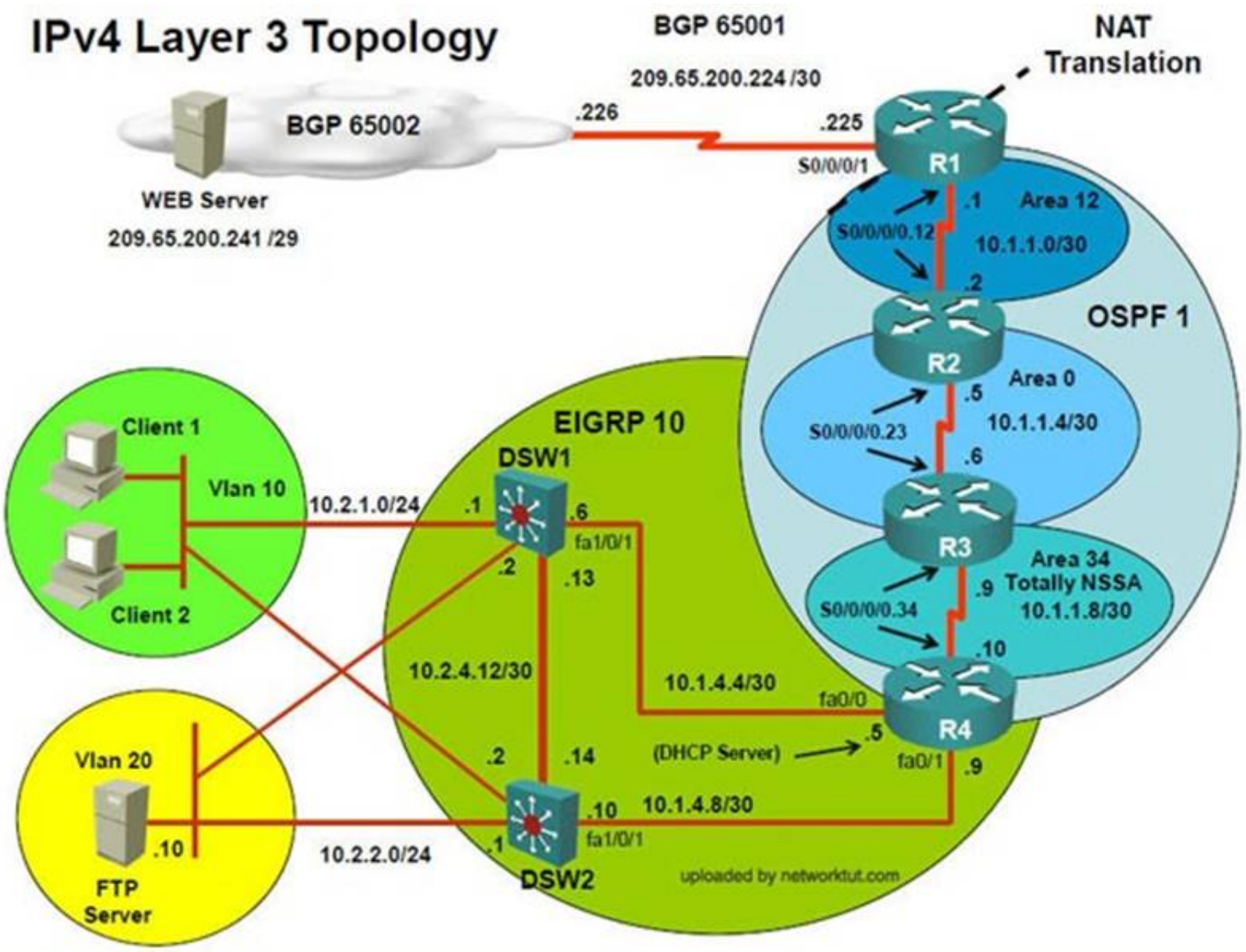
209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated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

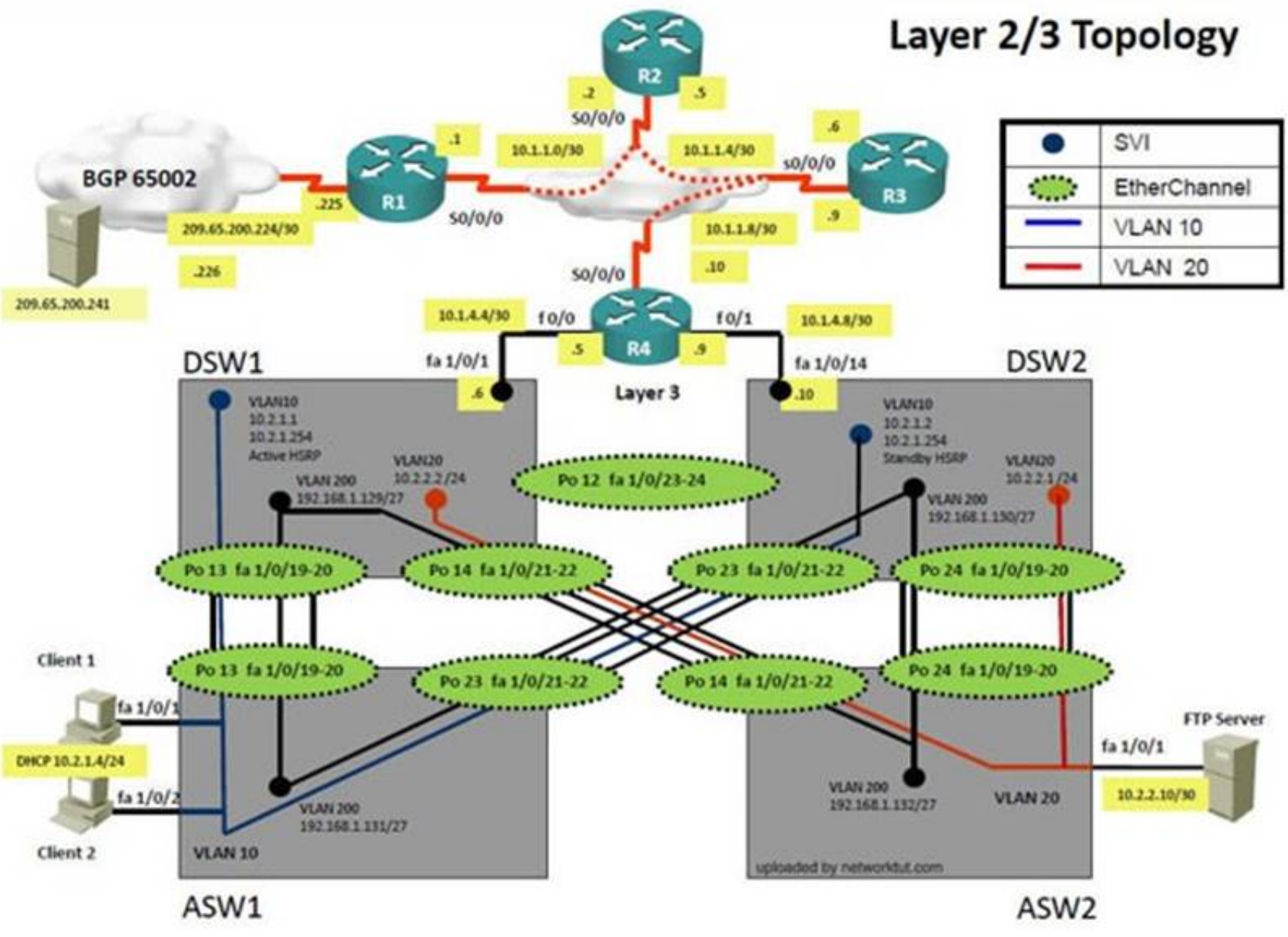
A. NTP
B. IP DHCP Server
C. IPv4 OSPF Routing
D. IPv4 EIGRP Routing
E. IPv4 Route Redistribution
F. IPv6 RIP Routing
G. IPv6 OSPF Routing
H. IPv4 and IPv6 Interoperability
I. IPv4 layer 3 security

