

Braindumps.300-135.65.QAs

Number: 300-135
Passing Score: 800
Time Limit: 120 min
File Version: 21.7

VCEplus.com

300-135



Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Real Exam Questions with Corrected Answers
Improved Images and Exhibits
Additionally Added Explanations where needed.

I found this dump file the best material for 300-135. You can also use as a key to success.

Topic 1, Mix Questions

Sections

1. Mix Questions
2. Troubleshooting VTP
3. Troubleshooting EIGRP
4. Troubleshooting HSRP
5. Troubleshooting OSPF
6. Ticket 1: Switch Port Trunk
7. Ticket 2 : ACCESS VLAN
8. Ticket 3 : OSPF Authentication
9. Ticket 4 : BGP Neighbor
10. Ticket 5 : NAT ACL
11. Ticket 6 : R1 ACL
12. Ticket 7 : Port Security
13. Ticket 8 : Redistribution of EIGRP to OSPF
14. Ticket 9 : EIGRP AS number
15. Ticket 10 : VLAN Access Map

16. Ticket 11 : IPV6 OSPF
17. Ticket 12 : HSRP Issue
18. Ticket 13 : DHCP Issue

Exam A

QUESTION 1

Exhibit:

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

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

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

Correct Answer: DF

Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 2

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.

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 3

Refer to the exhibit.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 212.50.185.126 to network 0.0.0.0

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

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

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

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 4

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

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

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 5

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

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

Correct Answer: ABD

Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 6

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.

Correct Answer: C

Section: Mix Questions

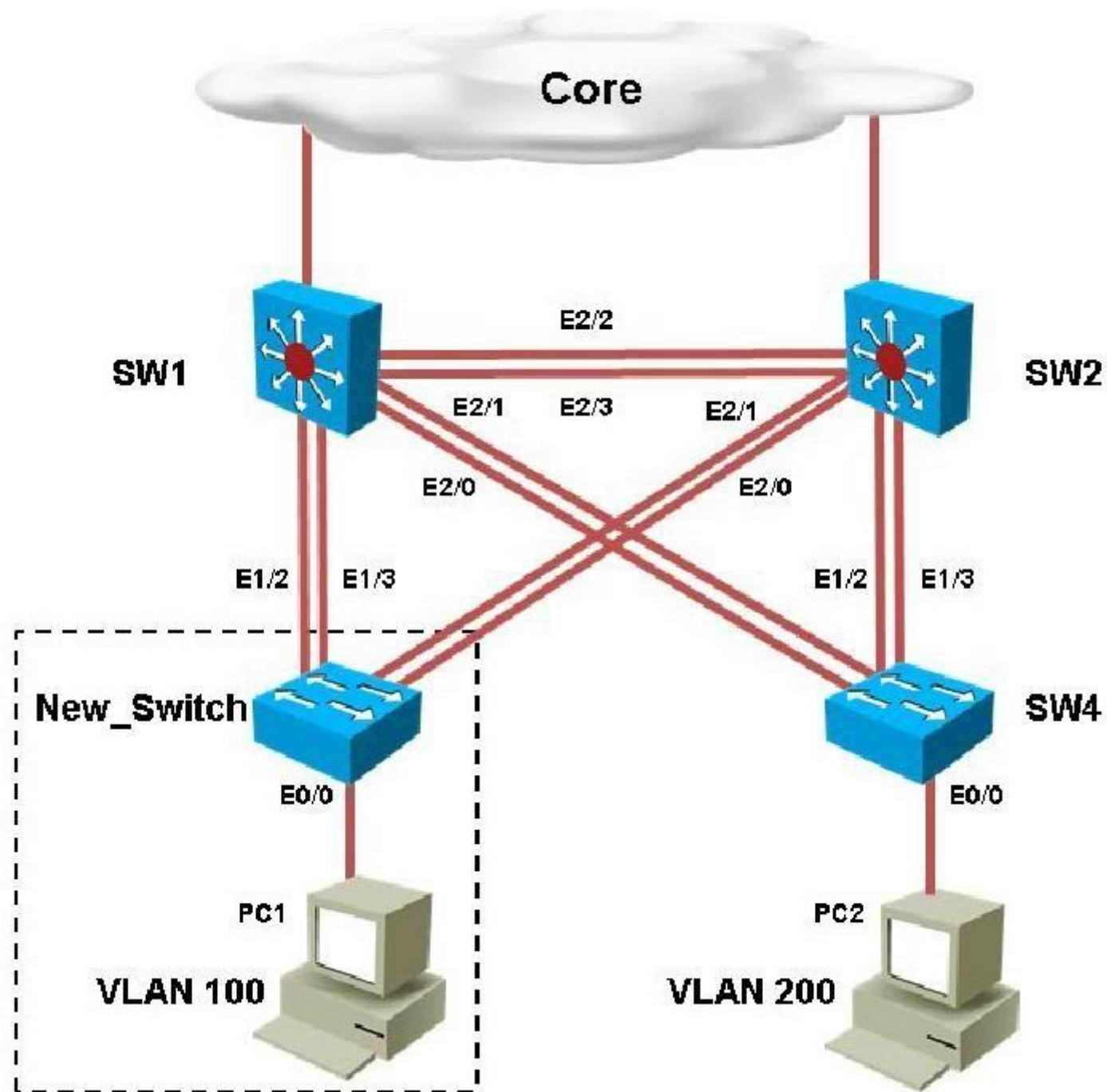
Explanation

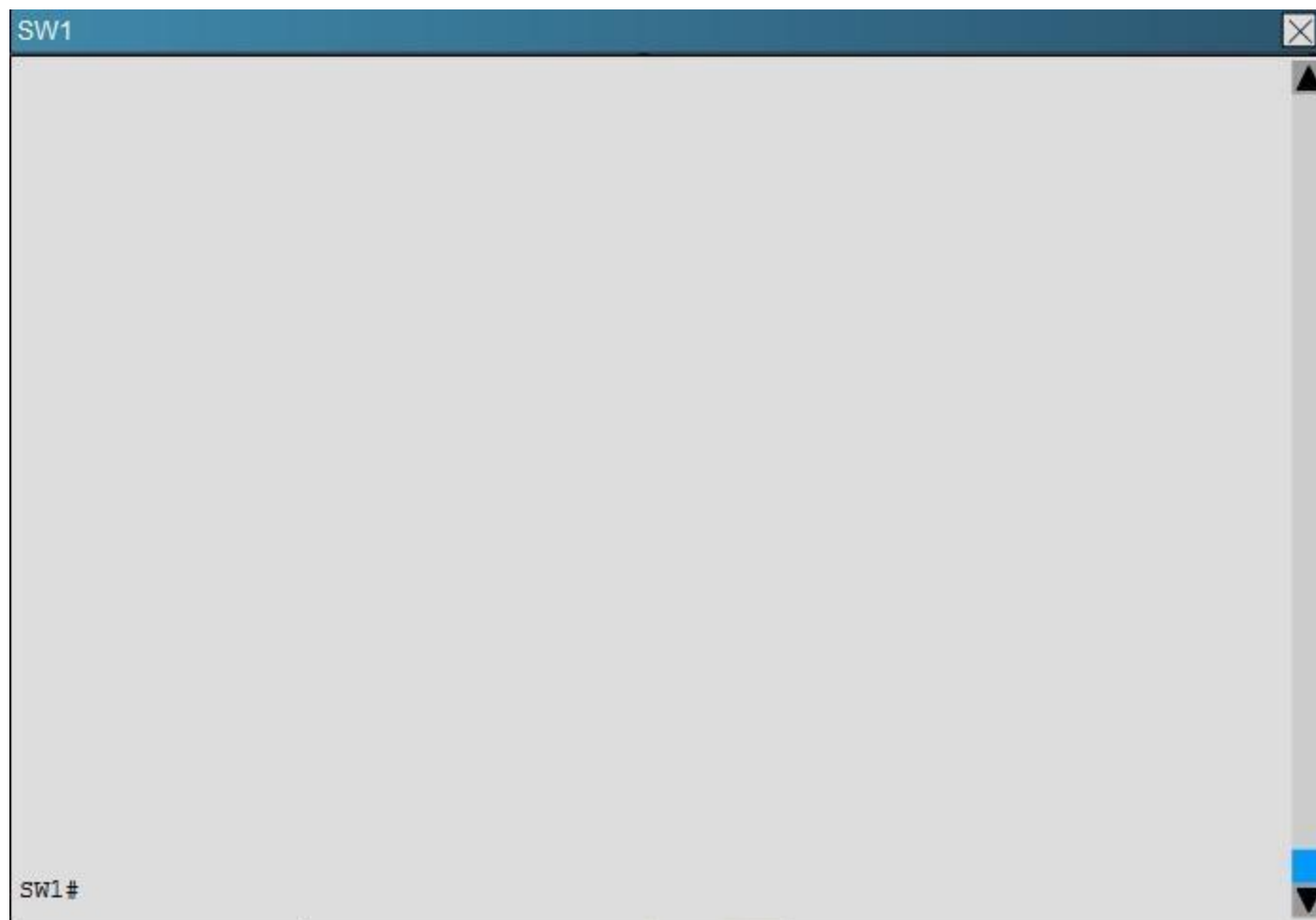
Explanation/Reference:

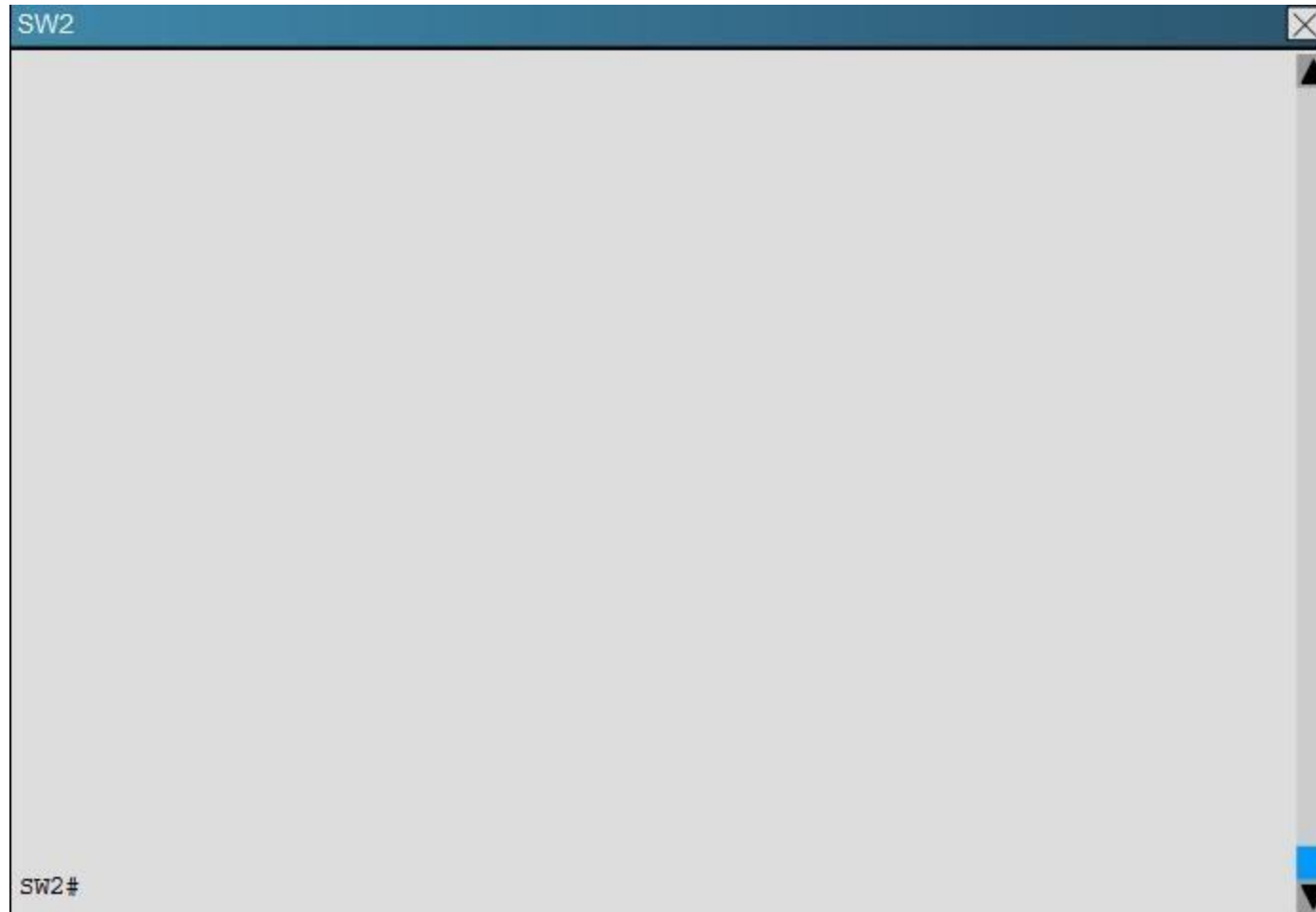
Topic 2, Troubleshooting VTP

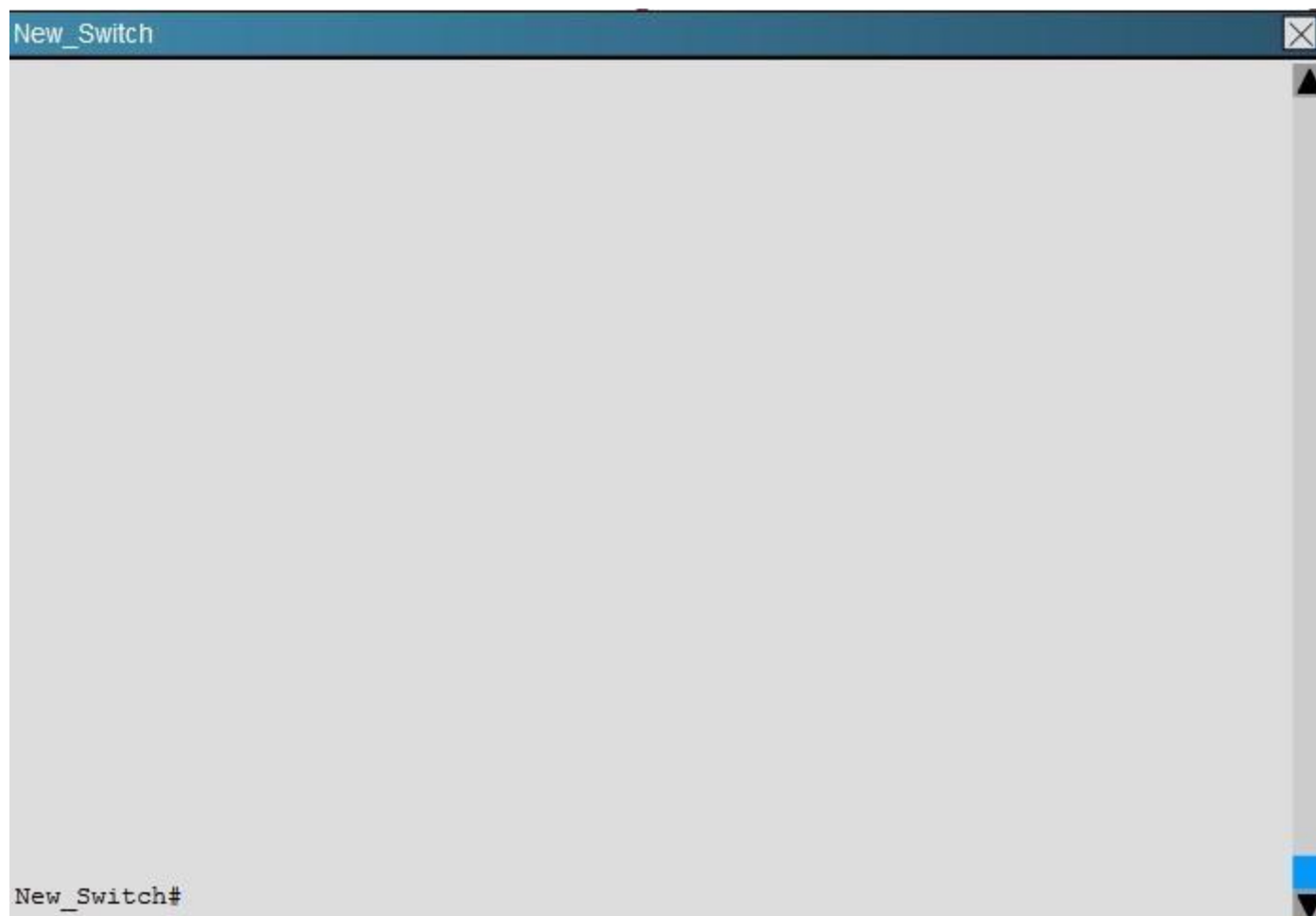
QUESTION 7

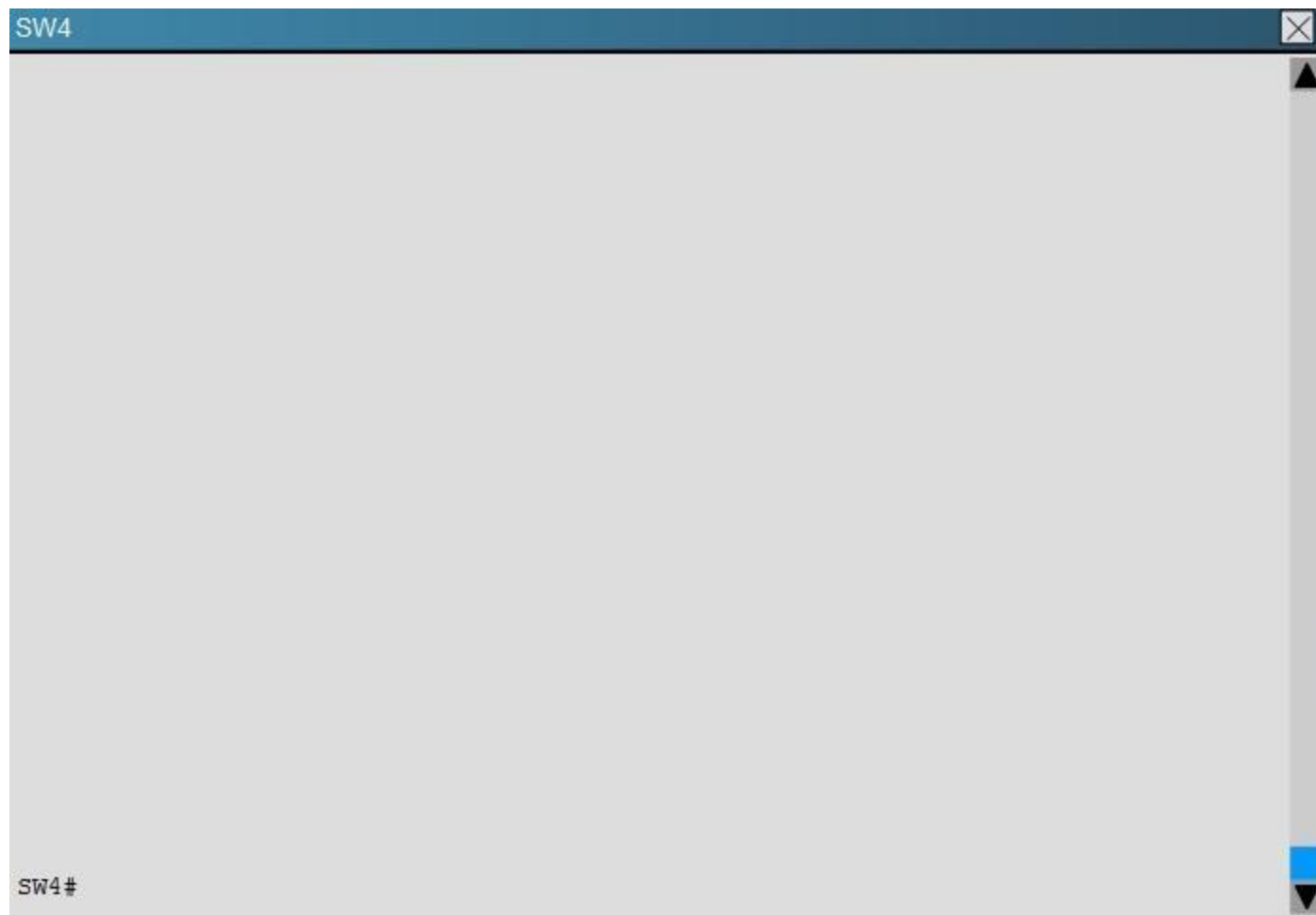
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.