Answer: D

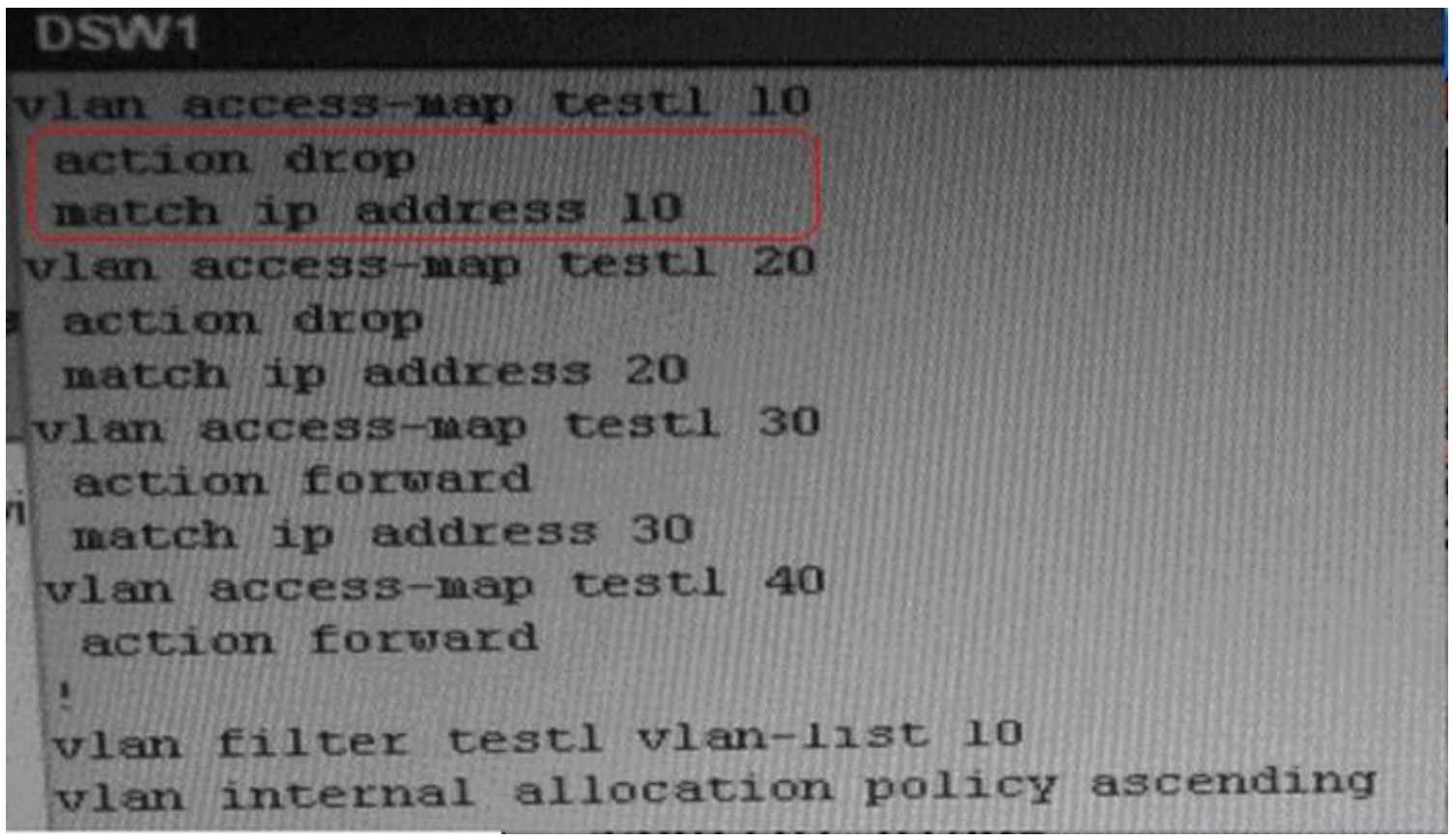
Explanation: On R4, IPV4 EIGRP Routing, need to change the EIGRP AS number from 1 to 10 since DSW1 & DSW2 is configured to be in EIGRP AS number 10.

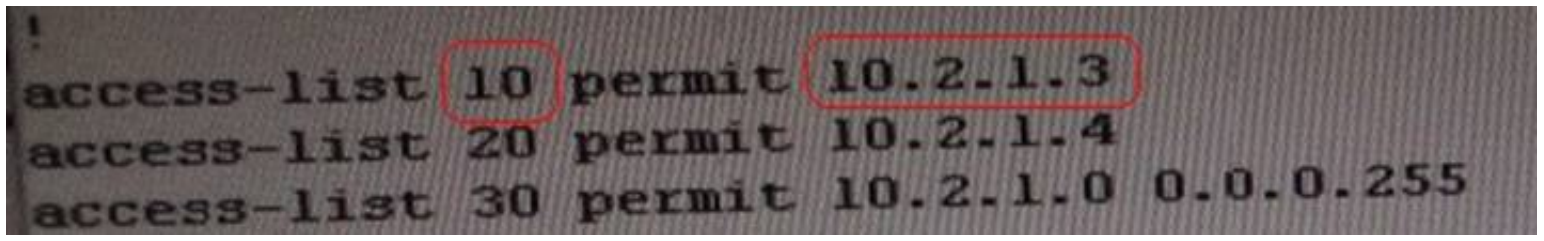
Topic 15, Ticket 10 : VLAN Access Map
Topology Overview (Actual Troubleshooting lab design is for below network design)
Client Should have IP 10.2.1.3
EIGRP 100 is running between switch DSW1 & DSW2
OSPF (Process ID 1) is running between R1, R2, R3, R4
Network of OSPF is redistributed in EIGRP
BGP 65001 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 128
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 133
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 136

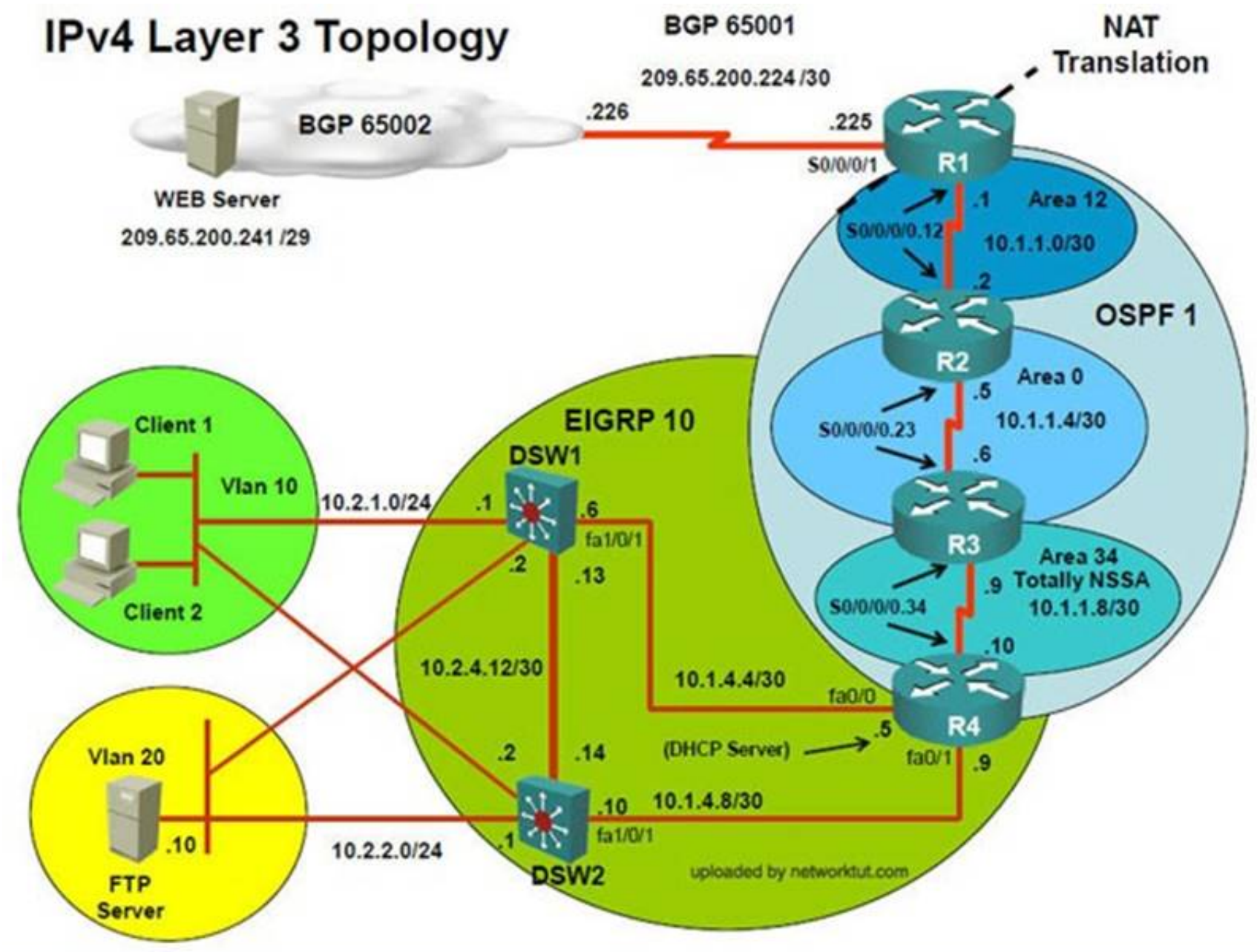
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and 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?