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

Correct Answer: C

Section: Troubleshooting VTP

Explanation

Explanation/Reference:

Explanation:

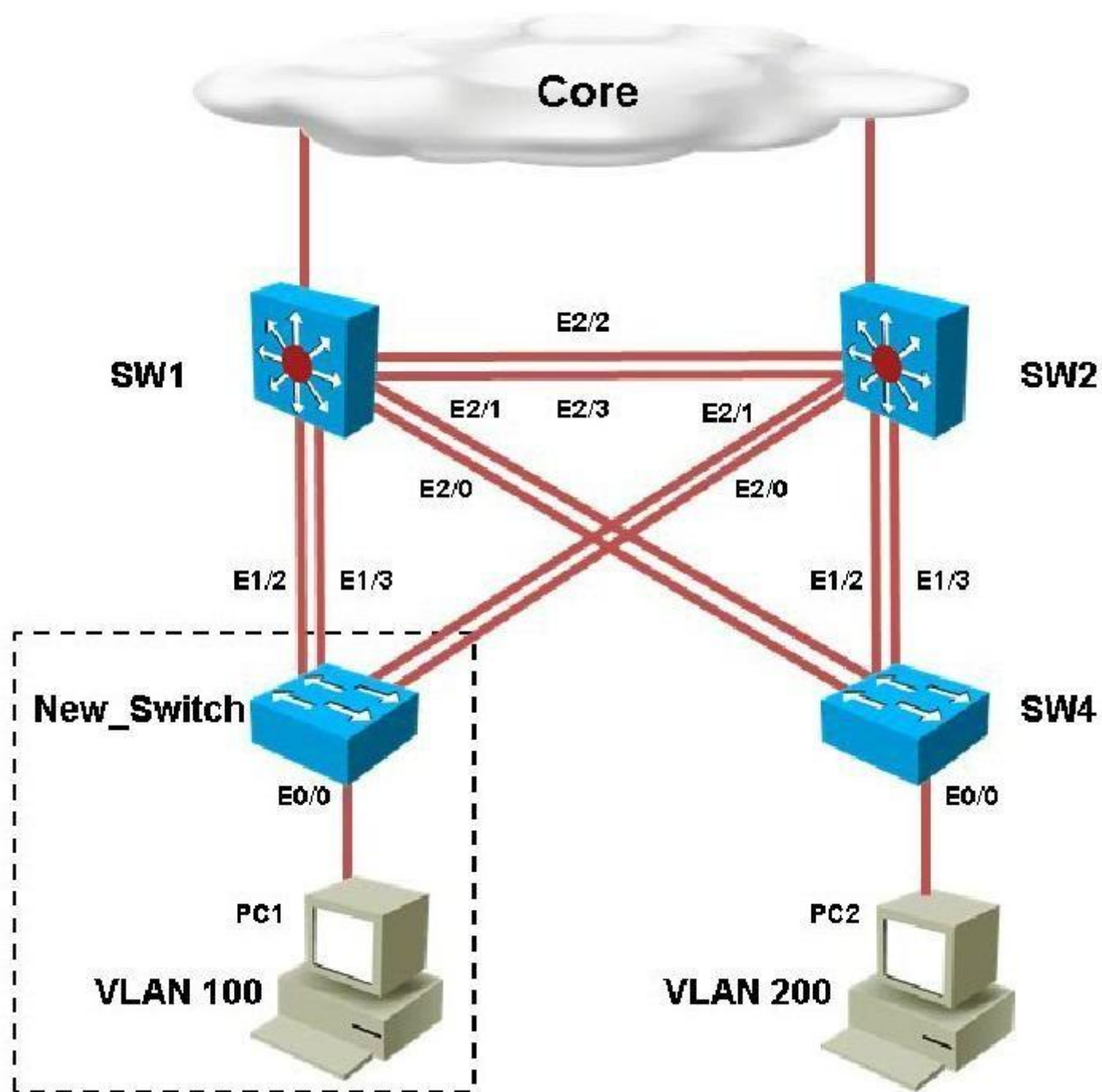
By looking at the configuration for SW2, we see that it is missing VLAN 200, and the "switchport access vlan 200" command is missing under interface eth 0/0:

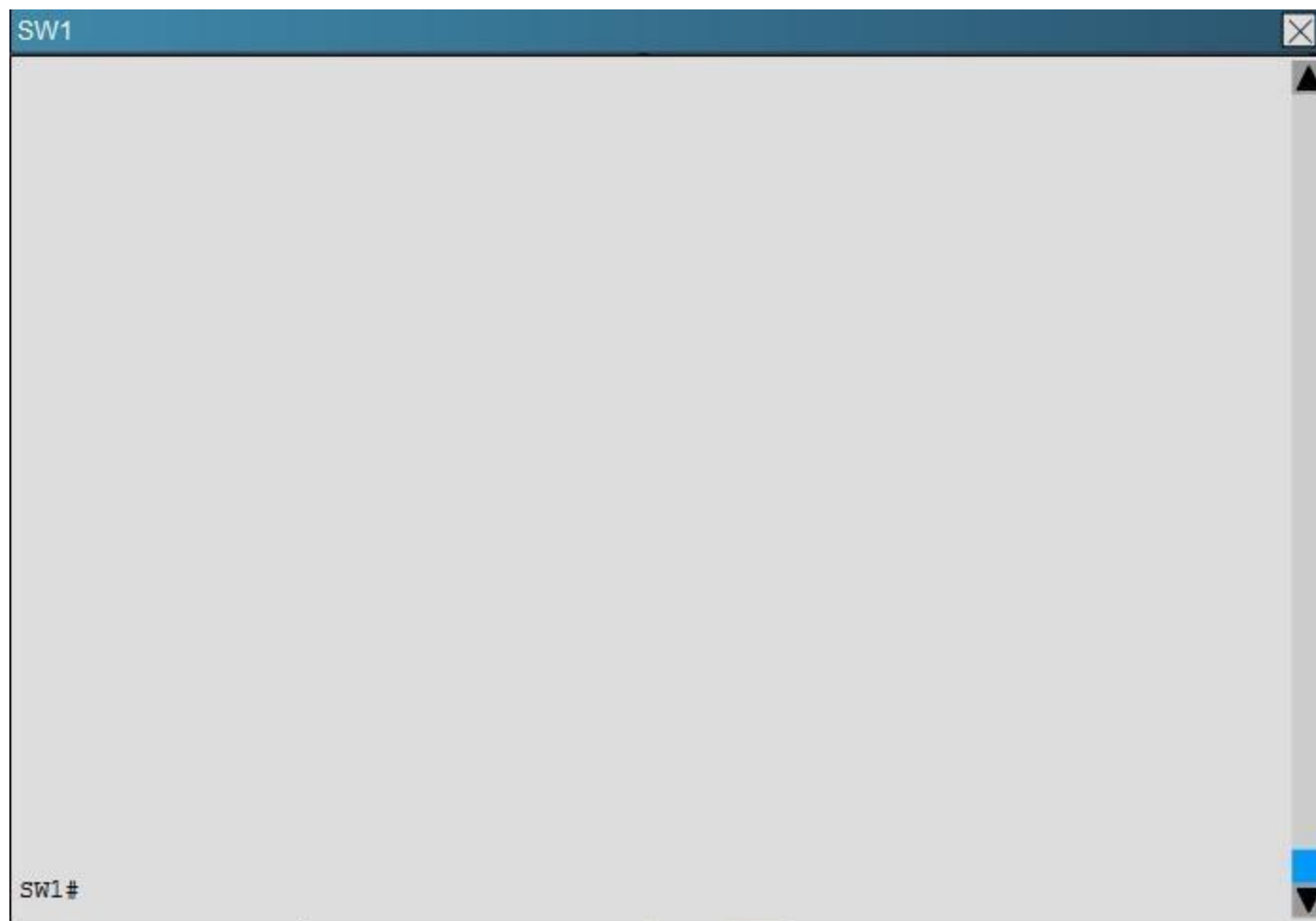
SW4

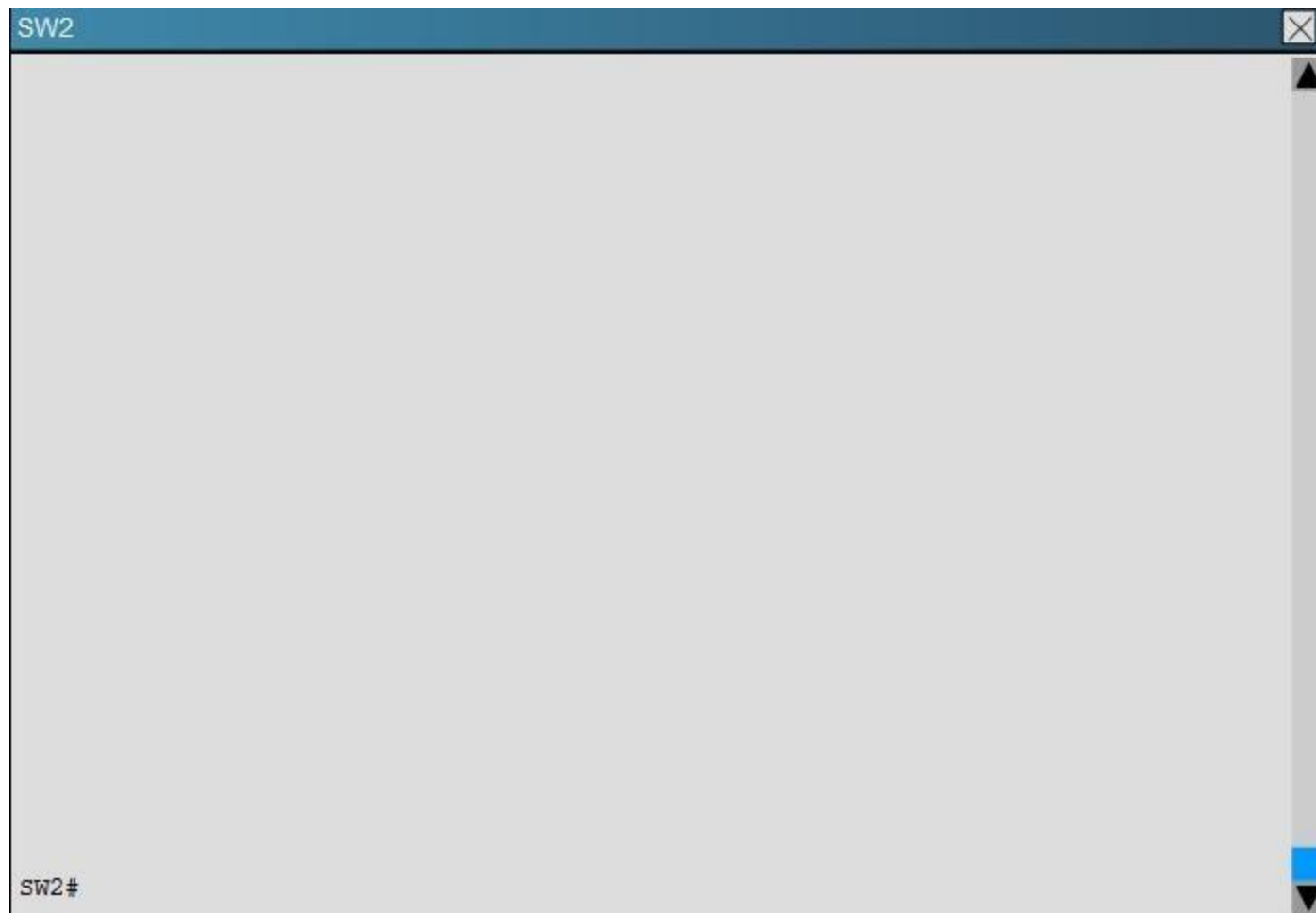
```
vlan internal allocation policy ascending
!
vlan 100
!
vlan 300
  name Management_VLAN
!
vlan 400
  name VLAN400
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
  description Connected to PC2
  switchport mode access
  duplex auto
!
```

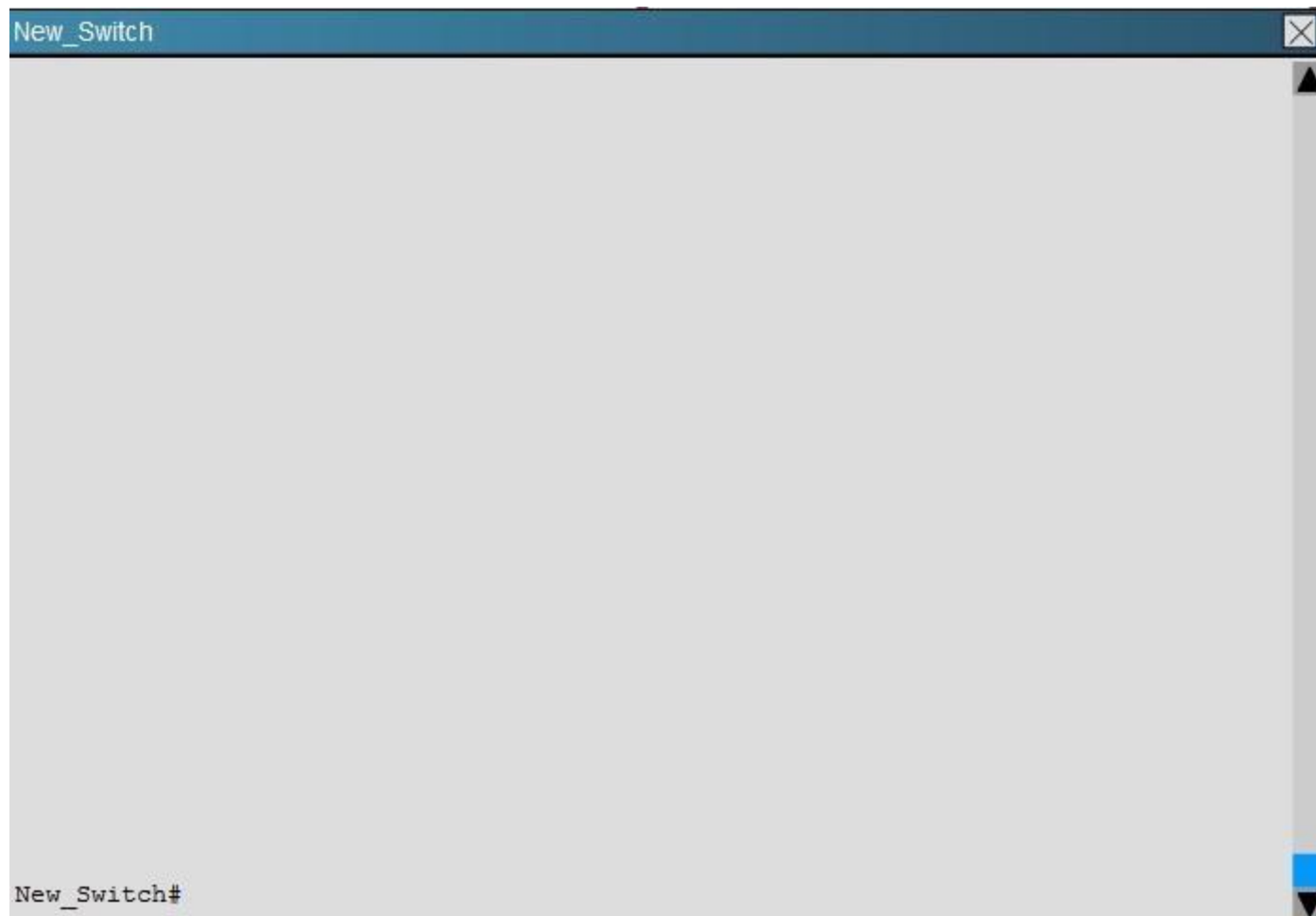
QUESTION 8

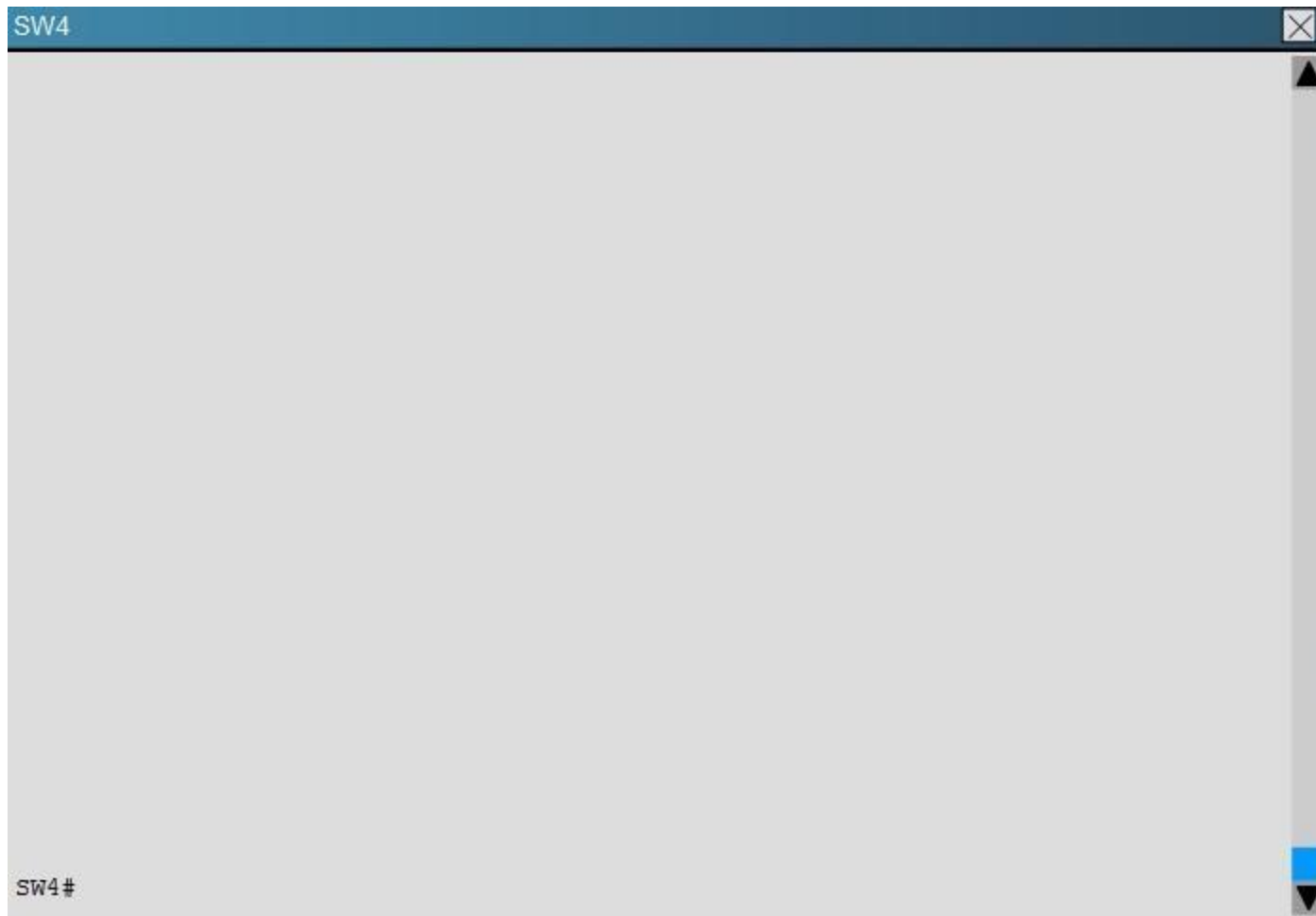
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.











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

Correct Answer: A

Section: Troubleshooting VTP

Explanation

Explanation/Reference:

Explanation:

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

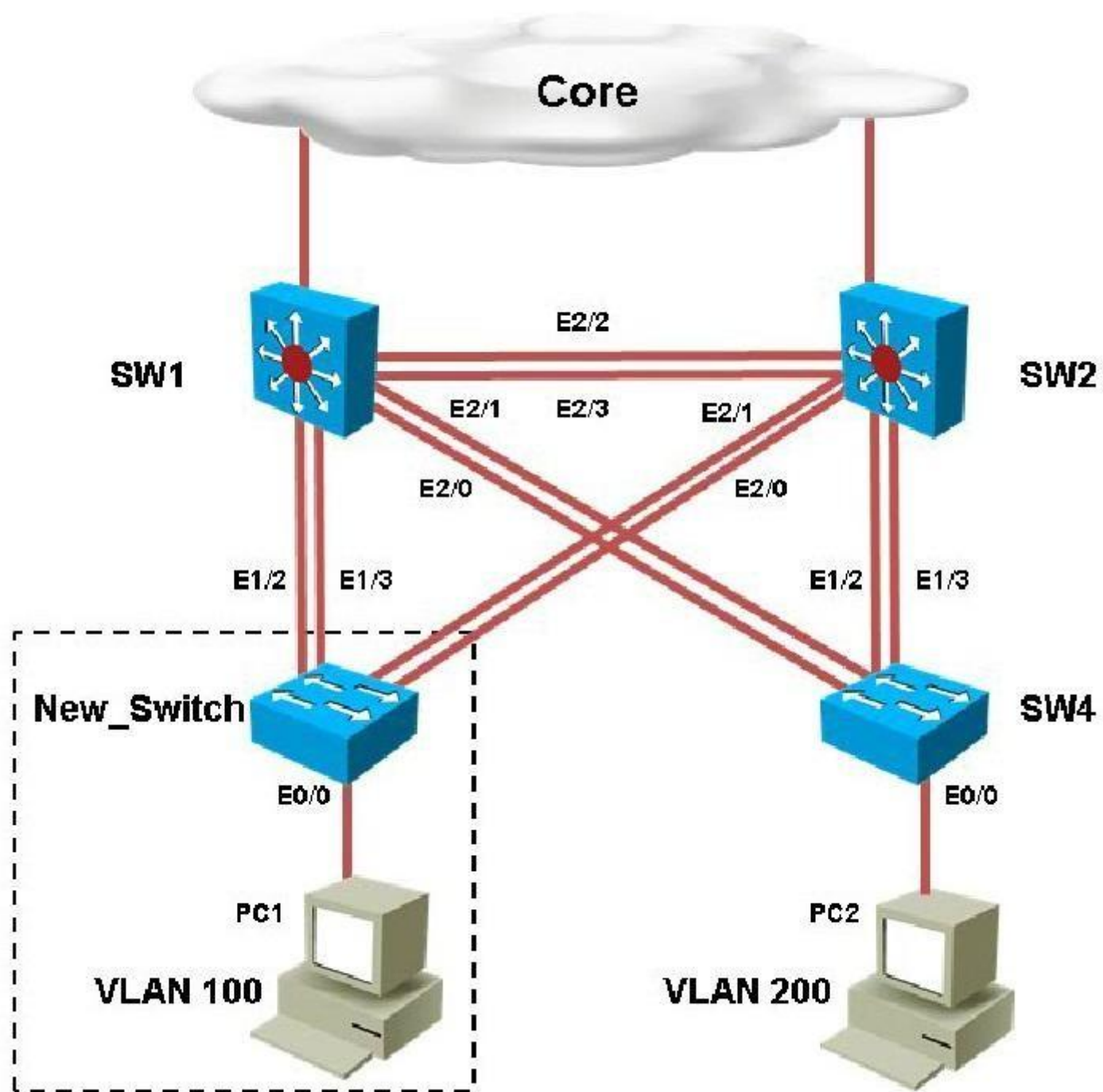
New_Switch

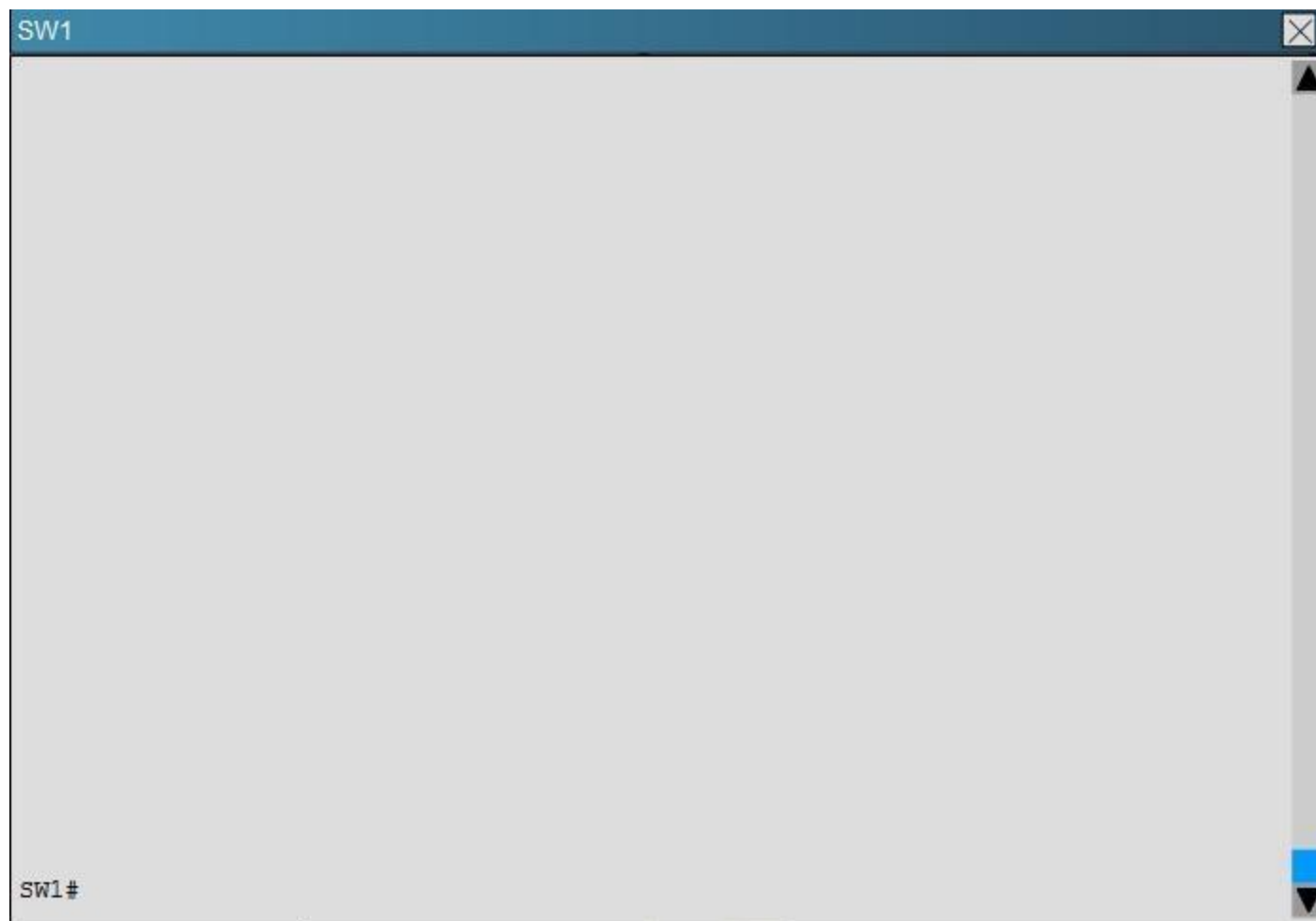
```
!  
interface Ethernet2/1  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  duplex auto  
  spanning-tree bpduguard enable  
  spanning-tree guard loop  
!
```

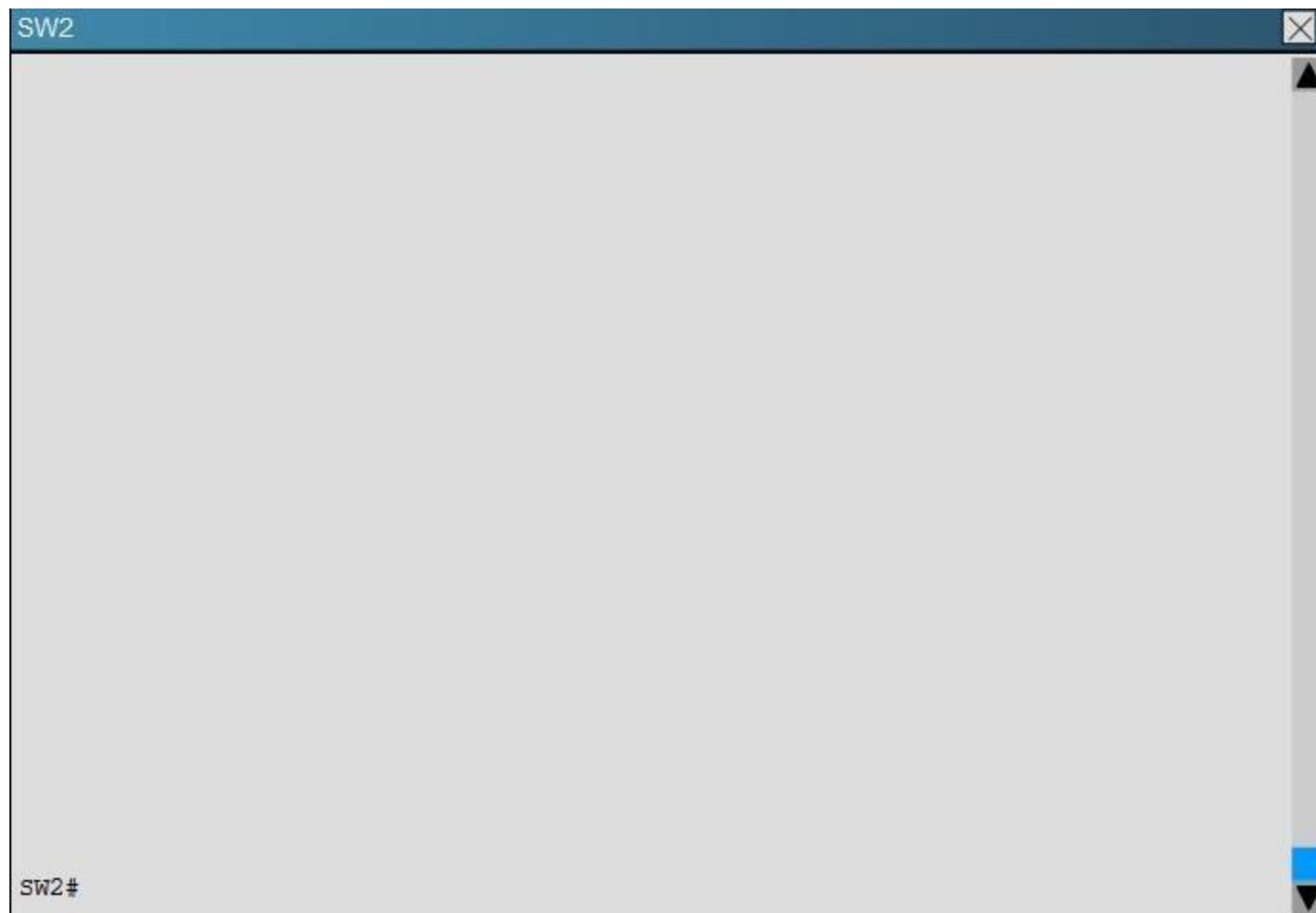
The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the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

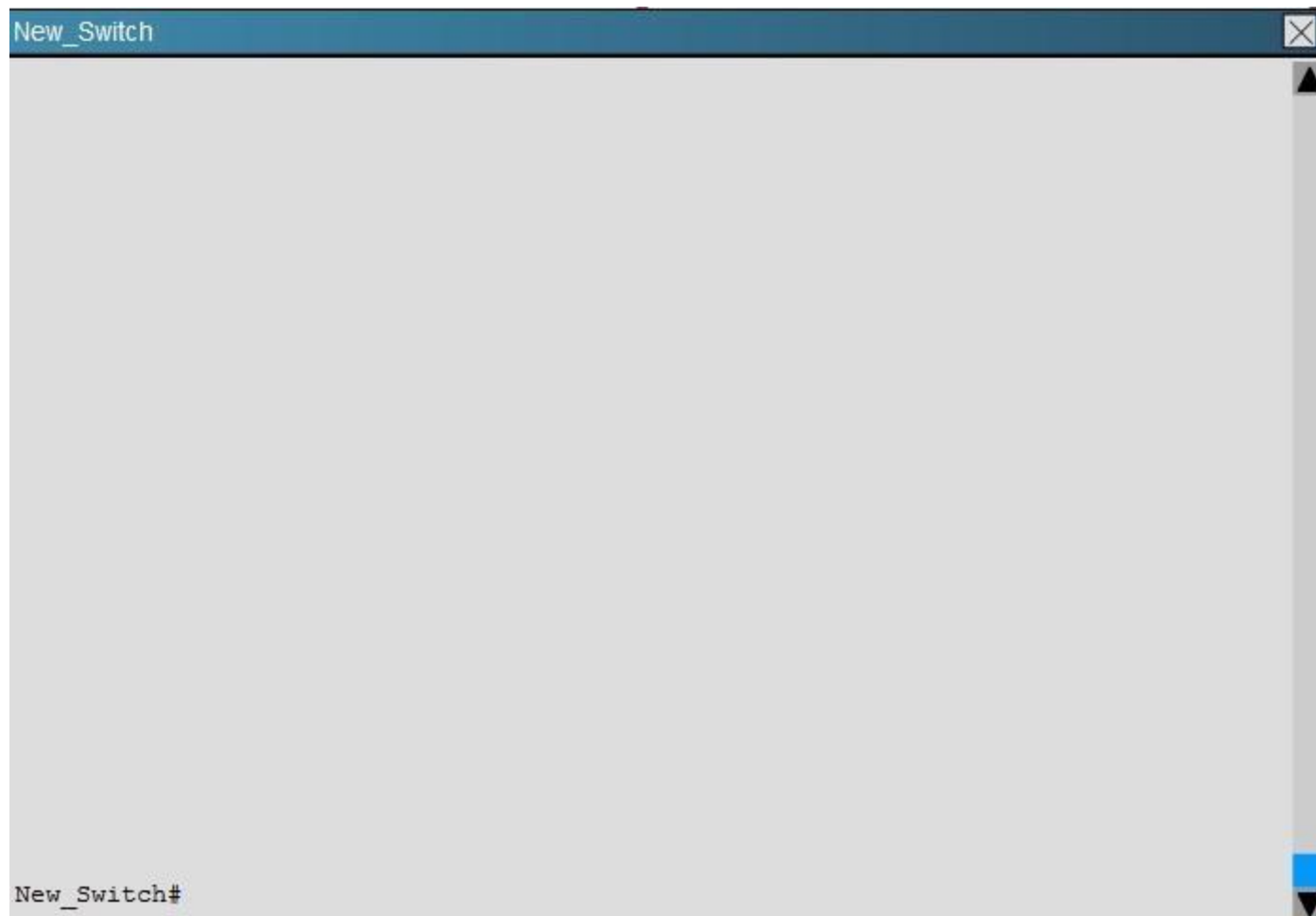
QUESTION 9

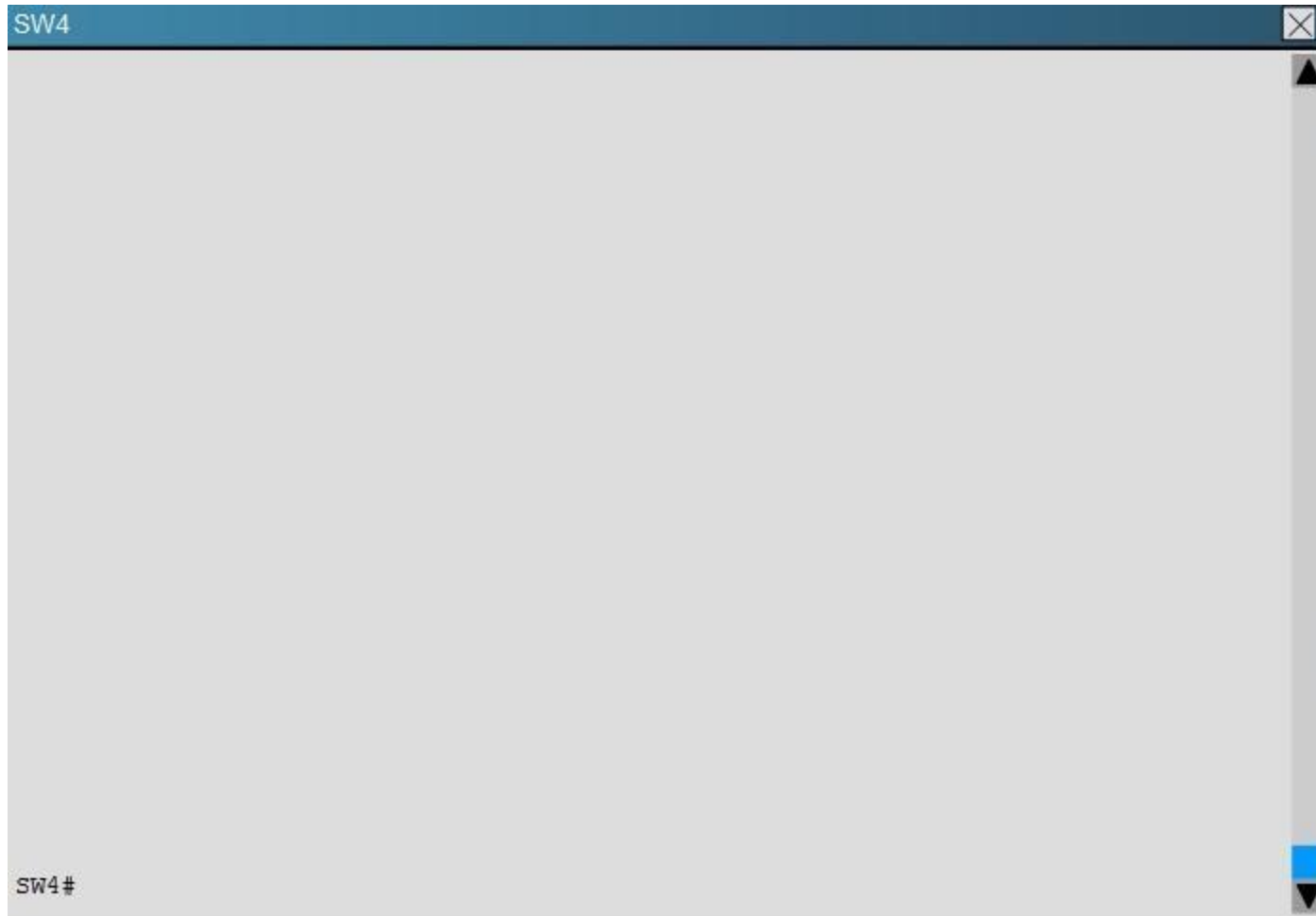
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.