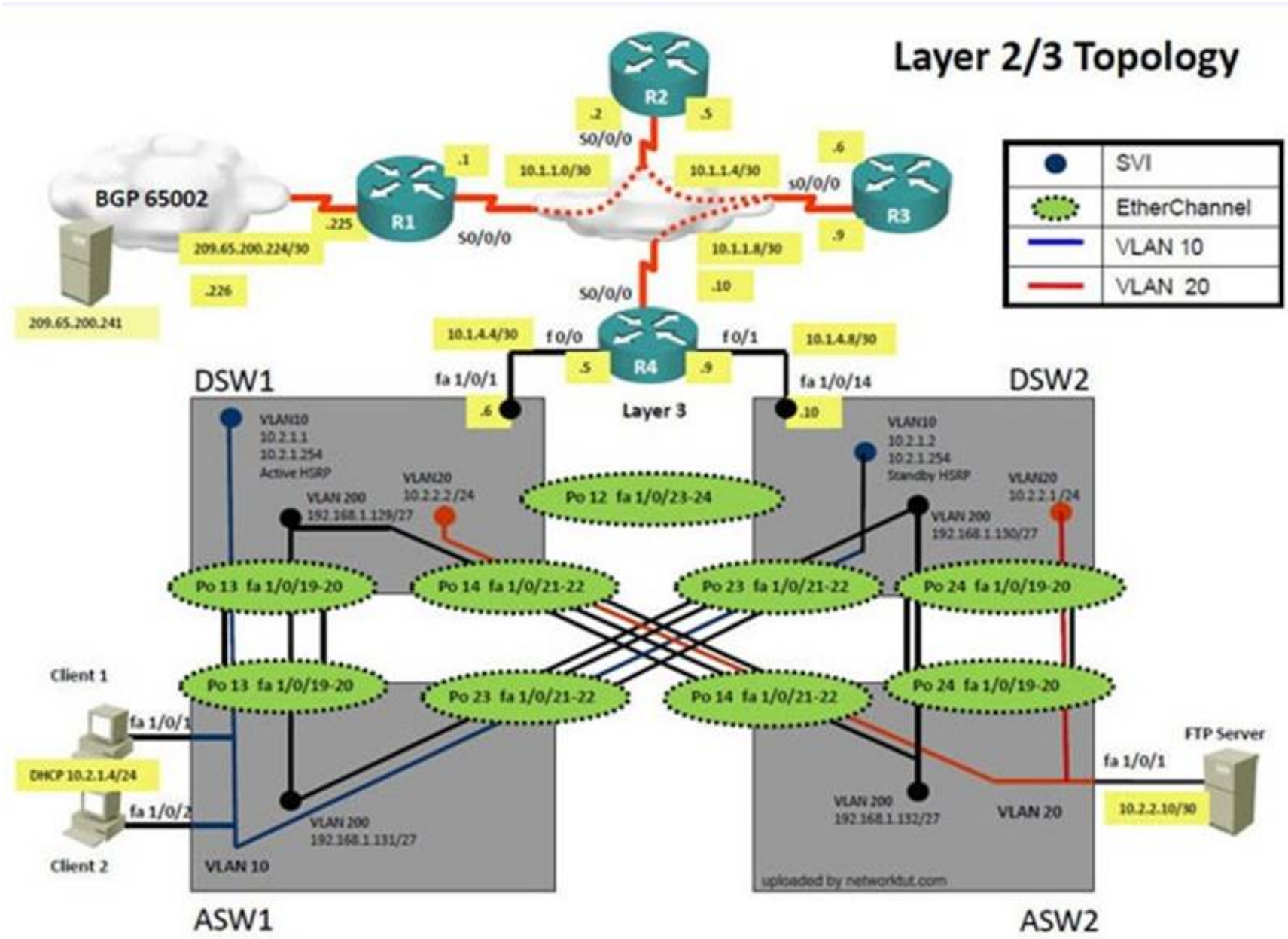
A. Under the global configuration mode enter no access-list 10 command.
B. Under the global configuration mode enter no access-map vlan 10 command.
C. Under the global configuration mode enter no vlan access-map test1 10 command.
D. Under the global configuration mode enter no vlan filter test1 vlan-list 10 command.

Answer: C

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

Topic 16, Ticket 11 : IPV6 OSPF
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 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).

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 able to ping from R4, R3, R2, R1.

Since the problem is R1 (2026::111:1) is not able to ping loopback of DSW1 (2026::102:1).

Kindly check for neighbourship of routers as IPV6…. As per design below neighbourship should be present for IPV6

R1 ---R2 --- R3 --- R4--- DSW1 & DSW2 ----- Neighbourship between devices of IPV6

```
R2#sh ipv6 ospf nei

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.1.10.1         1   FULL/  -        00:00:32    6               Serial0/0/0.12
R2#
```

R2 IPV6 OSPF neighbourship is with R1

```
R3>sh ipv6 ospf ne
R3>sh ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.1.21.129       1   FULL/  -        00:00:31    15              Tunnel34
R3>
```

R3 IPV6 OSPF neighbourship is with R4

```
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 Serial0/0/0.23 point-to-point
 ip address 10.1.1.6 255.255.255.252
 ipv6 address 2026::1:2/122
 ipv6 ospf 6 area 0
 frame-relay interface-dlci 203
!
```

As per above snapshot we cannot see IPV6 neighbourship between R2 & R3 when checked interface configuration ipv6 ospf area 0 is missing on R2 which is connected to R3

Change required: On R2, IPV6 OSPF routing, Configuration is required to add ipv6 ospf 6 area 0 under interface serial 0/0/0.23

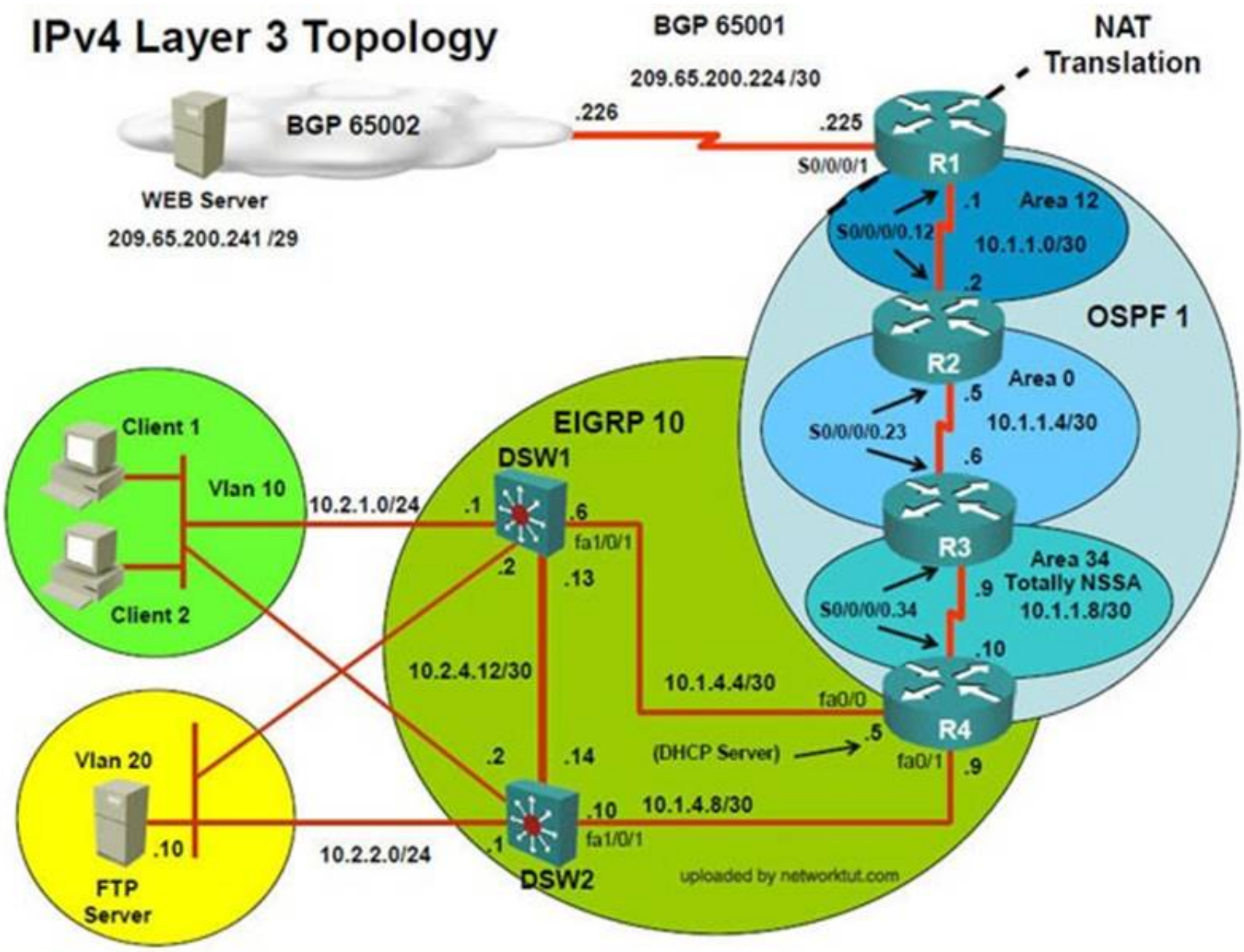
NEW QUESTION 137
The implementations group has been using the test bed to do a ‘proof-of-concept’. After several changes to the network addressing, routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2(2026::102:1).
Use the supported commands to isolated the cause of this fault and answer the following questions. The fault condition is related to which technology?

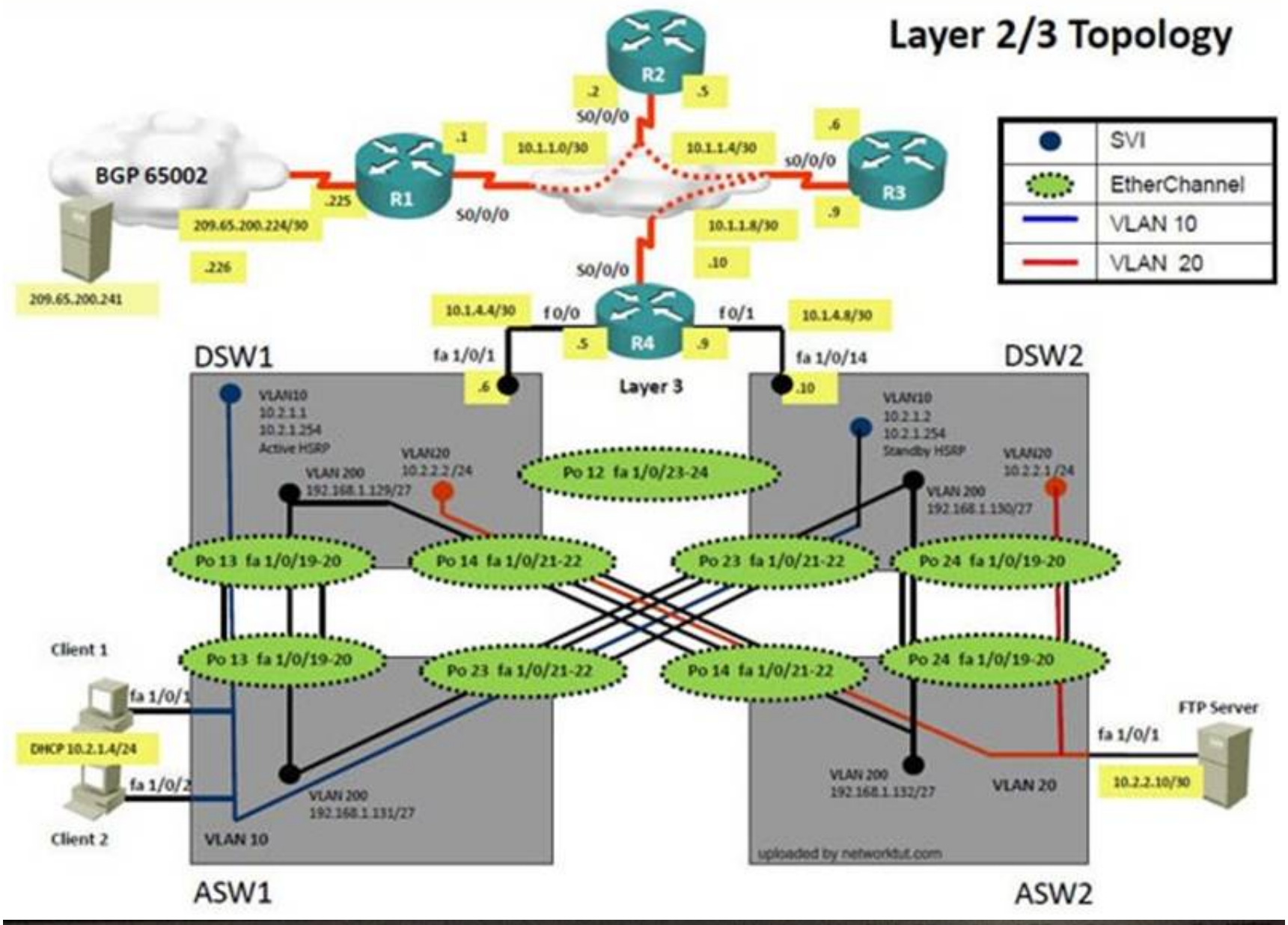
A. NTP
B. IPv4 OSPF Routing
C. IPv6 OSPF Routing
D. IPv4 layer 3 security