You have configured PVST+ load balancing between SW1 and the New_Switch in such a way that both the links E2/2 and E2/3 are utilized for traffic flow, which component of the configuration is preventing PVST+ load balancing between SW1 and SW2 links

- A. Port priority configuration on SW1
- B. Port priority configuration on the New_Switch
- C. Path cost configuration on SW1
- D. Path cost configuration on the New_Switch

Correct Answer: D

Section: Troubleshooting VTP

Explanation

Explanation/Reference:

Explanation:

Here is the configuration found on the New_Switch:

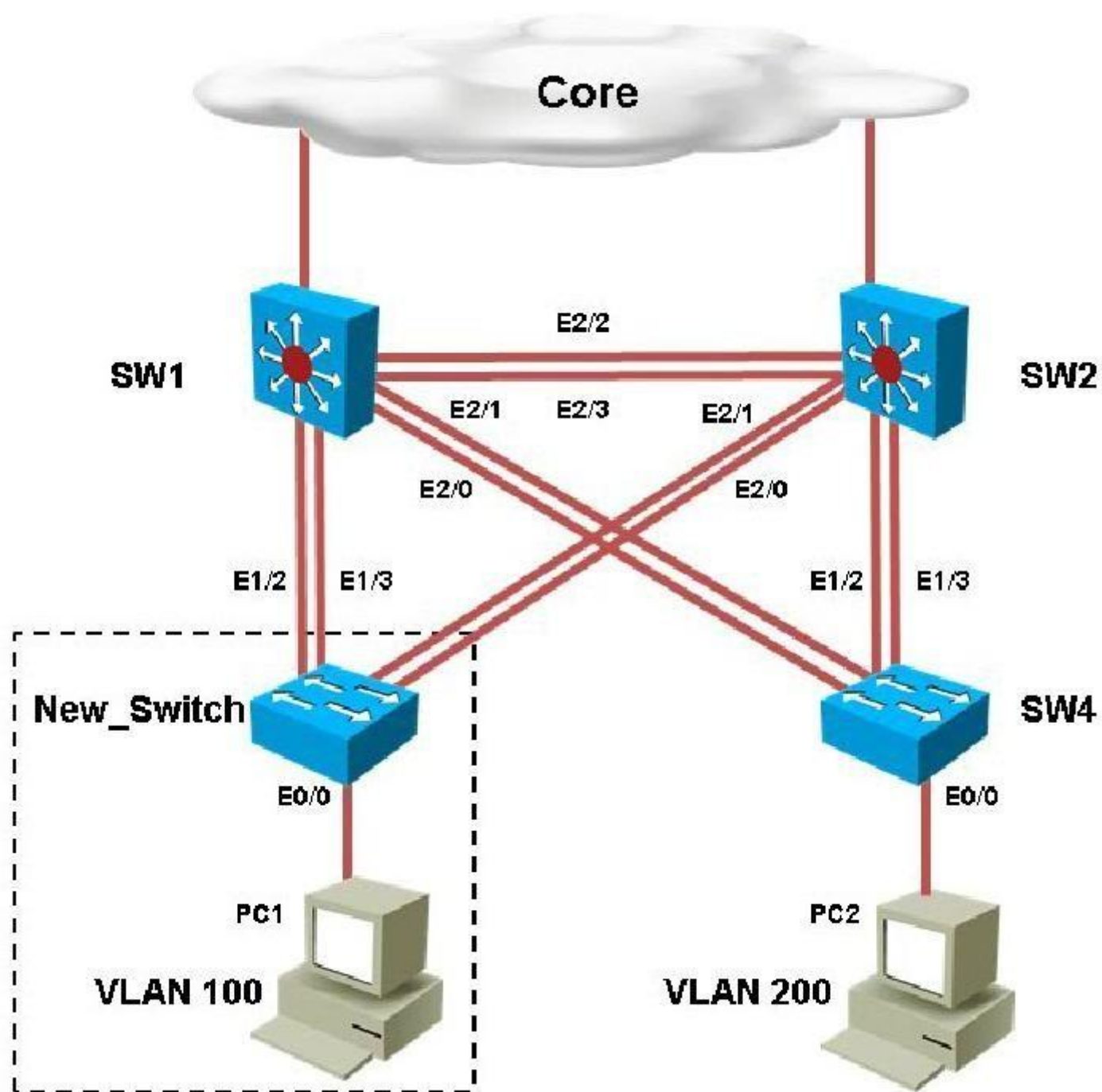
New_Switch

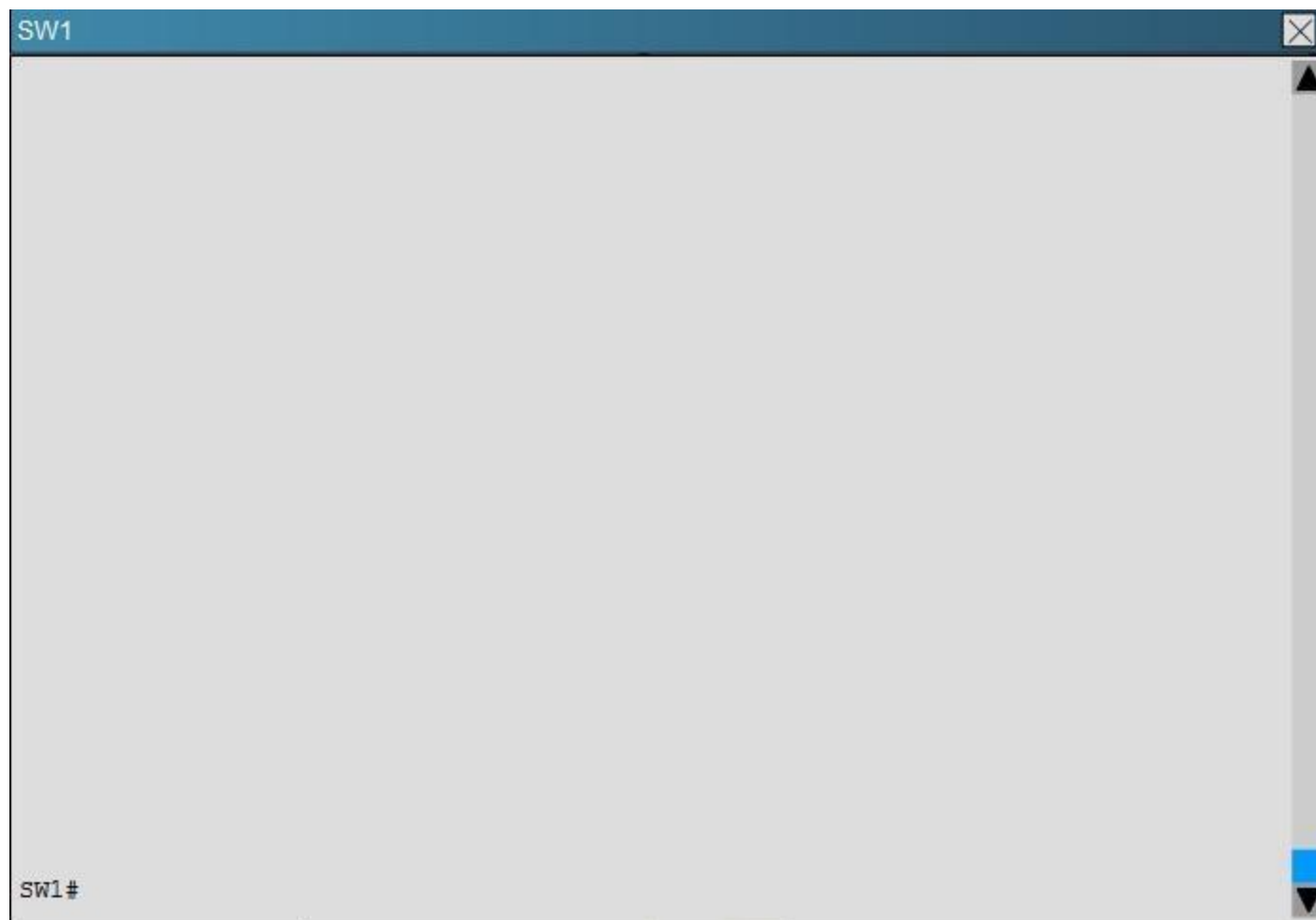
```
!  
interface Ethernet1/2  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  duplex auto  
!  
interface Ethernet1/3  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  duplex auto  
  spanning-tree cost 250  
!
```

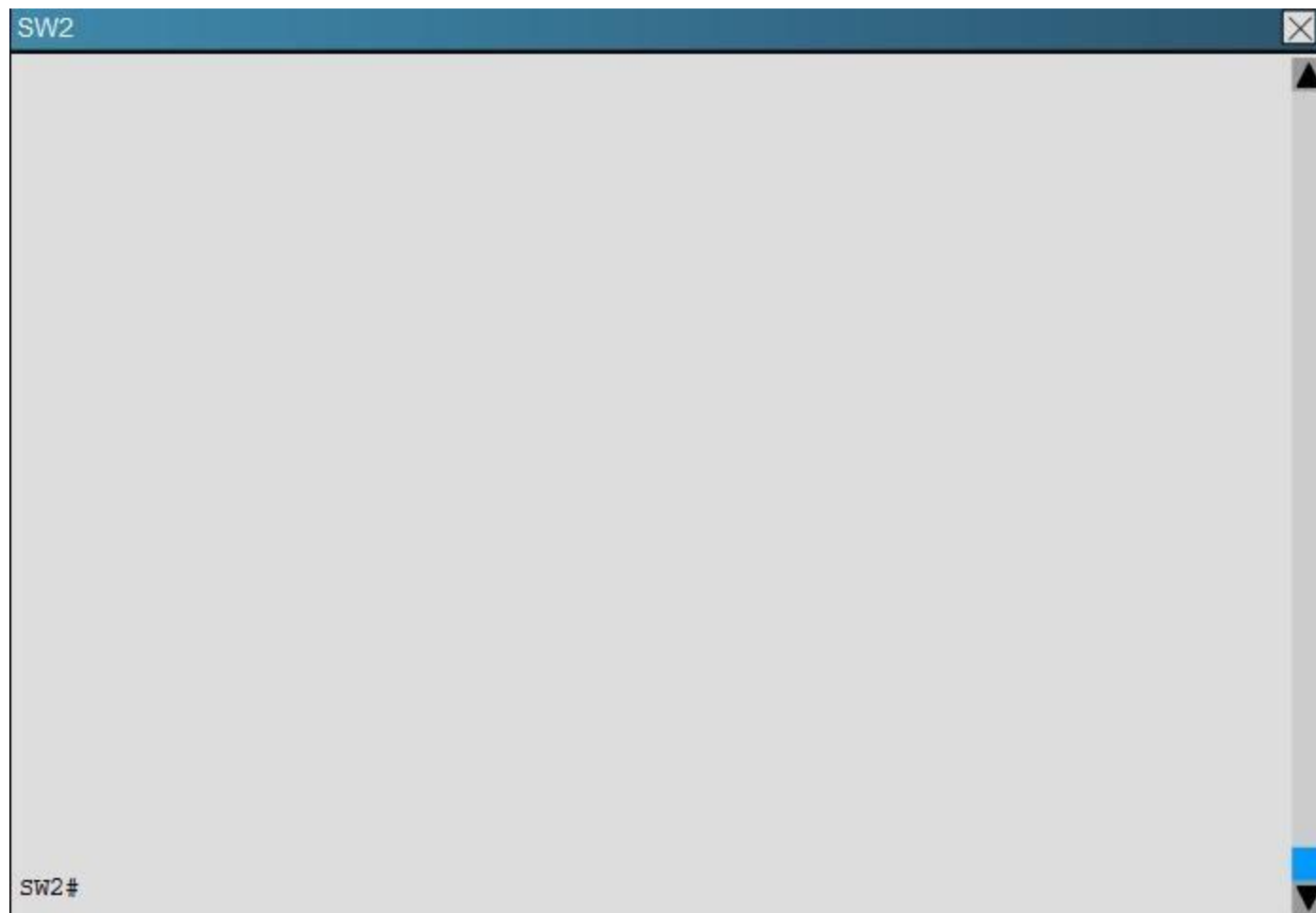
This causes the port cost for link eth 1/3 to increase the path cost to 250 for all VLANs, making that link less preferred so that only eth 1/2 will be used.

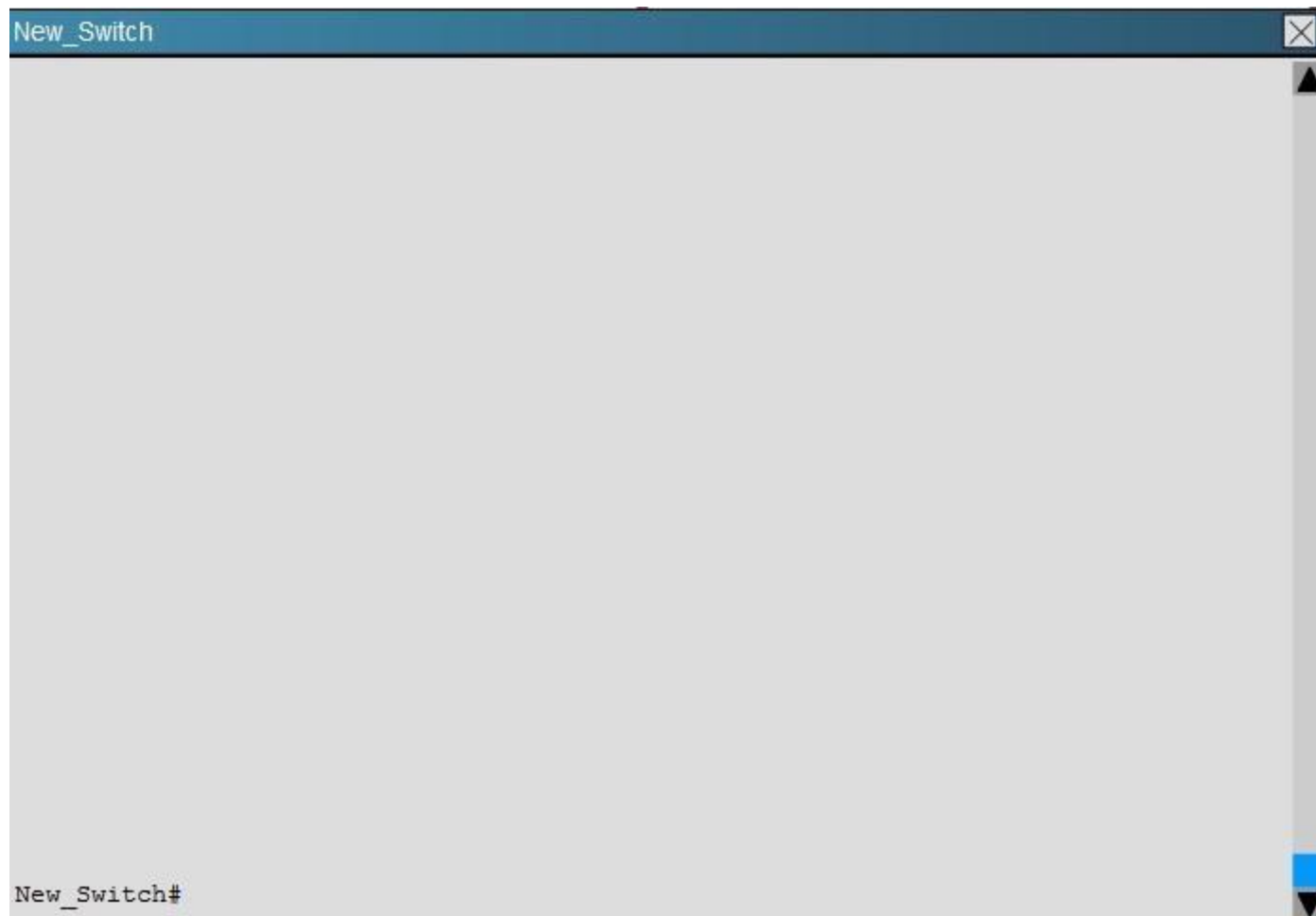
QUESTION 10

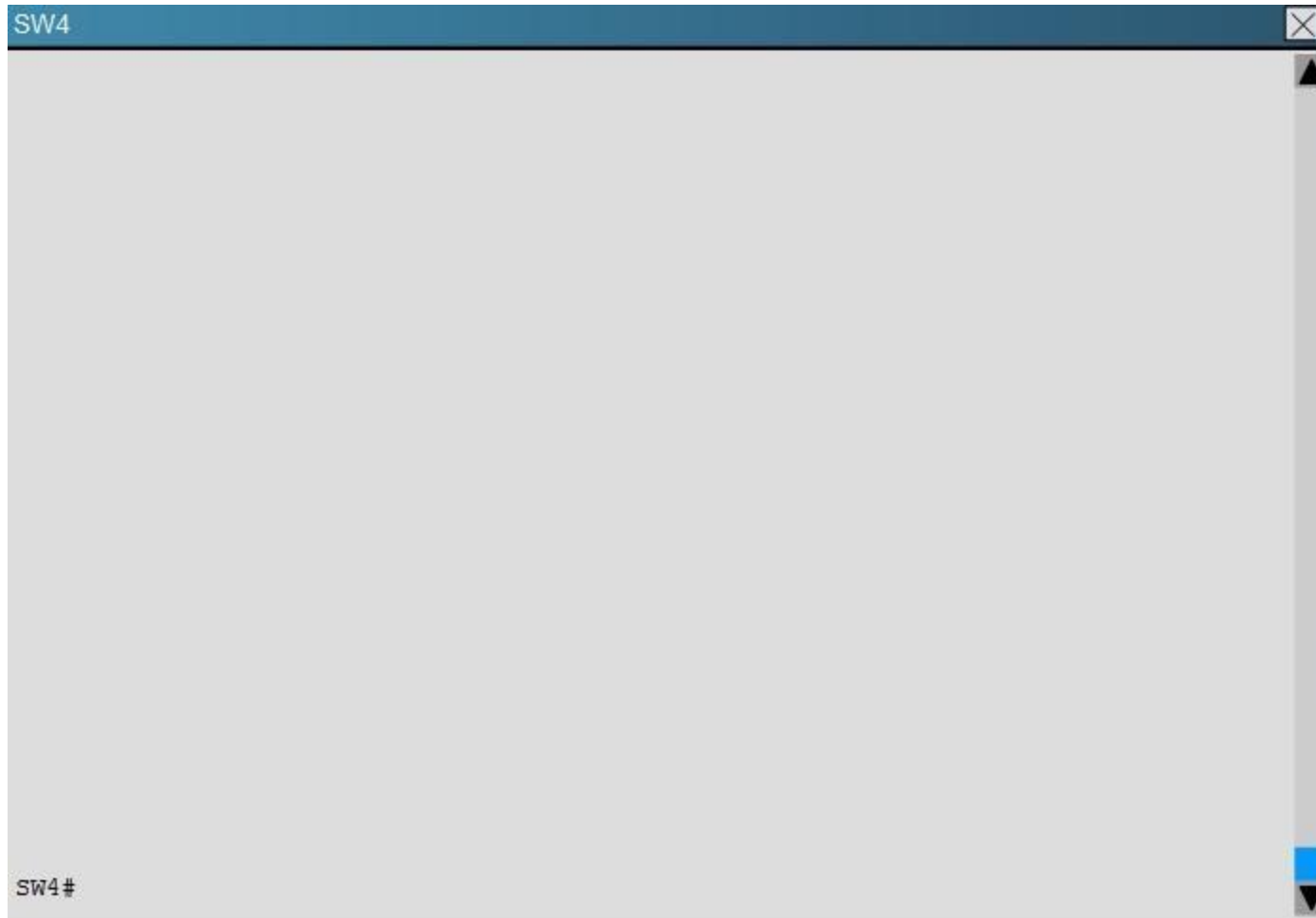
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.