Answer: C

Explanation: On R2, IPV6 OSPF routing, configuration is required to add ipv6 ospf 6 area 0 under interface serial 0/0/0.23

Topic 17, Ticket 12 : HSRP 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
==========





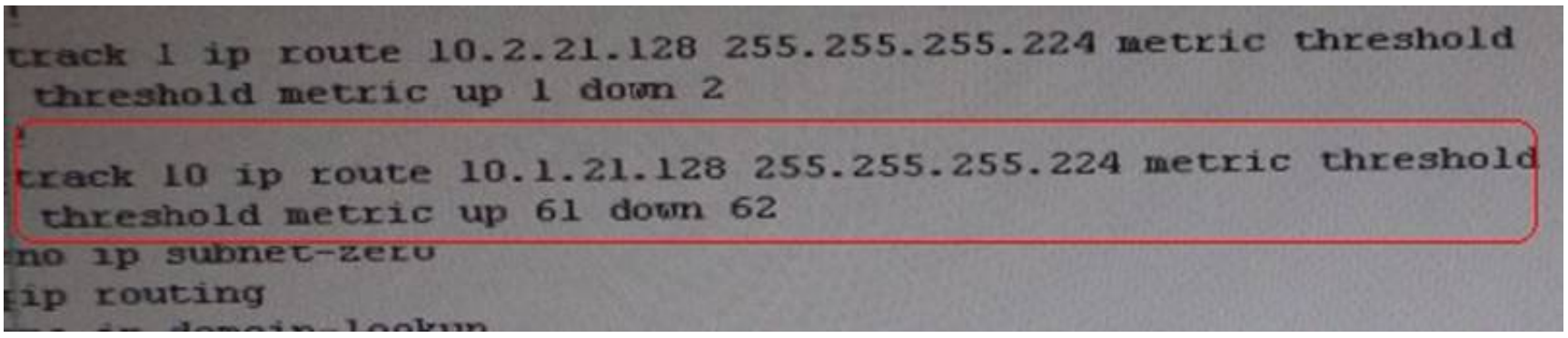
The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and,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

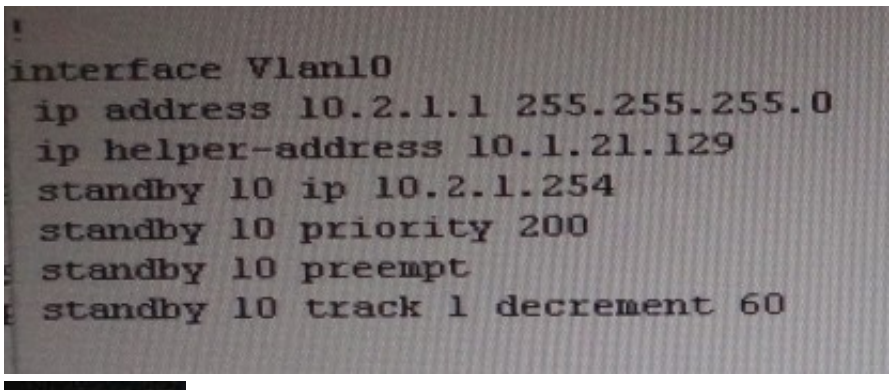
Solution

Steps need to follow as below:-

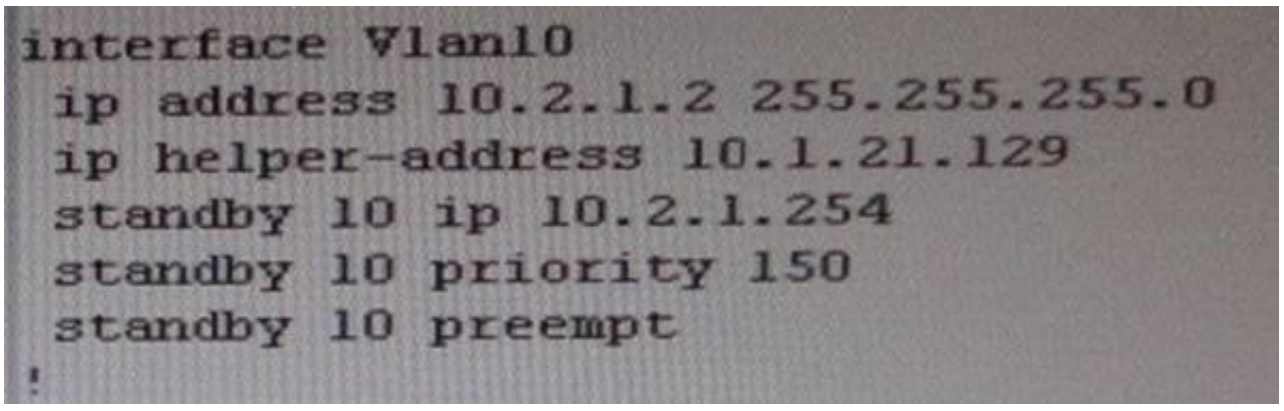
Since the problem is raised that DSW1 will not become active router for HSRP group 10 we will check for the HSRP configuration…

DSW1





DSW2



From snapshot we see that the track command given needs to be changed under active VLAN10 router
Change Required: On DSW1, related to HSRP, under vlan 10 change the given track 1 command to instead use the track 10 command.

NEW QUESTION 140
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. 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: DSW references the wrong track ID number.

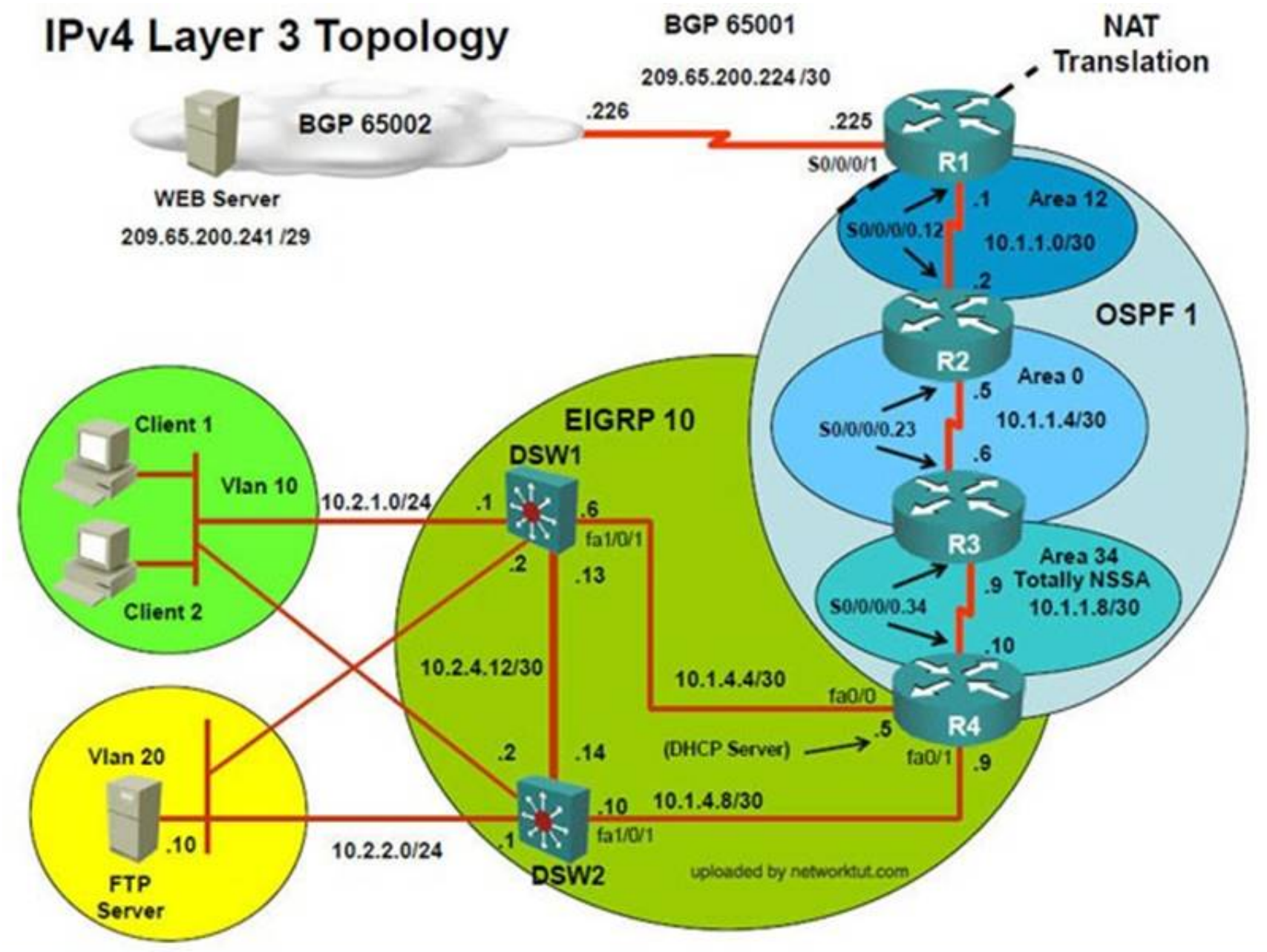
NEW QUESTION 142
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network
addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP 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?