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

Correct Answer: D

Section: Troubleshooting VTP

Explanation

Explanation/Reference:

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  
!  
!
```

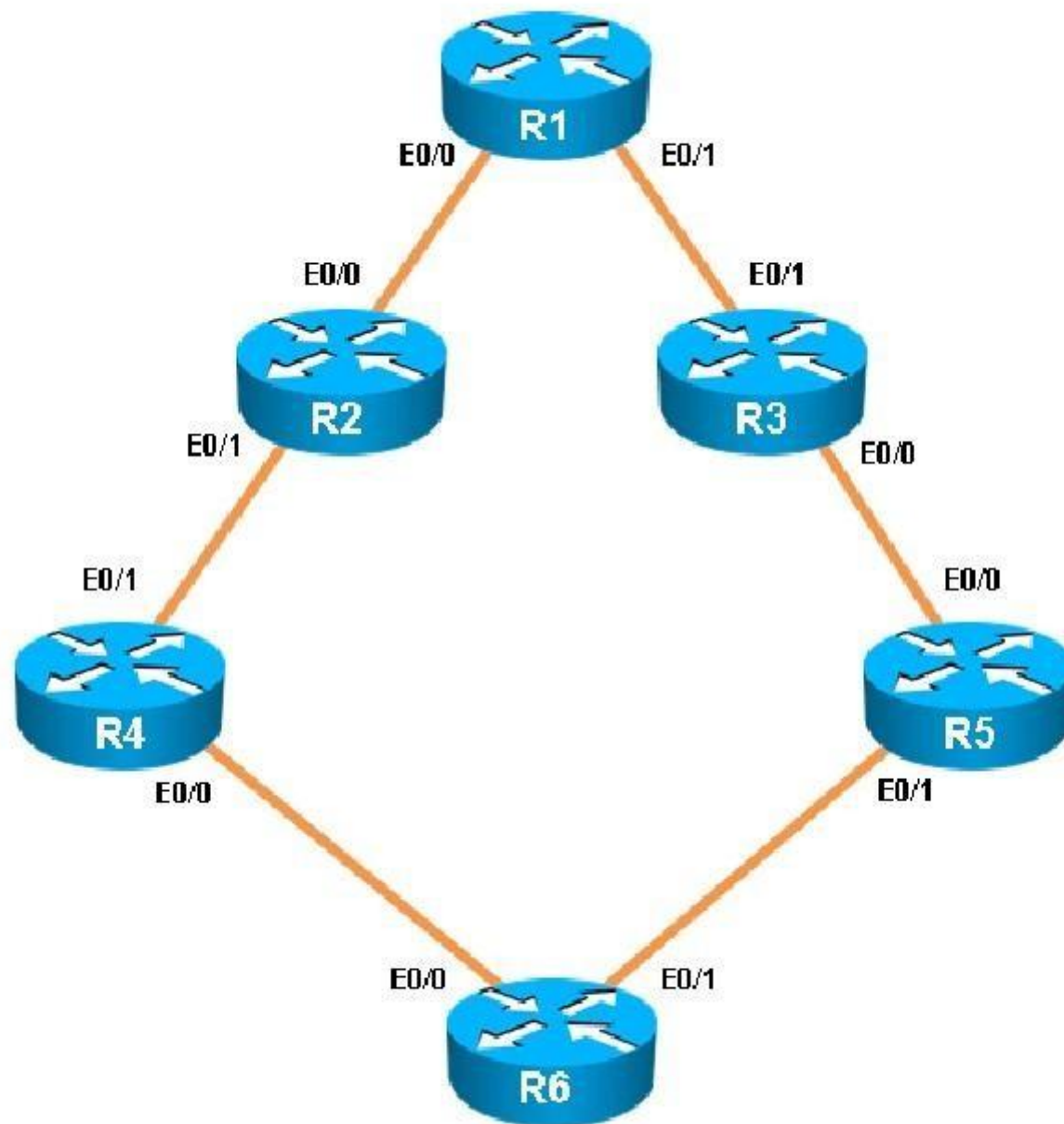

SW4

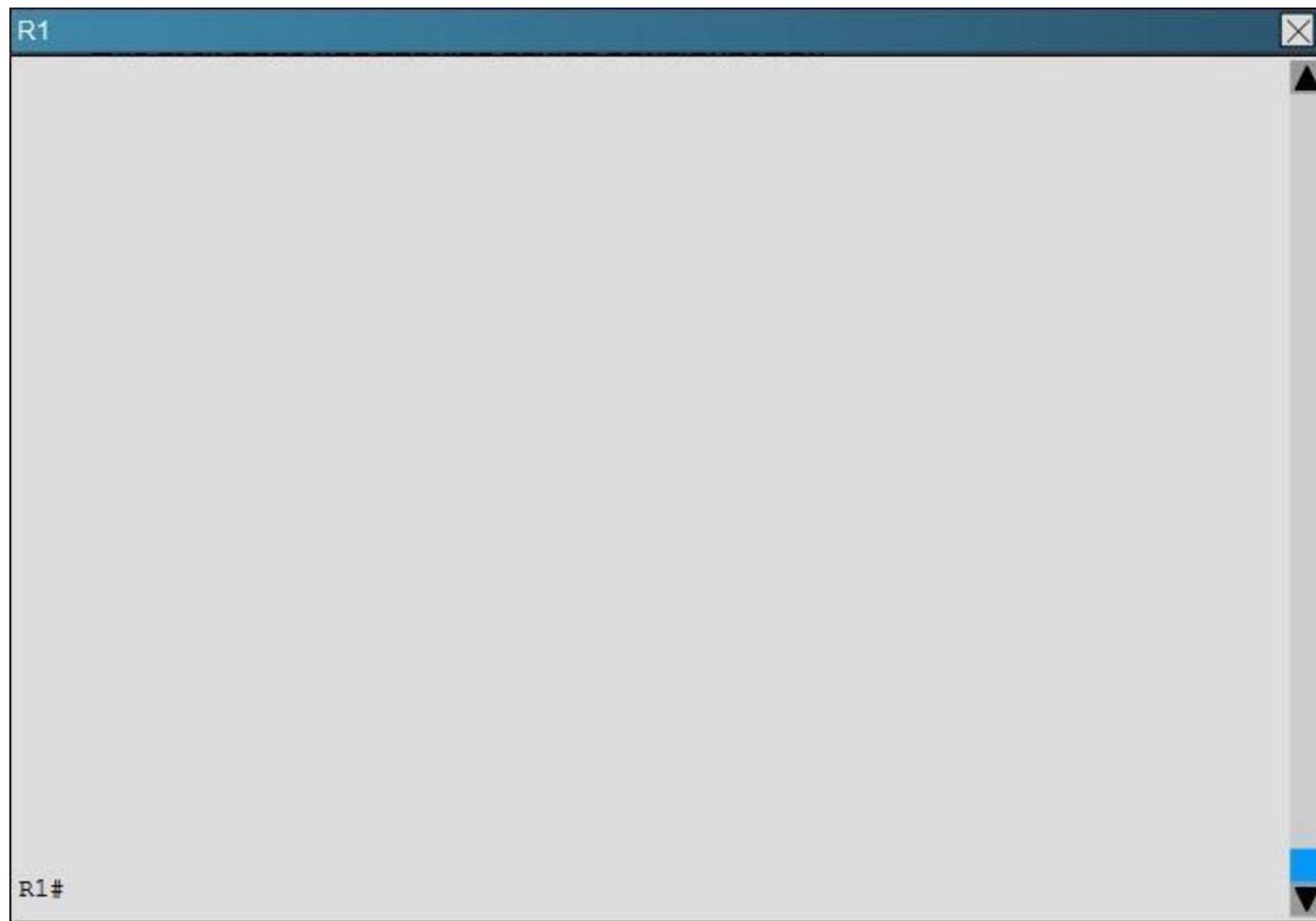
```
switchport mode trunk
duplex auto
!
interface Ethernet2/2
shutdown
duplex auto
!
interface Ethernet2/3
shutdown
duplex auto
!
interface Vlan1
no ip address
!
interface Vlan300
ip address 192.168.100.4 255.255.255.0
!
!
```

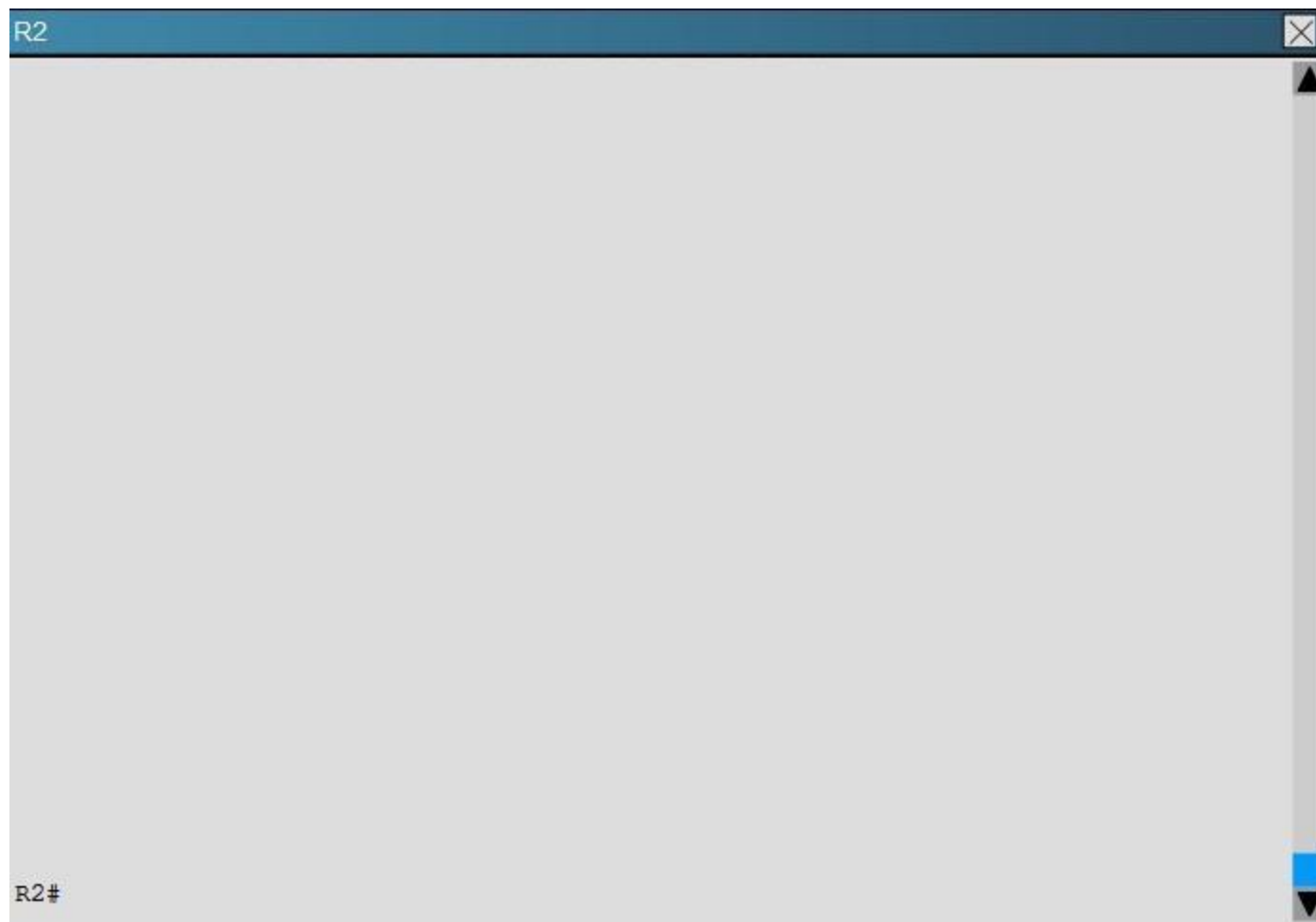
Topic 3, Troubleshooting EIGRP

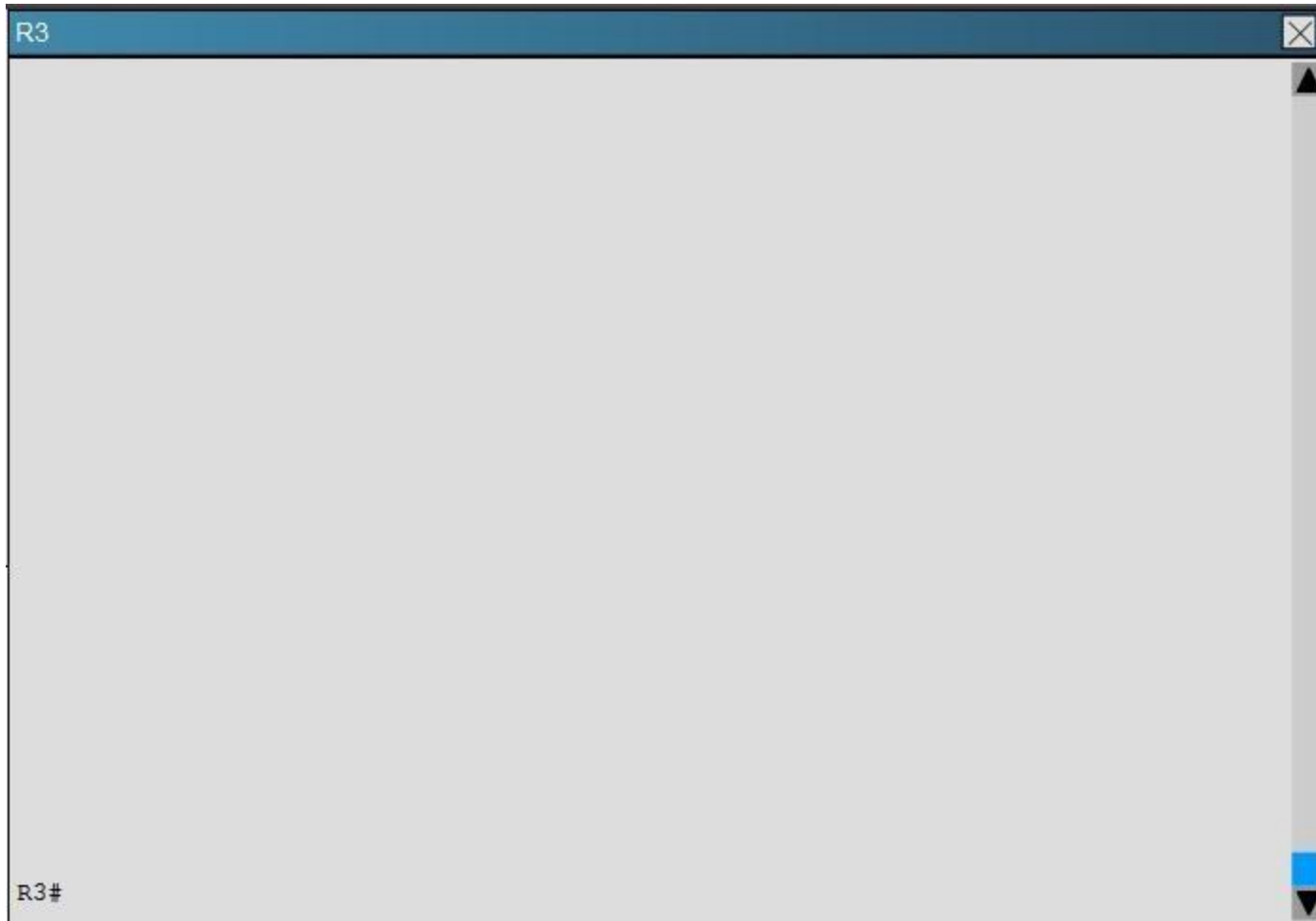
QUESTION 11

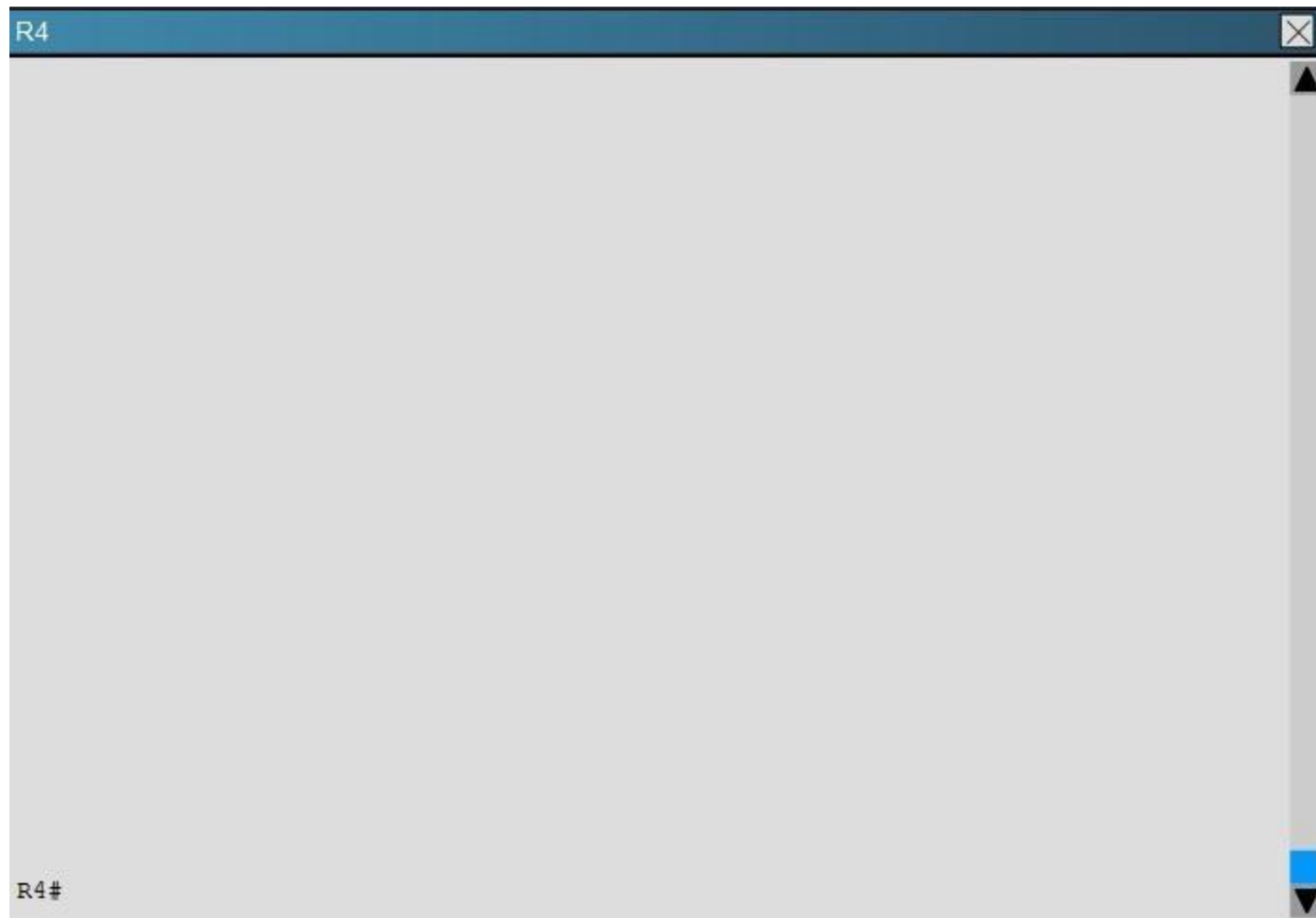
You have been brought in to troubleshoot an EIGRP network. A network engineer has made configuration changes to the network rendering some locations unreachable. You are to locate the problem and suggest solution to resolve the issue.

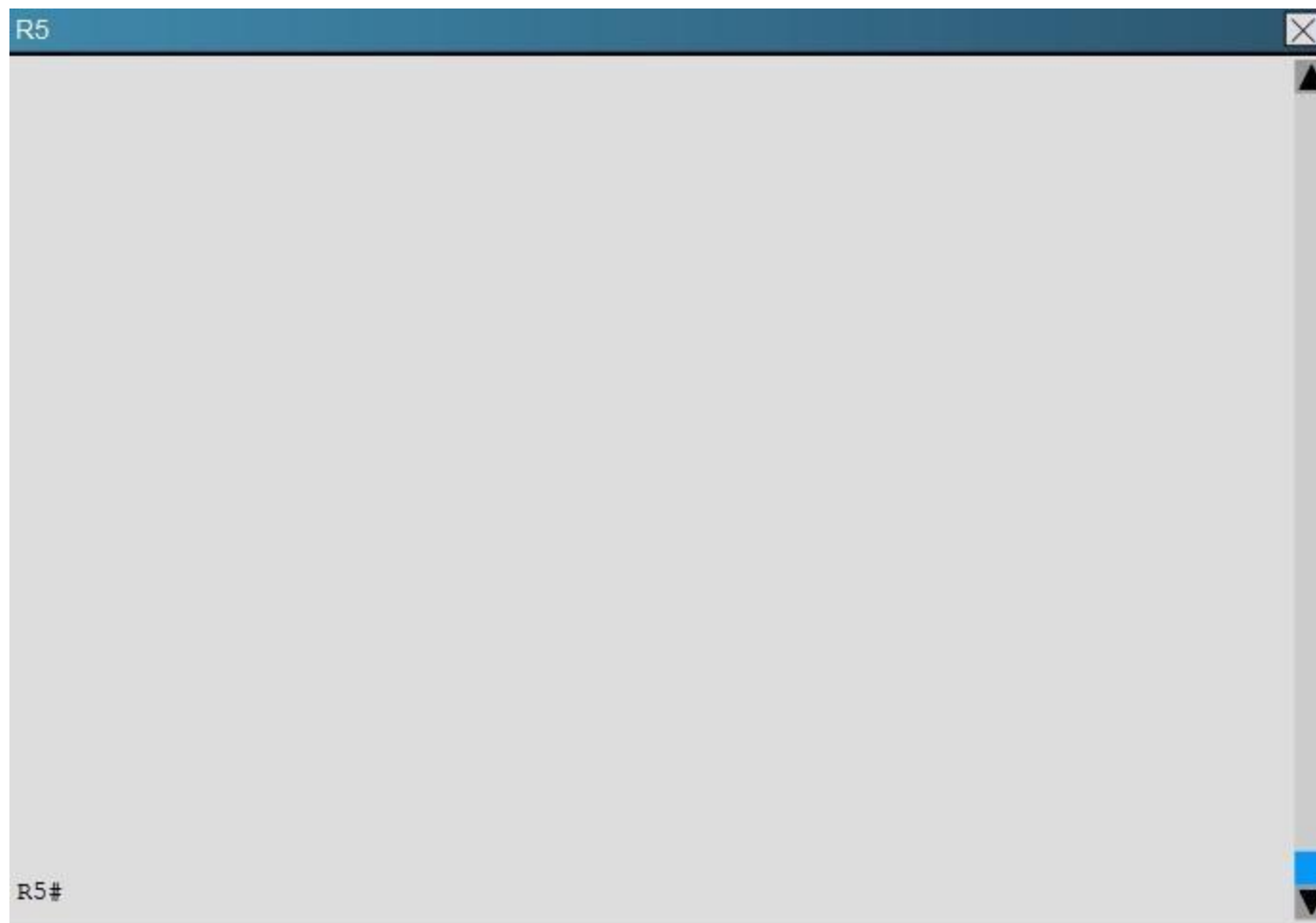














R5 has become partially isolated from the remainder of the network. R5 can reach devices on directly connected networks but nothing else. What is causing the problem?

- 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

Correct Answer: B

Section: Troubleshooting EIGRP

Explanation

Explanation/Reference:

Explanation:

Here we see that distribute list 3 has been applied to EIGRP on router R5, 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

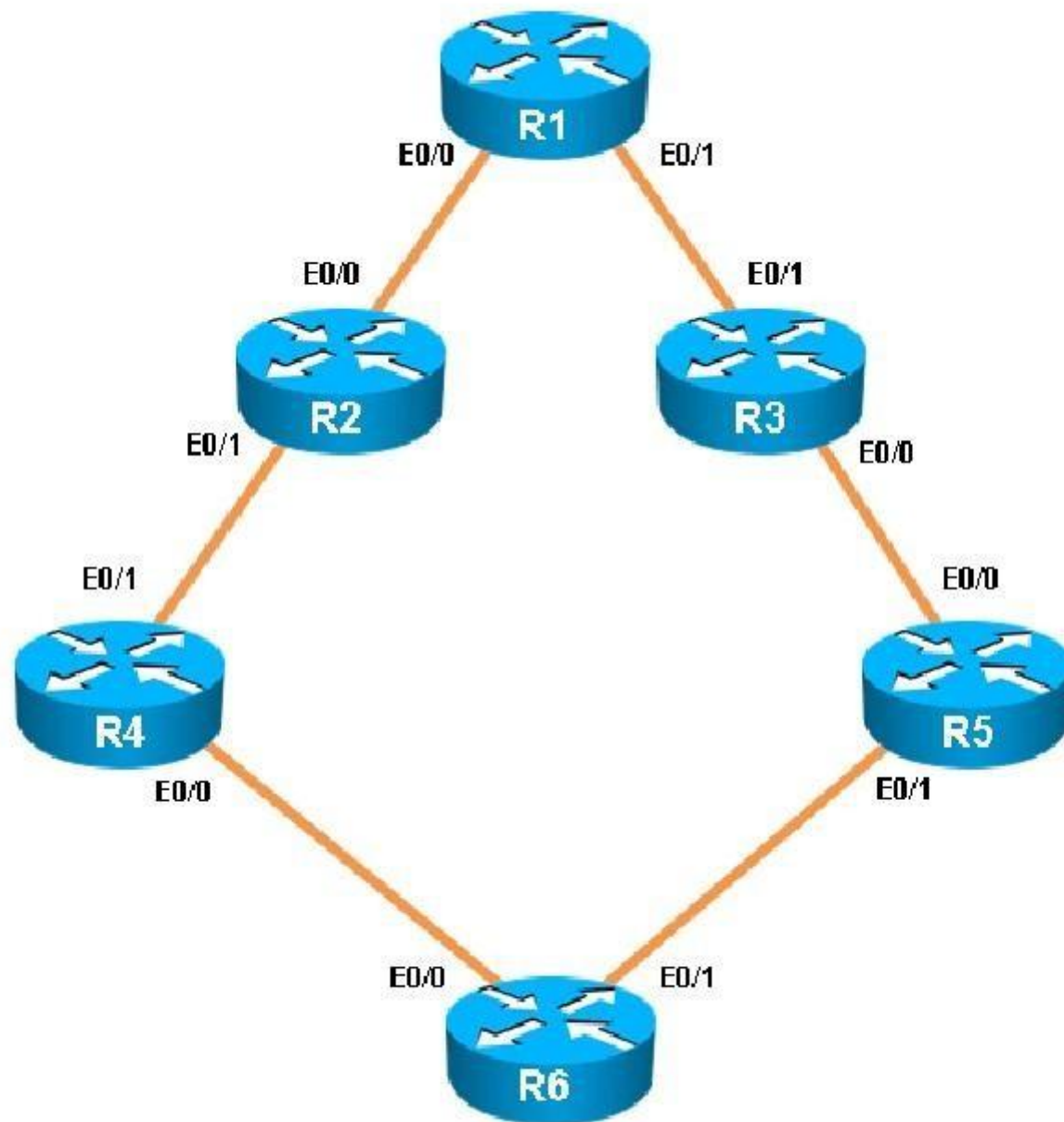
```
!  
access-list 1 permit 192.168.1.15  
access-list 1 permit 192.168.1.24  
access-list 1 permit 192.168.1.17  
access-list 1 permit 192.168.1.20  
access-list 2 permit 192.168.47.1  
access-list 2 permit 192.168.13.1  
access-list 2 permit 192.168.12.1  
access-list 2 deny 150.1.1.1  
access-list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