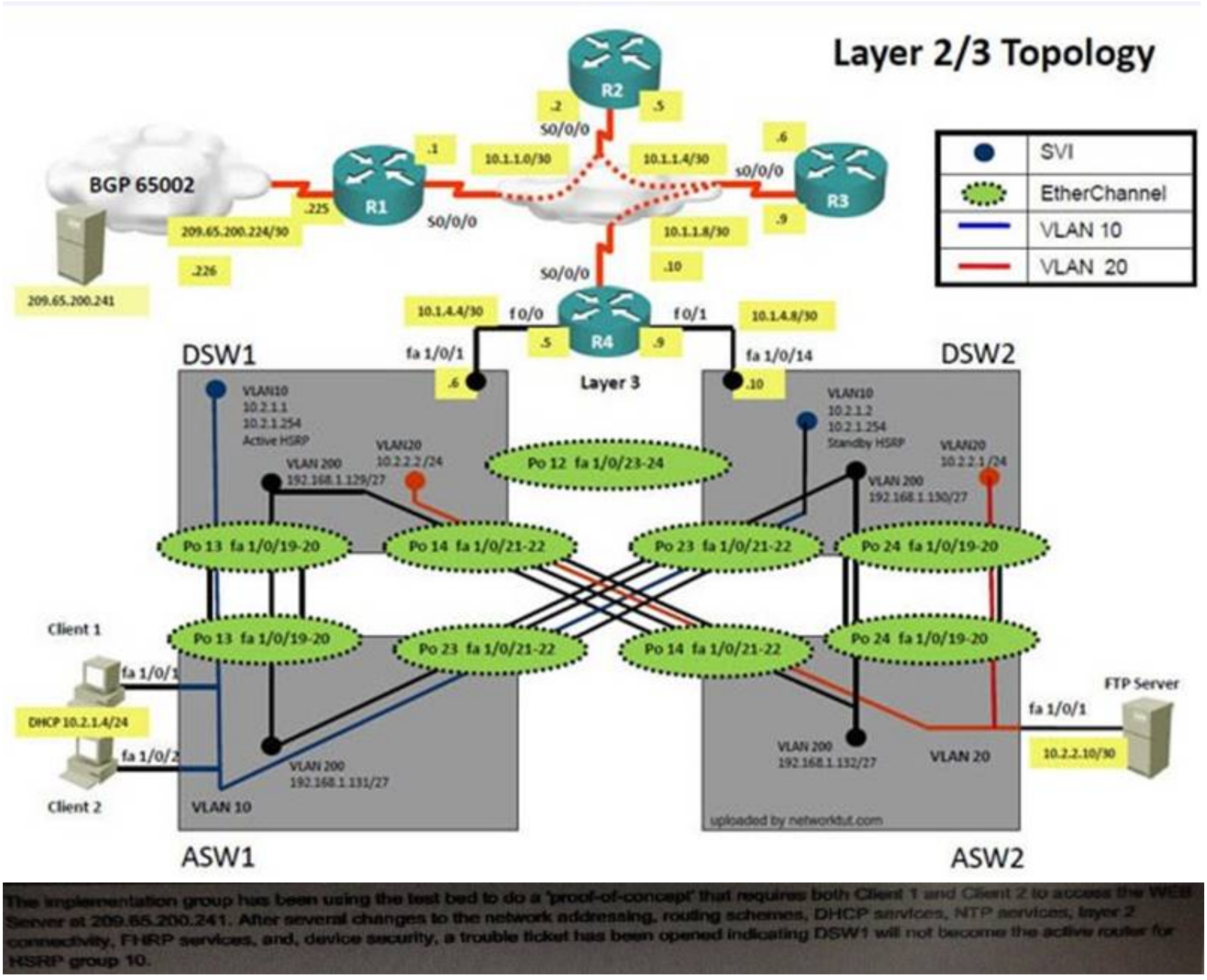
A. NTP
B. HSRP
C. IP DHCP Helper
D. IPv4 EIGRP Routing
E. IPv6 RIP Routing
F. IPv4 layer 3 security
G. Switch-to-Switch Connectivity
H. Loop Prevention
I. Access Vlans
J. Port Security
K. VLAN ACL/Port ACL
L. Switch Virtual Interface

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 143
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. 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 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 144
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?

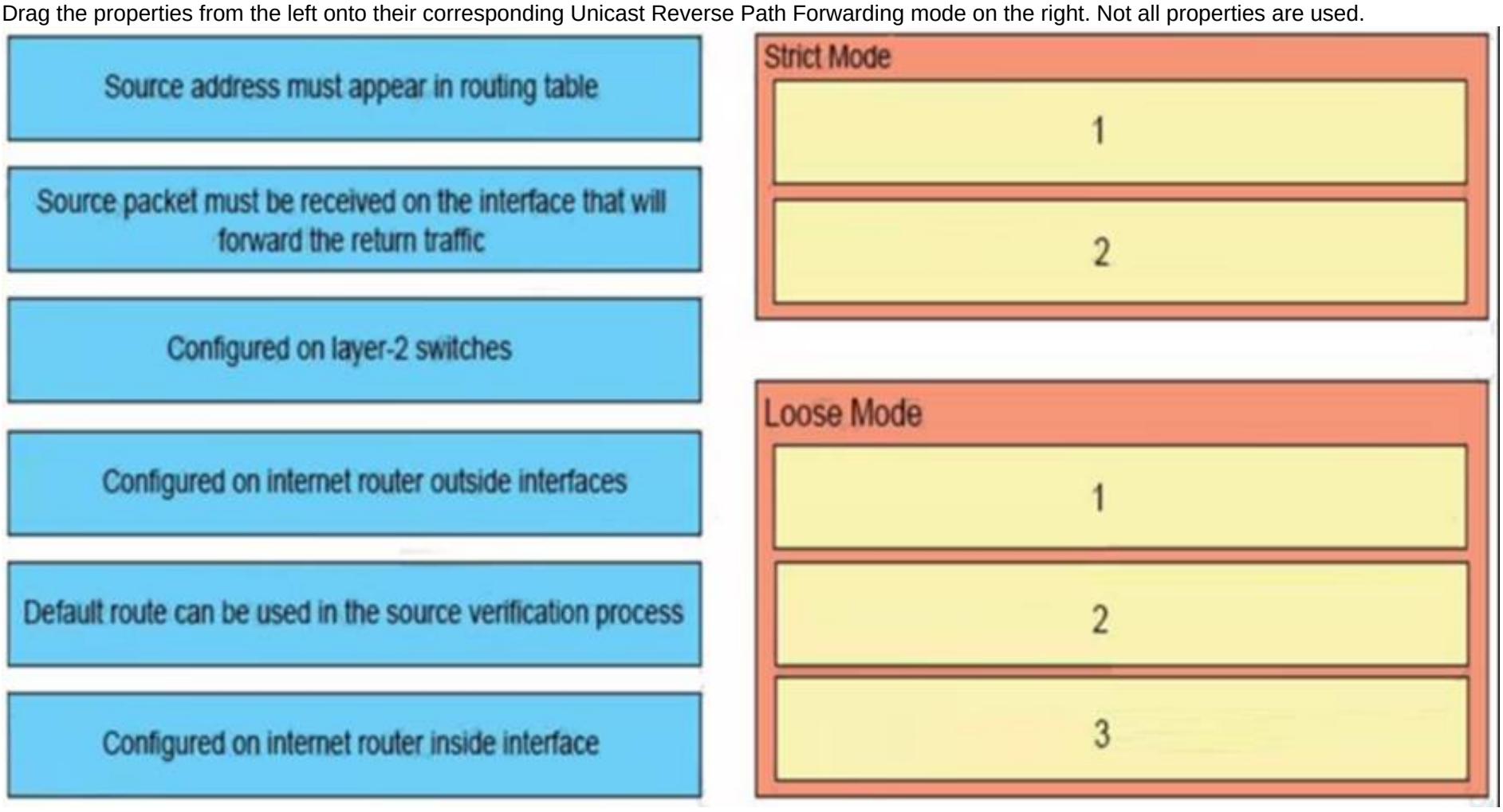
A. NTP
B. IP DHCP Server
C. Ipv4 OSPF Routing
D. Ipv4 EIGRP Routing.
E. Ipv4 Route Redistribution.
F. Ipv6 RIP Routing