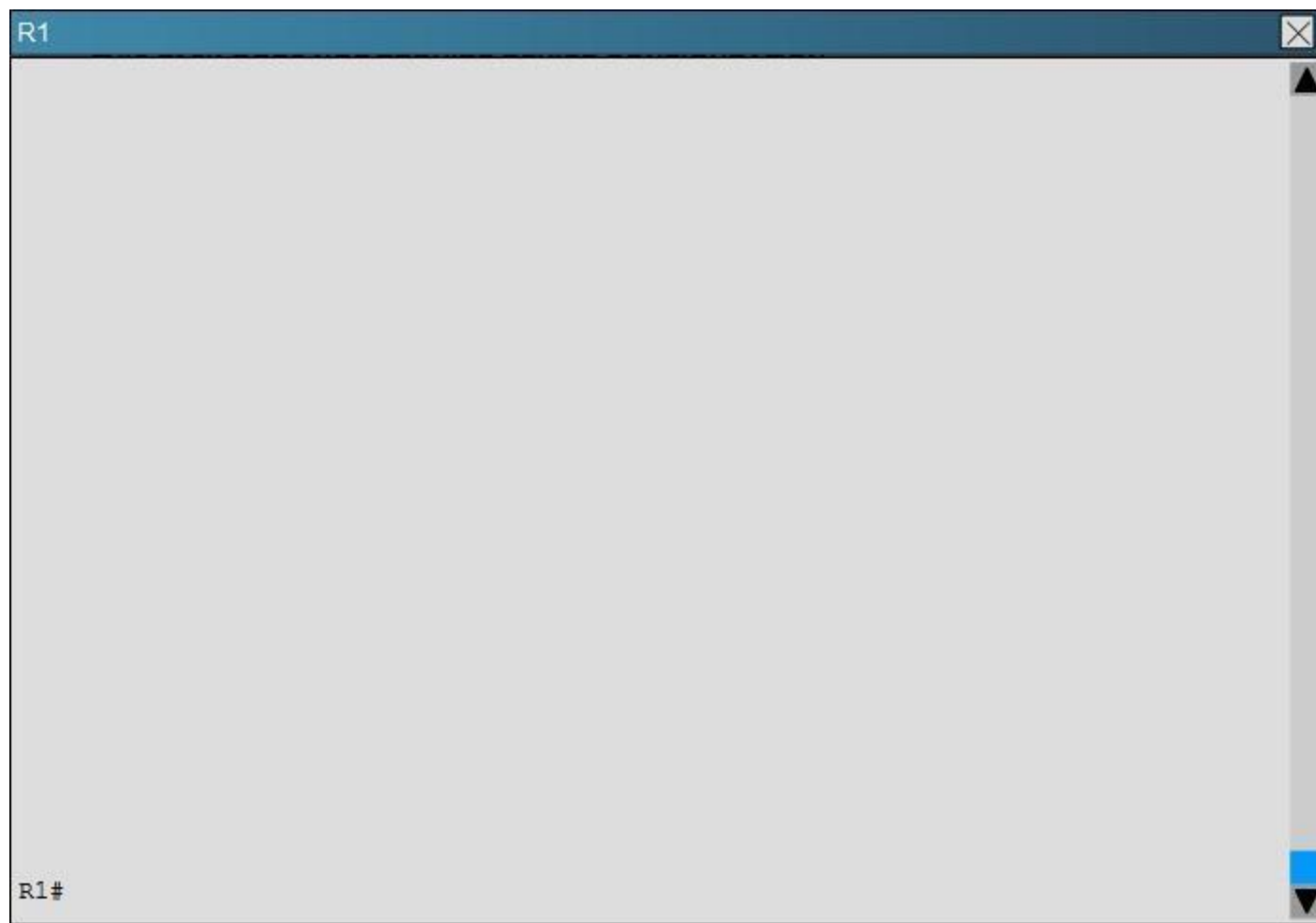
QUESTION 12

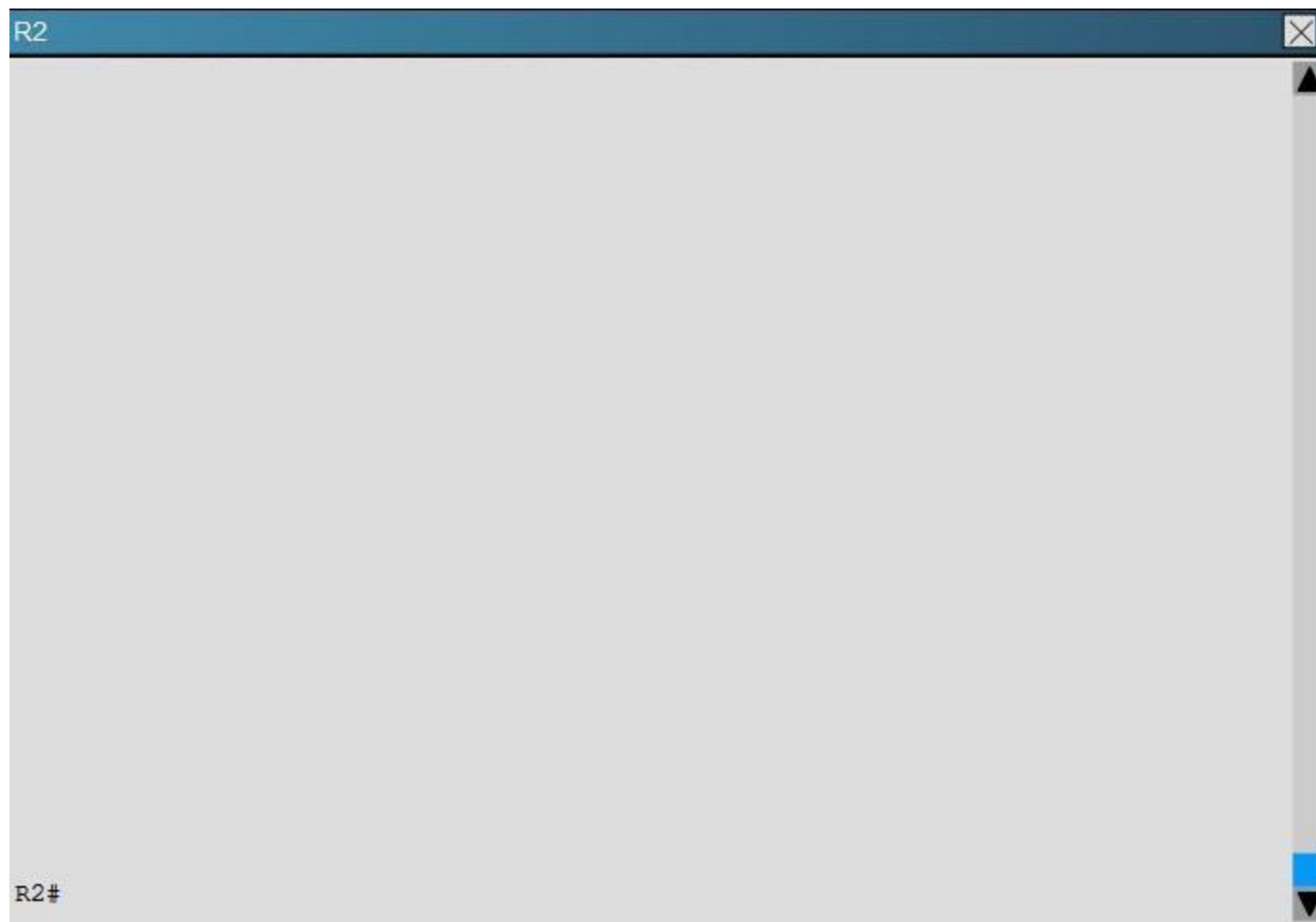
Scenario:

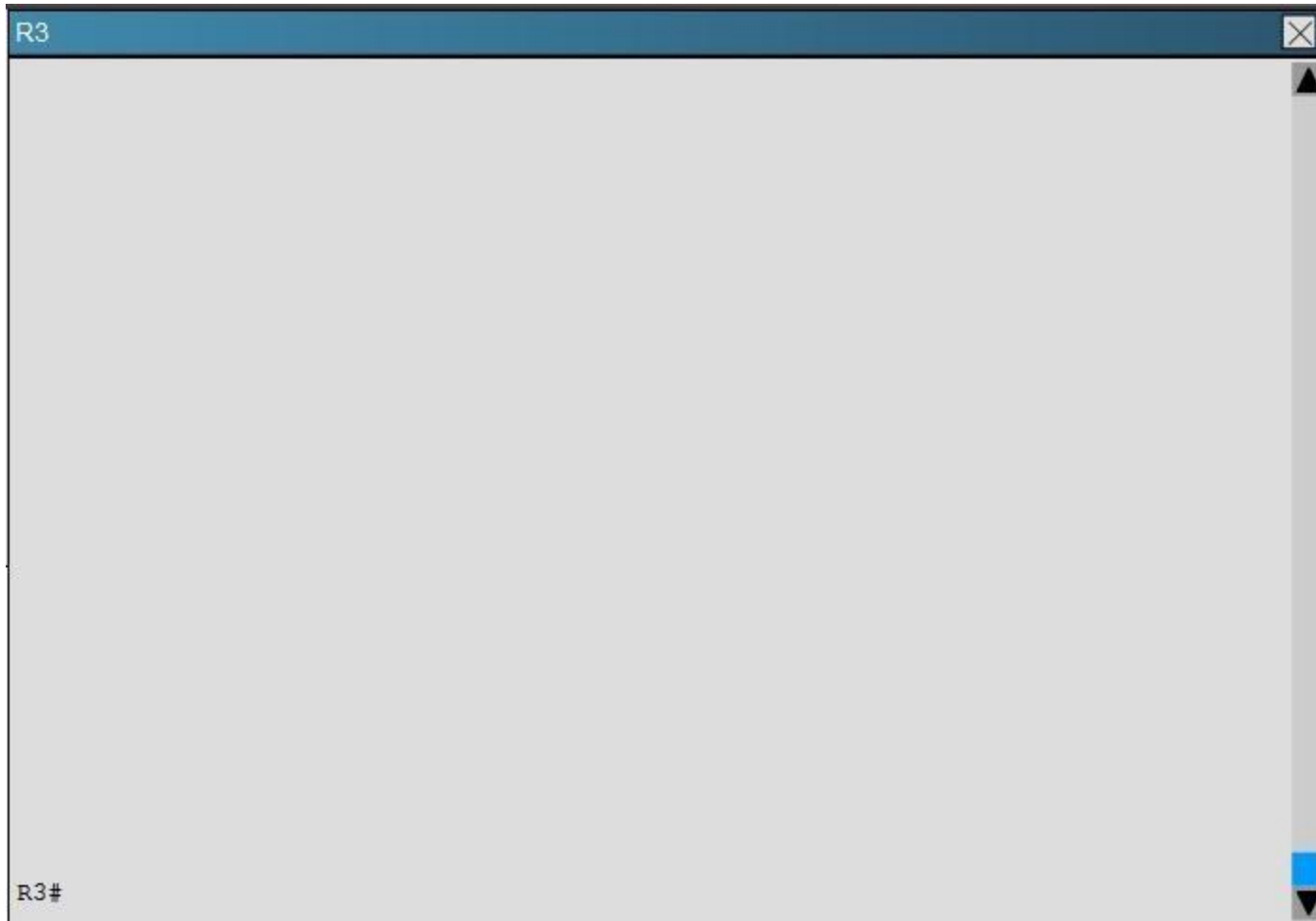
You have been brought in to troubleshoot an EIGRP network. You have resolved the initial issue between routers R2 and R4, but another issue remains. You are to locate the problem and suggest solution to resolve the issue.