G. Ipv6 OSPF Routing
H. Ipv4 and Ipv6 Interoperability
I. Ipv4 layer 3 security.

Answer: B

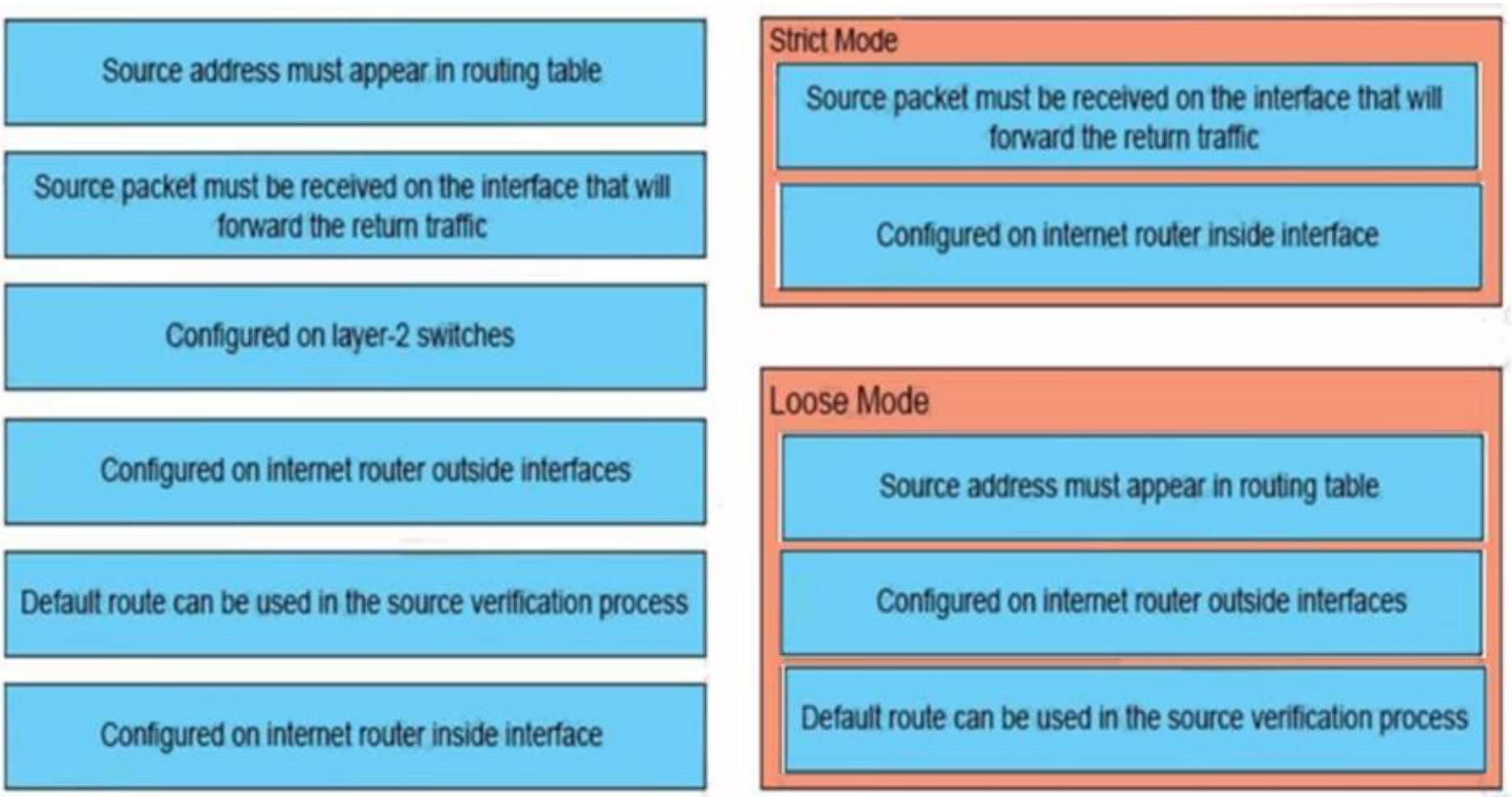
Explanation: On R4 the DHCP IP address is not allowed for network 10.2.1.0/24 which clearly shows the problem lies on R4 & the problem is with DHCP

NEW QUESTION 146
Drag the properties from the left onto their corresponding Unicast Reverse Path Forwarding mode on the right. Not all properties are used.

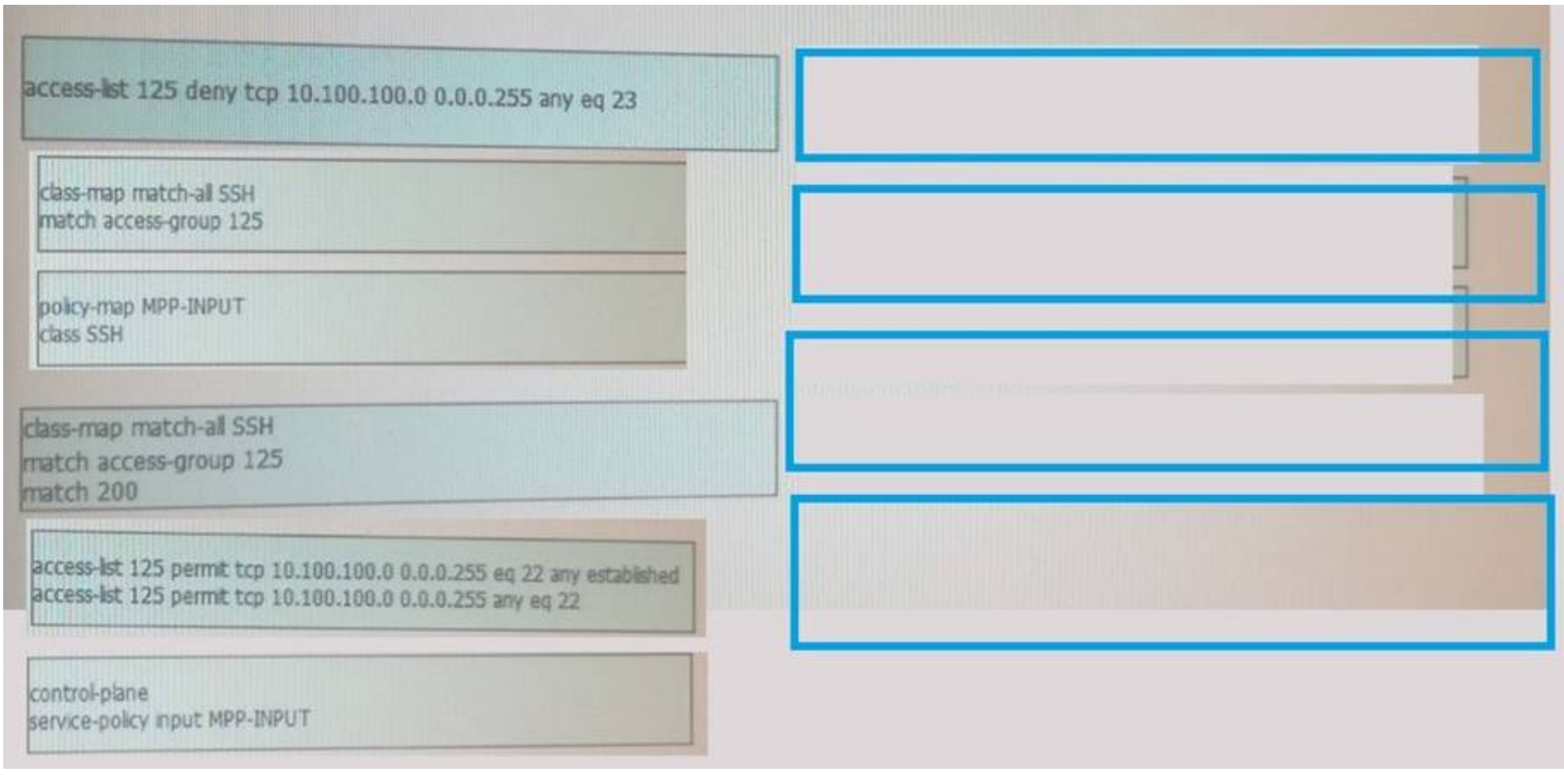


Answer:

Explanation:

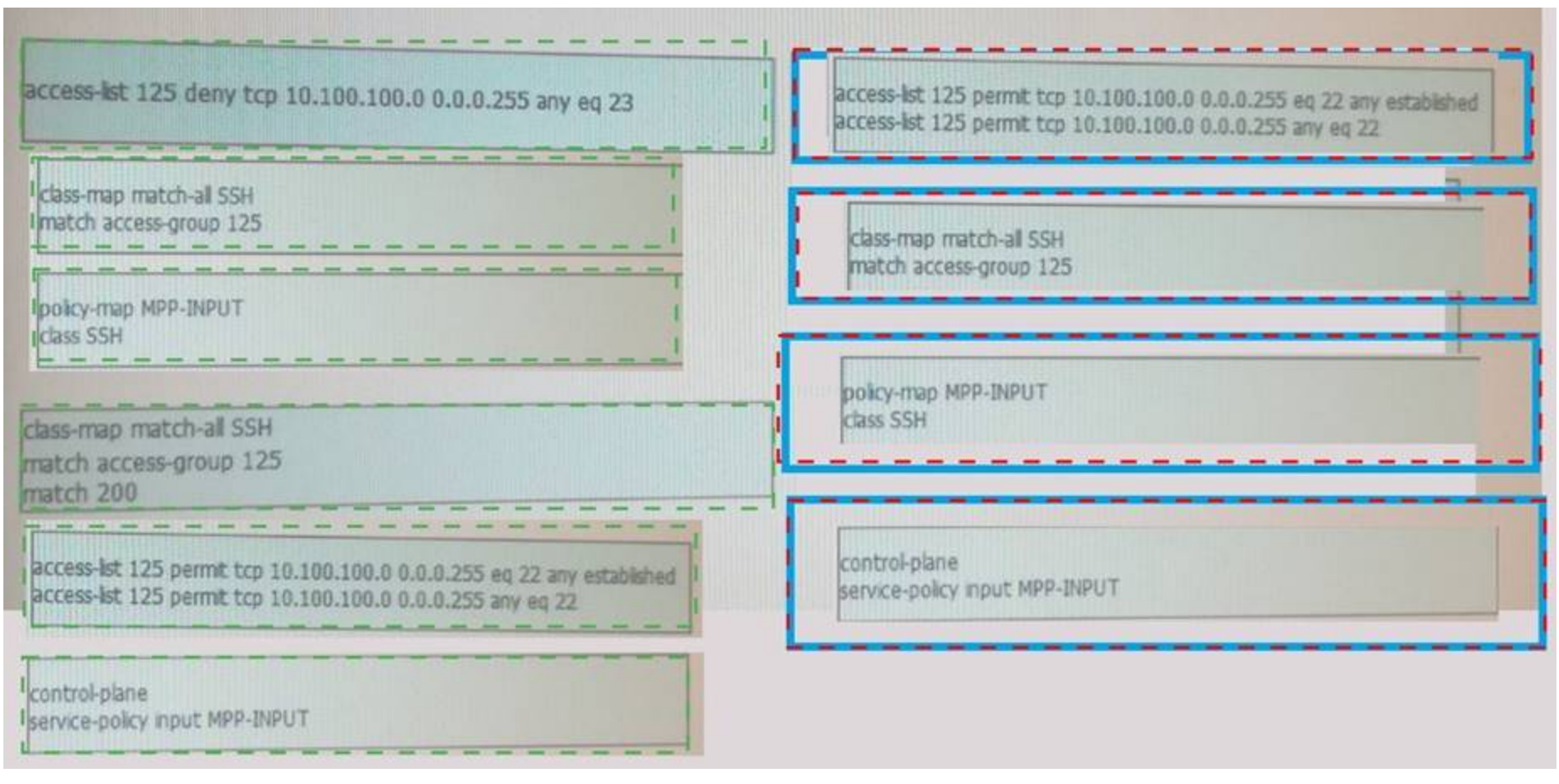


NEW QUESTION 149
You are configuring Management Plane Protection on R1, which connects to the 10.100.100.0/24 network using SSH. Drag and drop the required commands or command sequences from the left into the correct sequence on the right.



Answer:

Explanation:



NEW QUESTION 153
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: D

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 diagram, we see that R4 is redistributing the OSPF and RIP IPV6 routes. However, looking at the routing table we see that R4 has the 2026::102 network in the routing table known via RIP, but that R3 does not have the route:
Screen Shot 2015-03-11 at 4

```
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2026::1:0/122 [110/11175]
     via FE80::21B:2AFF:FE48:A130, Tunnel34
OI  2026::1:0/123 [110/11239]
     via FE80::21B:2AFF:FE48:A130, Tunnel34
C   2026::2:0/122 [0/0]
     via ::, FastEthernet0/0
L   2026::2:1/128 [0/0]
     via ::, FastEthernet0/0
R   2026::3:0/122 [120/2]
     via FE80::21B:8FFF:FEB8:2A41, FastEthernet0/0
OI  2026::12:0/122 [110/11239]
     via FE80::21B:2AFF:FE48:A130, Tunnel34
C   2026::34:0/122 [0/0]
     via ::, Tunnel34
L   2026::34:2/128 [0/0]
     via ::, Tunnel34
R   2026::101:0/122 [120/2]
     via FE80::21B:8FFF:FEB8:2A41, FastEthernet0/0
R   2026::102:0/122 [120/3]
     via FE80::21B:8FFF:FEB8:2A41, FastEthernet0/0
OI  2026::111:0/122 [110/11240]
```

Screen Shot 2015-03-11 at 4

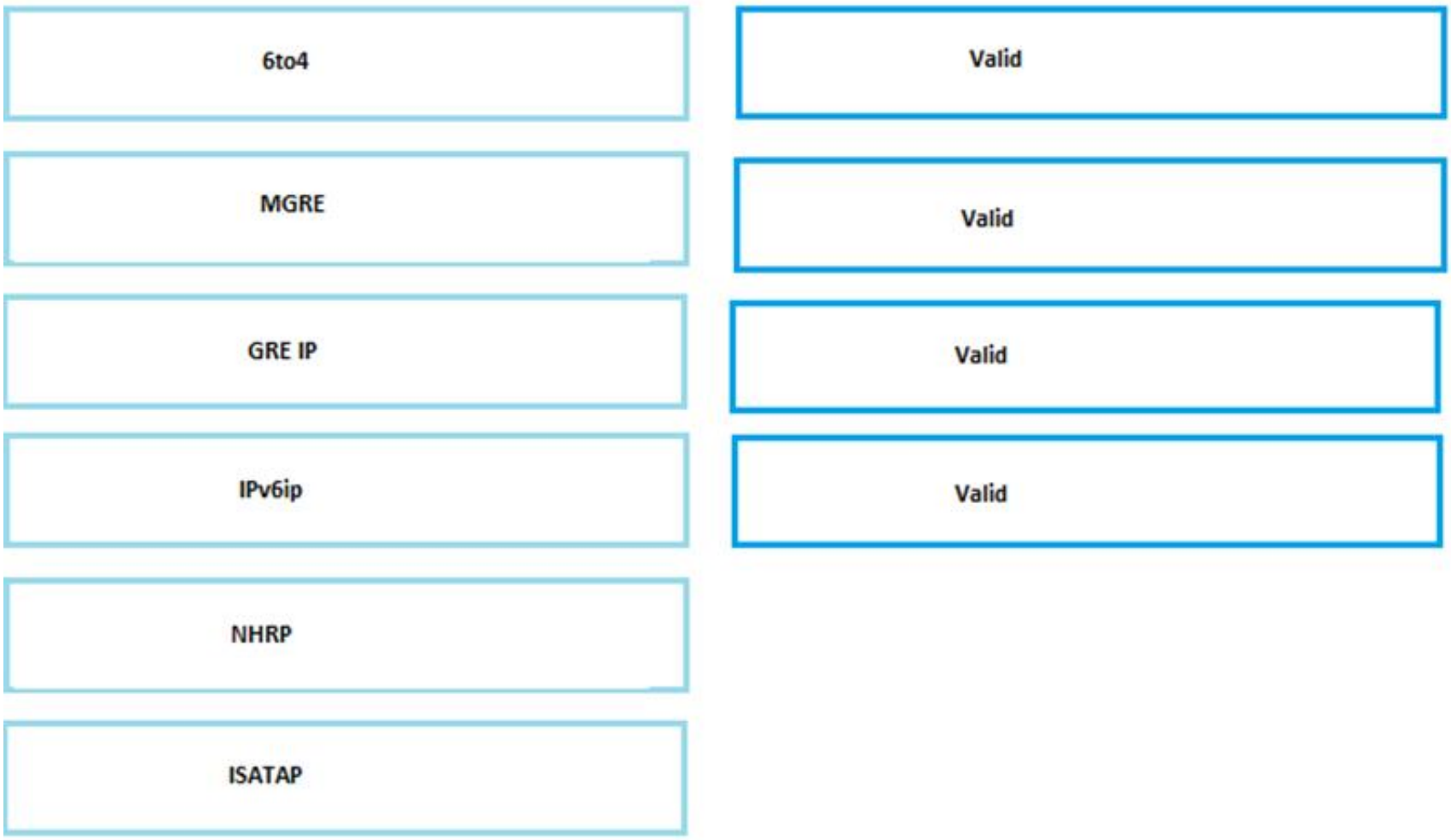
```
R3>show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2026::1:0/122 [0/0]
     via ::, Serial0/0/0.23
O   2026::1:0/123 [110/128]
     via FE80::21B:2AFF:FE48:A0A0, Serial0/0/0.23
L   2026::1:2/128 [0/0]
     via ::, Serial0/0/0.23
OI  2026::12:0/122 [110/128]
     via FE80::21B:2AFF:FE48:A0A0, Serial0/0/0.23
C   2026::34:0/122 [0/0]
     via ::, Tunnel34
L   2026::34:1/128 [0/0]
     via ::, Tunnel34
OI  2026::111:0/122 [110/129]
     via FE80::21B:2AFF:FE48:A0A0, Serial0/0/0.23
OI  2026::222:0/122 [110/65]
     via FE80::21B:2AFF:FE48:A0A0, Serial0/0/0.23
C   2026::333:0/122 [0/0]
```

When we look more closely at the configuration of R4, we see that it is redistributing OSPF routes into RIP for IPv6, but the RIP routes are not being redistributed into OSPF. That is why R3 sees R4 as an IPV6 OSPF neighbor, but does not get the 2026::102 network installed.
Screen Shot 2015-03-11 at 4

```
!
ipv6 router ospf 6
 log-adjacency-changes
!
ipv6 router rip RIP_ZONE
 redistribute ospf 6 metric 2 include-connected
!
!
```

So, problem is with route redistribution on R4.

NEW QUESTION 157
Drag and drop the valid tunnel modes from the left into the Valid Column on the right. Order does not matter and not all options are used.