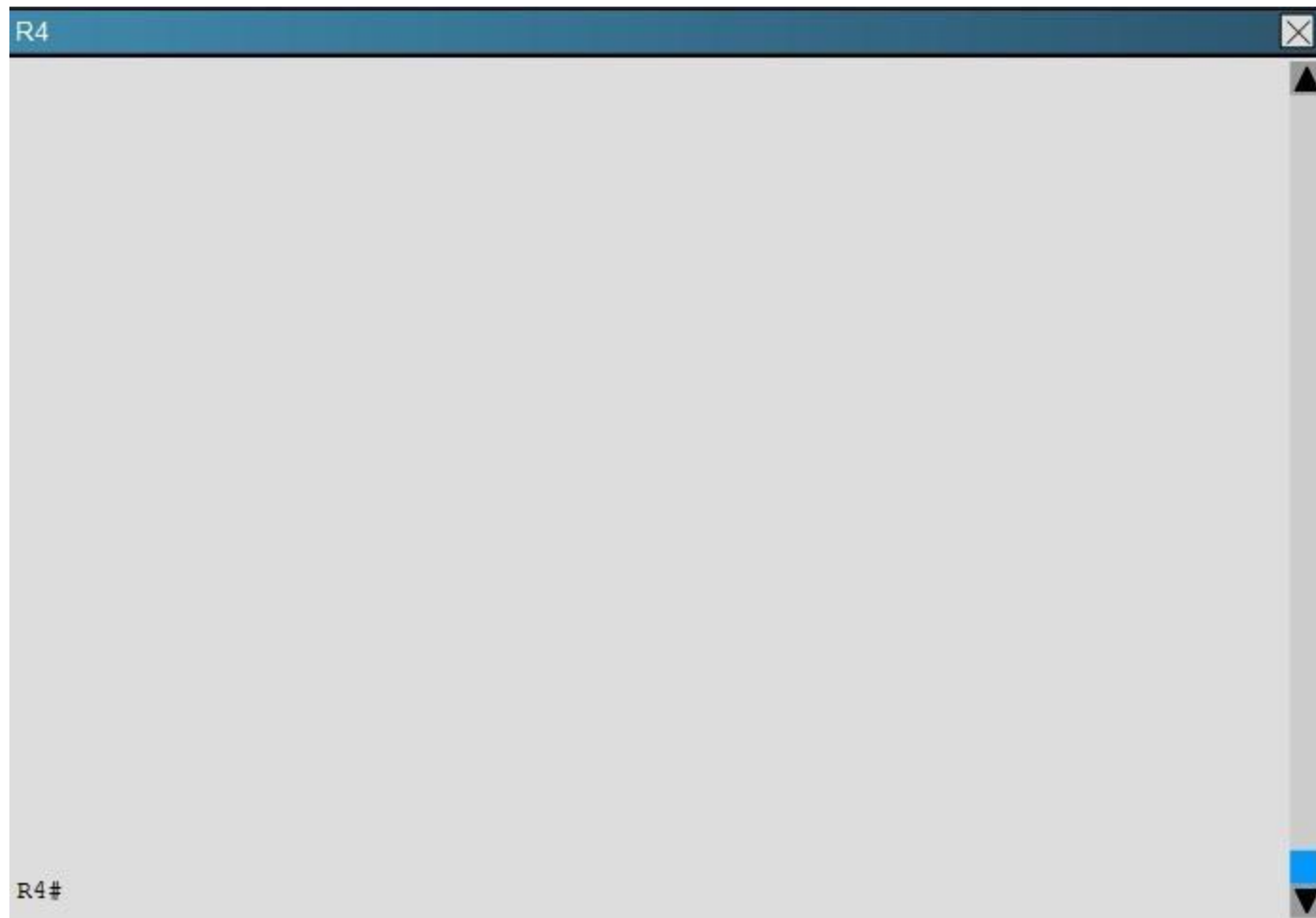
The customer has disabled access to the show running-config command.

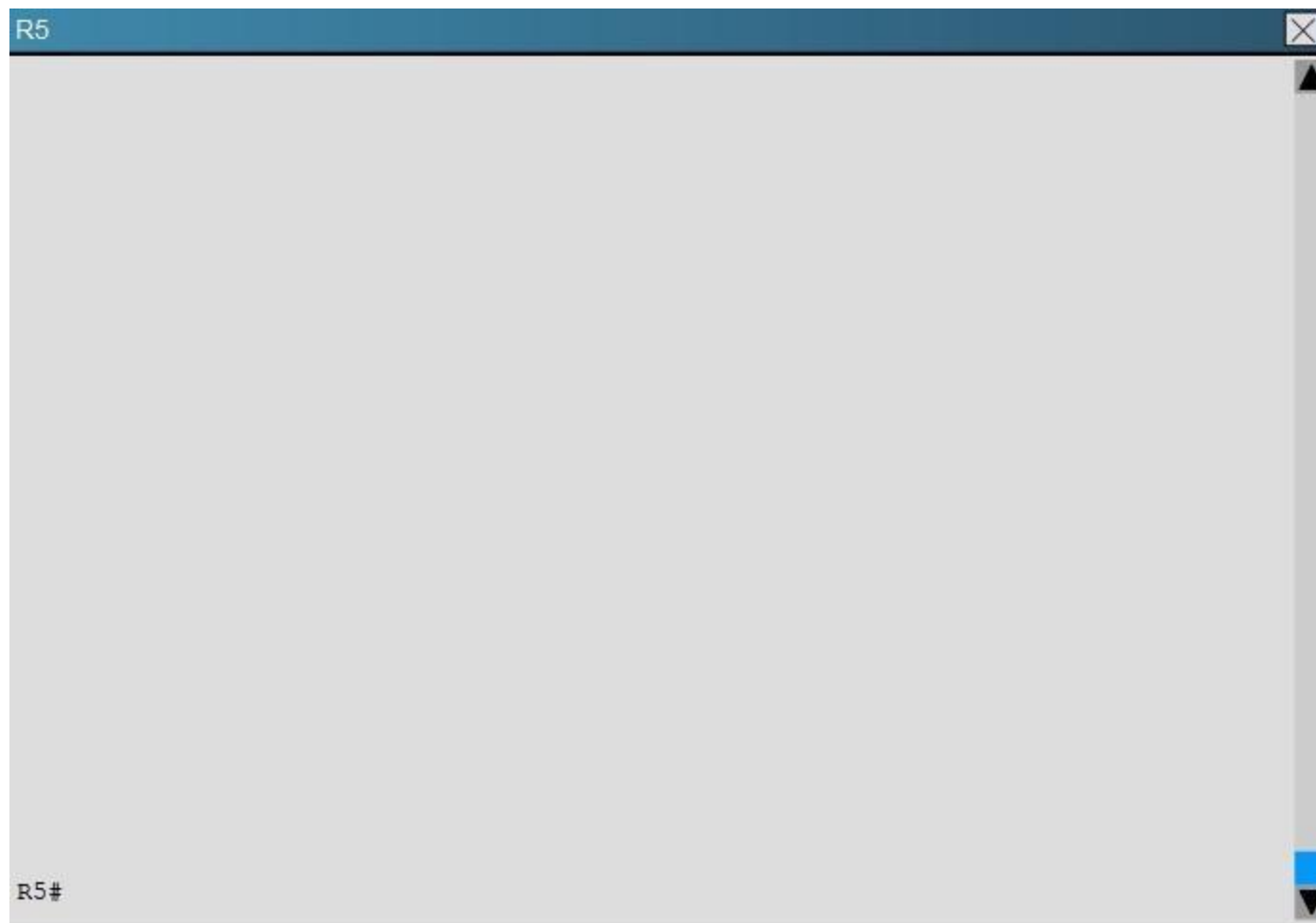


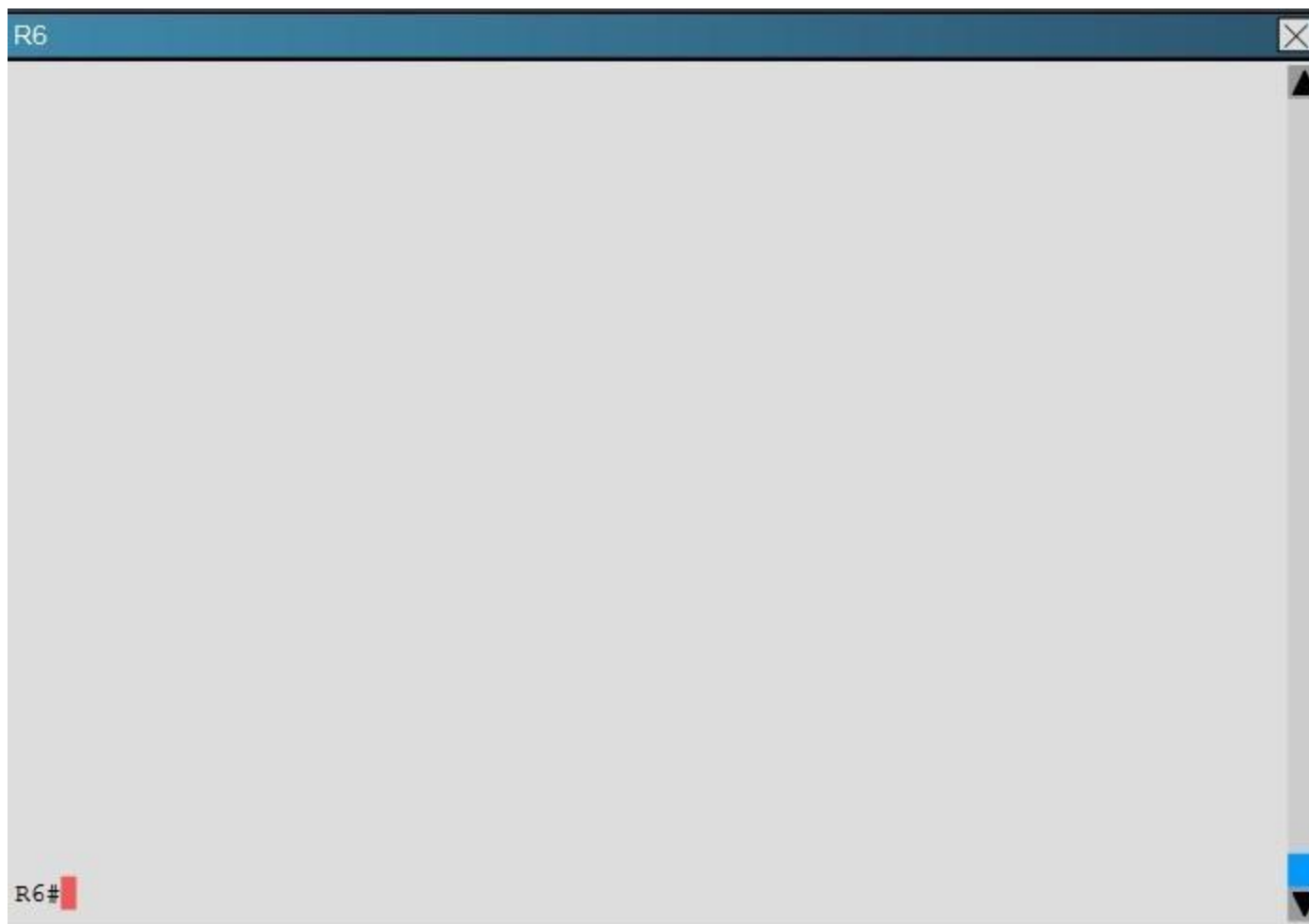












The network segment between R2 and R4 has become disconnected from the remainder of the network. How should this issue be resolved?

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

Correct Answer: B

Section: Troubleshooting EIGRP

Explanation

Explanation/Reference:

Explanation:

When issuing the "show ip eigrp neighbor" command (which is about the only command that it lets you do in this question) you will see that all other routers are configured for EIGRP AS 1. However, the 192.168.24.0 network between R2 and R4 is incorrectly configured for EIGRP AS 100:

```
R4
R4#sho ip eiq neighbors
R4#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                Interface      Hold Uptime    SRTT    RTO    Q
Seq                                     (sec)         (ms)         Cnt
Num
1   192.168.46.6            Et0/0         14 00:36:53    5     100    0
17
EIGRP-IPv4 Neighbors for AS(100)
H   Address                Interface      Hold Uptime    SRTT    RTO    Q
Seq                                     (sec)         (ms)         Cnt
Num
0   192.168.24.2            Et0/1         14 00:32:38    9     100    0
1
R4#
R4#
```

```

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

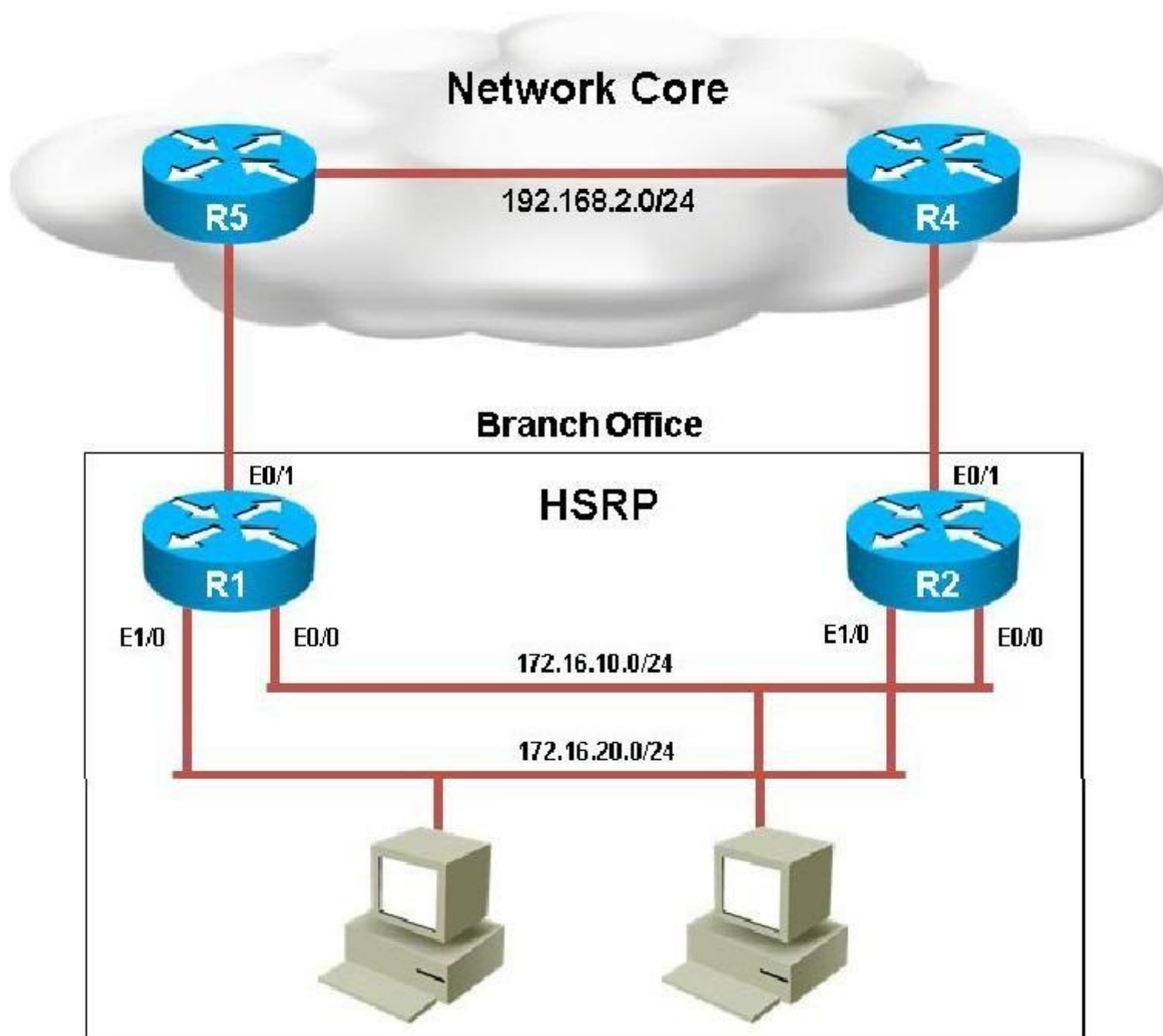
```