Answer:

Explanation: 6to4 GRE IP IPV6 IP ISATAP

NEW QUESTION 159
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

R4

```
!
!
!
interface Loopback0
 ip address 10.1.10.3 255.255.255.255
!
interface Loopback1
 ip address 10.1.2.65 255.255.255.224
 ip ospf network point-to-point
!
interface Loopback6
 no ip address
 ipv6 address 2026::333:1/122
 ipv6 ospf network point-to-point
 ipv6 ospf 6 area 0
!
interface Tunnel34
 no ip address
 ipv6 address 2026::34:1/122
 ipv6 ospf 6 area 34
 tunnel mode ipv6
 tunnel source Serial0/0/0.34
 tunnel destination 10.1.1.10
!
```

```
!
!
!
!
interface Loopback0
 ip address 10.1.10.4 255.255.255.255
!
interface Loopback1
 ip address 10.1.21.129 255.255.255.224
 ip ospf network point-to-point
!
interface Loopback6
 no ip address
 ipv6 address 2026::444:1/122
 ipv6 rip RIP_ZONE enable
 ipv6 ospf 6 area 34
!
interface Tunnel34
 no ip address
 ipv6 address 2026::34:2/122
 ipv6 ospf 6 area 34
 tunnel source Serial0/0/0.34
 tunnel destination 10.1.1.9
!
```

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

NEW QUESTION 160
How long will a port remain in the listening state by default?

A. Depends on the number of switches in the spanning tree domain
B. 50 seconds
C. 15 seconds
D. Until the root directs it to start forwarding
E. 20 seconds
F. Depends on the pott speed

Answer: C

NEW QUESTION 165
What level of logging is enabled on a Router where the following logs are seen?
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

A. alerts
B. critical
C. errors
D. notifications

Answer: D

Explanation: Cisco routers, switches, PIX and ASA firewalls prioritize log messages into 8 levels (0-7), as shown below: LevelLevel NameDescription
0 Emergencies System is unusable 1 Alerts Immediate action needed 2 Critical Critical conditions
3 Errors Error conditions
4 Warnings Warning conditions
5 Notifications Informational messages
6 Informational Normal but significant conditions 7 Debugging Debugging messages
When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case we can see that logging level of 3 (as seen by the 3 in “LINK-3-UPDOWN”) and level 5 (as seen by the 5 in “LINEPROTO-5-UPDOWN”) are shown, which means that logging level 5 must have been configured. As shown by the table, logging level 5 is Notifications.

NEW QUESTION 166
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 170
The following command is issued on a Cisco Router: Router(configuration)#logging console warnings Which alerts will be seen on the console?

A. Warnings only
B. debugging, informational, notifications, warnings
C. warnings, errors, critical, alerts, emergencies
D. notifications, warnings, errors
E. warnings, errors, critical, alerts

Answer: C

Explanation: Cisco routers prioritize log messages into 8 levels (0-7), as shown below: LevelLevel NameDescription
0 Emergencies System is unusable 1 Alerts Immediate action needed 2 Critical Critical conditions
3 Errors Error conditions
4 Warnings Warning conditions
5 Notifications Informational messages
6 Informational Normal but significant conditions 7 Debugging Debugging messages
When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case, when you enable console logging of warning messages (level 4), it will log levels 0-4, making the correct answer warnings, errors, critical, alerts, and emergencies.

NEW QUESTION 171
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 175
Which of the following commands will restore a previously archived configuration by replacing the running configuration with the archived configuration?

A. configure archive running-config
B. configure replace
C. copy archive running config
D. copy startup-config running-config
E. copy tftp running-config
F. configure tftp running-config

Answer: B

NEW QUESTION 179
Which of the following is an accurate description of the command copy startup-config
ftp://kevin:cisco@192.168.1.74?

A. The configuration on the FTP server is copied to RAM.
B. The command is not valid on a Cisco router.
C. The configuration file in RAM is copied to an FTP server.
D. The configuration file in NVRAM is copied to an FTP server.
E. The configuration on the FTP server is copied to NVRAM.
F. The configuration will be copied from NVRAM to an FTP server with a filename of Kevin.

Answer: D

NEW QUESTION 182
The following commands are issued on a Cisco Router: Router(configuration)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
Router(configuration)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1 Router(configuration)#exit
Router#debug ip packet 199
What will the debug output on the console show?

A. All IP packets passing through the router
B. Only IP packets with the source address of 10.1.1.1
C. All IP packets from 10.1.1.1 to 172.16.1.1
D. All IP Packets between 10.1.1.1 and 172.16.1.1

Answer: D

Explanation: In this example, the “debug ip packet” command is tied to access list 199, specifying which IP packets should be debugged. Access list 199 contains two lines, one going from the host with IP address 10.1.1.1 to
172.16.1.1 and the other specifying all TCP packets from host 172.16.1.1 to 10.1.1.1.

NEW QUESTION 186
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 190
Which of the following is not an essential prerequisite for AutoQoS to be correctly applied to an interface? (Choose all that apply.)

A. The interface must be configured as a Multilink PPP interface.
B. The correct bandwidth should be configured on the interface.
C. A QoS policy must not be currently attached to the interface.
D. CEF must be enabled.
E. AutoQoS must be enabled globally before it can be enabled on the interface.
F. An IP address must be configured on the interface if its speed is equal to or less than 768 kbps.

Answer: AE

NEW QUESTION 195
Which of the following options represents the correct sequence of DHCP messages after a client initially boots?

A. DHCPREQUEST, DHCPOFFER, DHCPDISCOVER, DHCPACK
B. DHCPDISCOVER, DHCPOFER, DHCPREQUEST, DHCPACK
C. DHCPOFFER, DHCPACK, DHCPREQUEST, DHCPDISCOVER
D. DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK
E. DHCPREQUE5T, DHCPDISCOVER, DHCPOFFER, DHCPACK
F. DHCPDISCOVER, DHCPACK, DHCPREQUEST, DHCPOFFER

Answer: B

NEW QUESTION 200
Several troubleshooters are about to work on the same problem. Which of the following troubleshooting methods would be most appropriate to make the best use of the troubleshooters1 time?

A. Bottom up
B. Component swapping
C. Top down
D. Shoot from the hip
E. Divide and conquer
F. Follow the traffic path

Answer: E

NEW QUESTION 205
Which of the following statements are true concerning the command ip sla monitor responder type tcpconnect ipaddress 10.1.1.1 port 23? (Choose all that apply.)

A. The command will initiate a probe with a destination IP address of 10.1.1.1.
B. The command is used on the IP SLA responder and the IP SLA source.
C. The command will allow only source address 10.1.1.1 to source probes.
D. The command will initiate a probe with a destination Telnet port.
E. The command is used to make the router a responder.

F. The command will initiate a probe with a source port of 23.

Answer: AD

NEW QUESTION 206
A new router is added to an existing HSRP standby group. One of the existing routers is in an active state, the other is in a standby state. Under what circumstance will the new router become the active router?

A. The new router will become active immediately because it's the newest router introduced into the group.
B. The new router can become active only when the existing active router and the existing standby router become unavailable.
C. The new router has a lower priority value.
D. The new router will never become active unless the existing active router becomes unavailable.
E. The new router has preempt configured and a higher priority
F. The new router has a higher priority value.

Answer: E

NEW QUESTION 211
Which of the following characteristics describe the Root Guard feature? (Choose all that apply.)

A. The port must be put into forwarding state manually after root-inconsistent state has been corrected.
B. A Root Guard port receiving superior BPDU goes into a root-inconsistent state.
C. A Root Guard port receiving inferior BPDU goes into a root-inconsistent state.
D. While the port is in a root-inconsistent state no user data is sent across that port.
E. The port returns to a forwarding state if inferior BPDUs stop.
F. It should be applied to all switch ports.

Answer: BD

Explanation: Reference: Spanning Tree Protocol Root Guard Enhancementhttp://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml

NEW QUESTION 213
Which of the following are TACACS+ characteristics? (Choose all that apply.)

A. Cisco proprietary
B. Standards-based protocol
C. Provides separate services for authentication, authorization, and accounting
D. Encrypts only the password
E. Uses UDP for a transport layer
F. Encrypts the entire packet

Answer: ACF

NEW QUESTION 214
Which of the following is not a valid reason for a packet to be punted?

A. The TCAM has reached capacity
B. An unknown destination MAC address
C. A packet being discarded due to a security violation
D. A Telnet packet from a session being initiated with the switch
E. Routing protocols sending broadcast traffic
F. A packet belonging to a GRE tunnel

Answer: C

Explanation: Not A:
Reference: CCNP TSHOOT Certification Guide: Advanced Cisco CatalystSwitch Troubleshooting

NEW QUESTION 217
Which of the following pieces of information will the command show interface provide? (Choose all that apply.)

A. Layer 1 status
B. Output queue drops
C. Interface CPU utilization
D. Cable type connected to interface
E. Layer 2 status
F. Input queue drops

Answer: ABEF

NEW QUESTION 218
Which of the following are common issues that should be considered when establishing or troubleshooting site-to-site VPNs? (Choose all that apply.)

A. User authentication
B. Overlapping IP address space
C. GRE or IPsec configuration
D. MTU size
E. VPN client software
F. Authentication server configured ly

Answer: BCD

NEW QUESTION 221
Which two of the following options are categories of Network Maintenance tasks?

A. Firefighting
B. Interrupt-driven
C. Policy-based
D. Structured
E. Foundational

Answer: BD

Explanation: Proactive Versus Reactive Network Maintenance:
Network maintenance tasks can be categorized as one of the following: Structured tasks: Performed as a predefined plan.
Interrupt-driven tasks: Involve resolving issues as they are reported.
Reference: CCNP TSHOOT Official Certification Guide, Kevin Wallace, Chapter 1, p.7

NEW QUESTION 224
Whichof the following are valid modes of packet switching on most routers? (Choose all that apply.)

A. Cisco Express Fonvarding
B. FIB switching
C. Cache switching
D. Optimized switching
E. Process switching
F. Fast switching

Answer: AEF

NEW QUESTION 229
.....

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