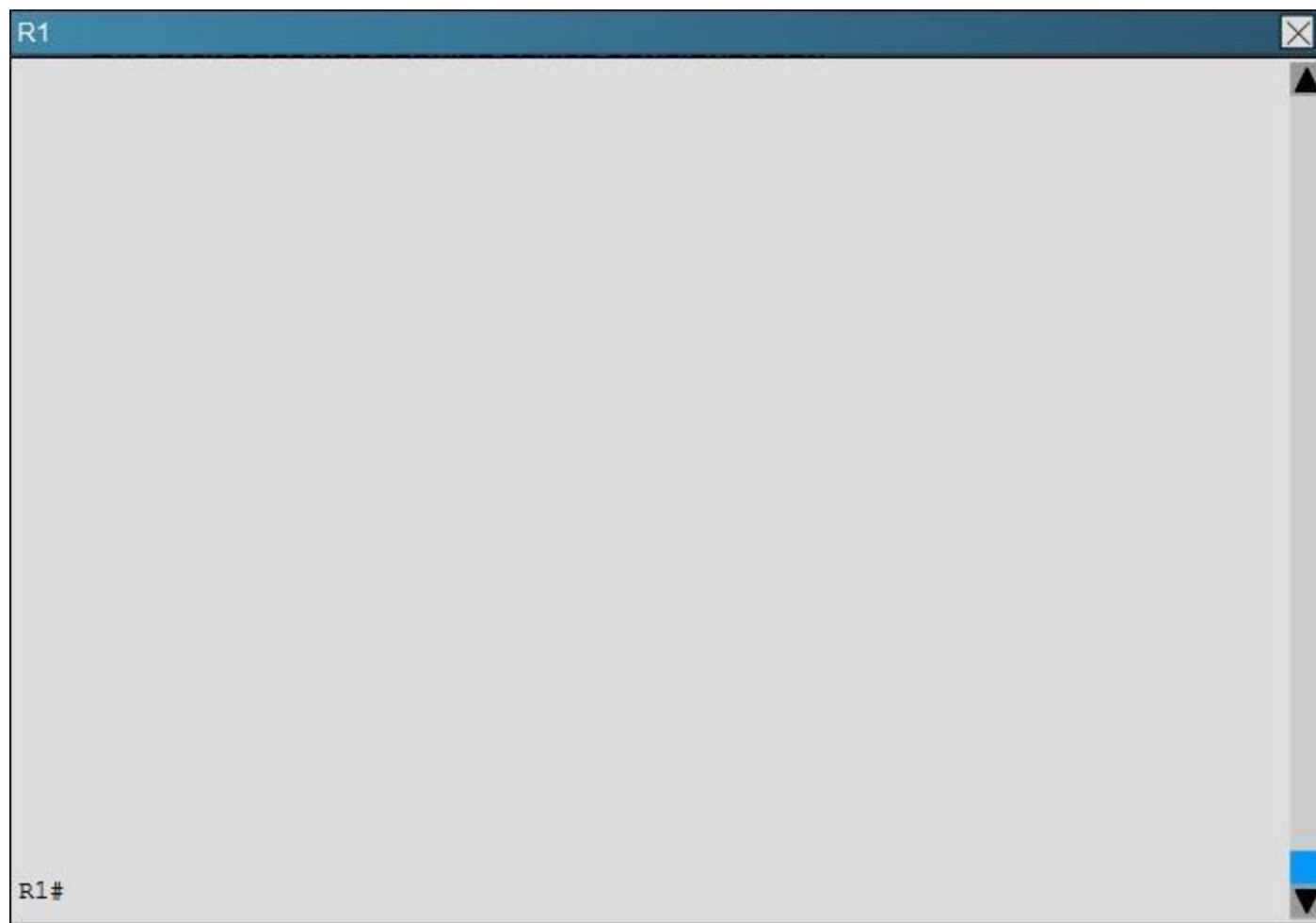
Topic 4, Troubleshooting HSRP

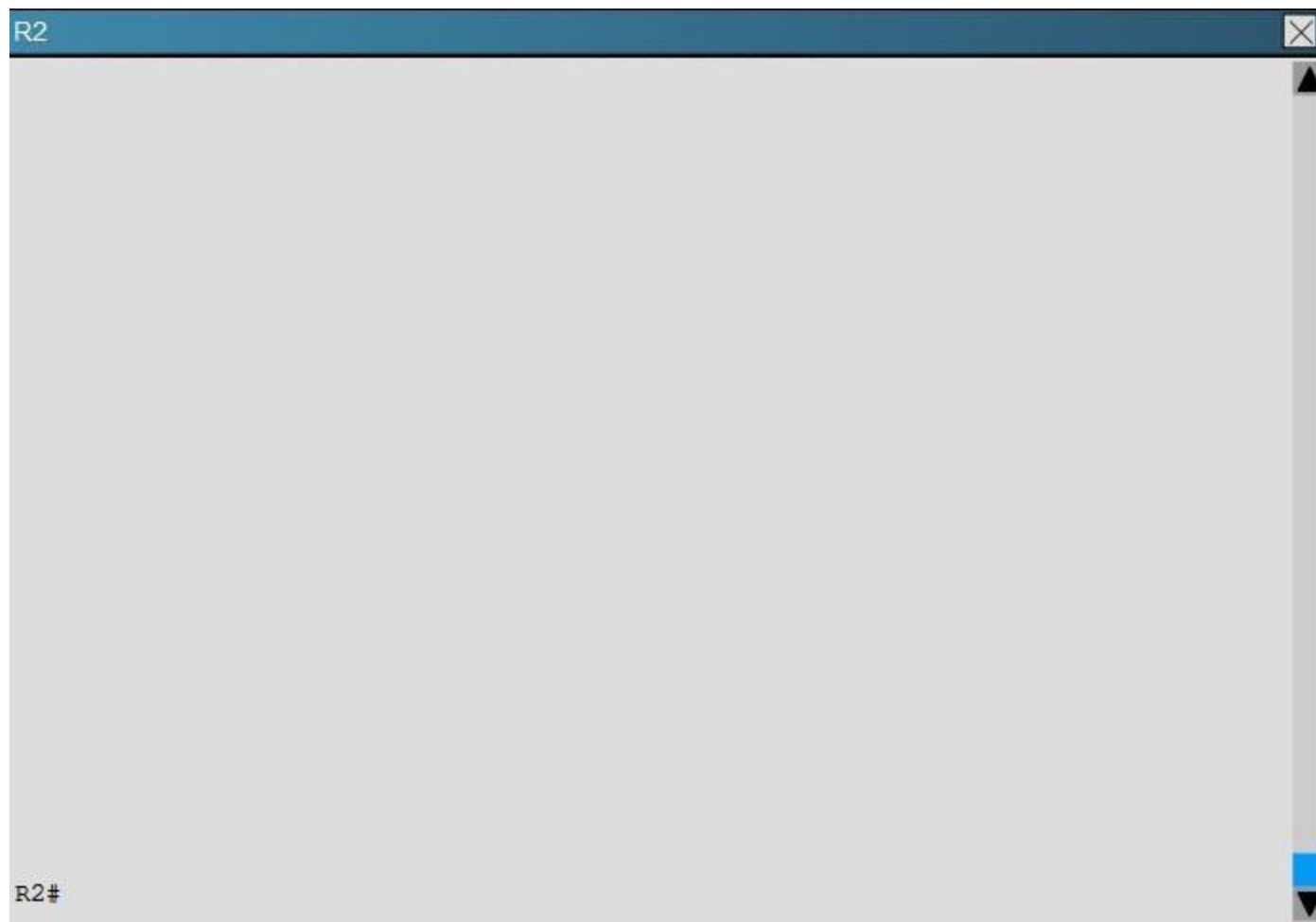
QUESTION 13

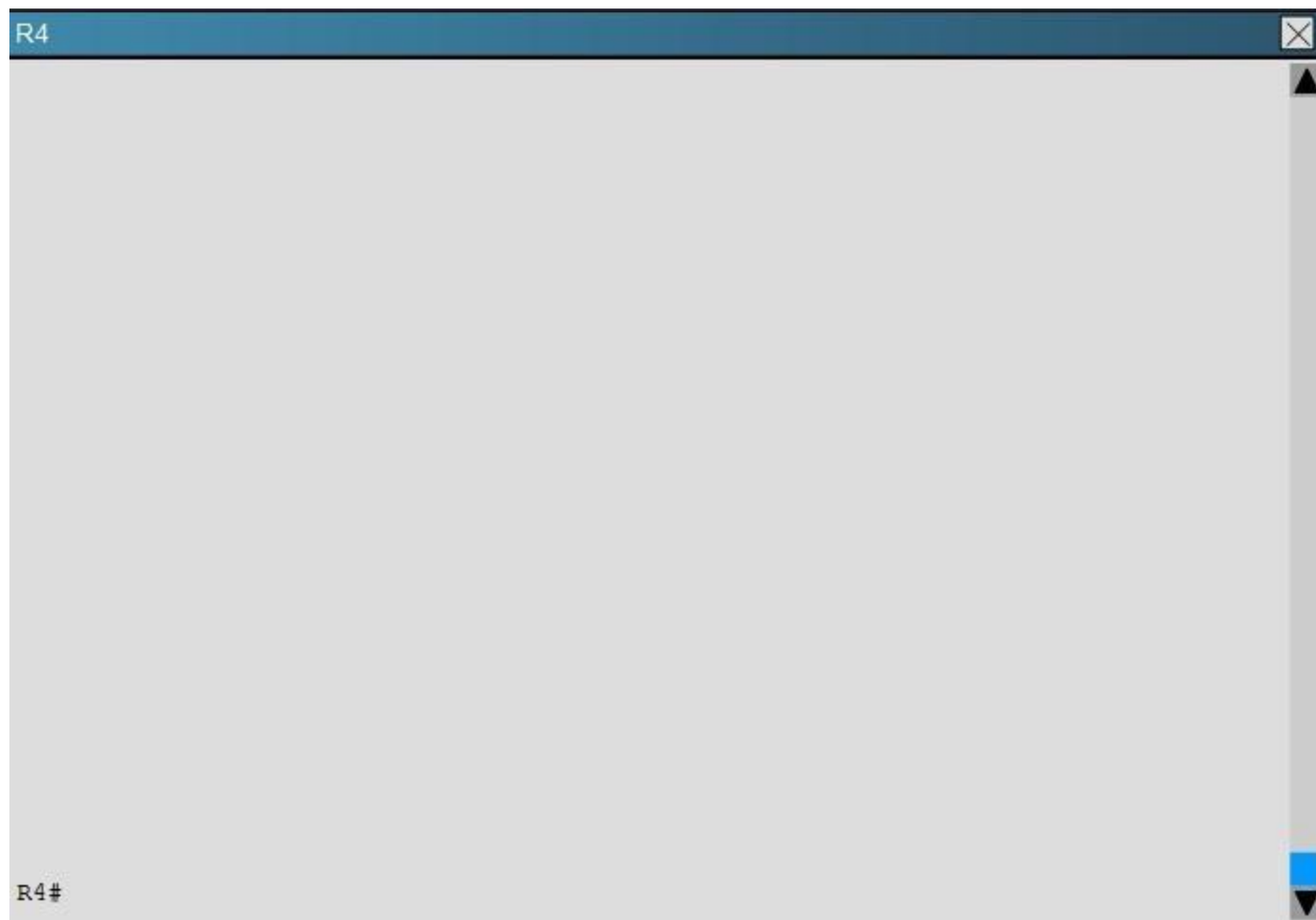
Scenario:

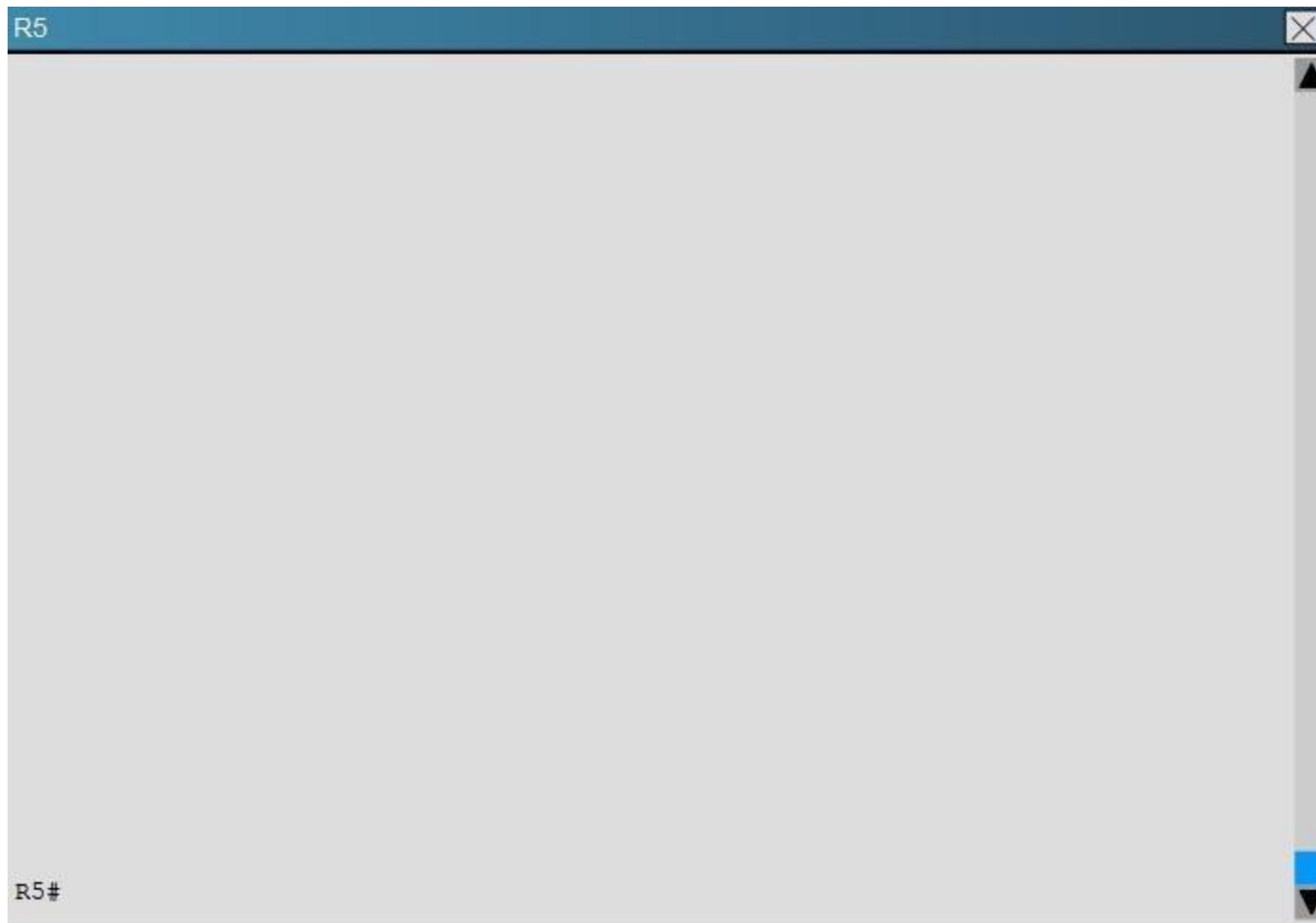
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.











You have received notification from network monitoring system that link between R1 and R5 is down and you noticed that the active router for HSRP group 1 has not failed over to the standby router for group 1. You are required to troubleshoot and identify the issue.

- A. There is an HSRP group track command misconfiguration
- B. There is an HSRP group priority misconfiguration
- C. There is an HSRP authentication misconfiguration
- D. There is an HSRP group number mismatch

E. This is not an HSRP issue; this is routing issue.

Correct Answer: A

Section: Troubleshooting HSRP

Explanation

Explanation/Reference:

Explanation:

When looking at the HSRP configuration of R1, we see that tracking has been enabled, but that it is not tracking the link to R5, only the link to R2:

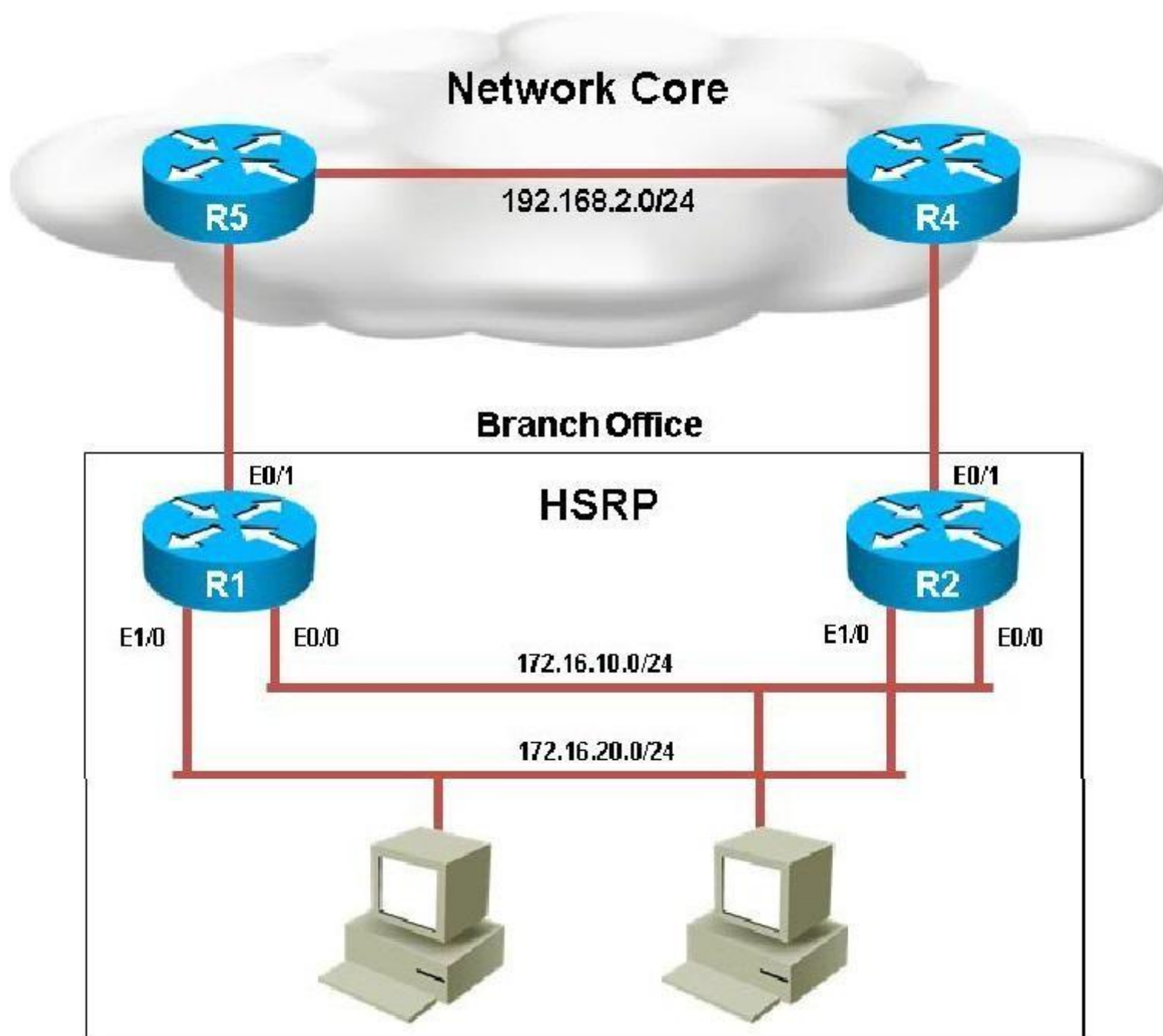
```
R1
!
track 1 interface Ethernet0/0 line-protocol
!
!
!
!
!
interface Ethernet0/0
  description connection to 172.16.10.0/24 network
  ip address 172.16.10.2 255.255.255.0
  standby 1 ip 172.16.10.254
  standby 1 priority 130
  standby 1 preempt delay reload 180
  standby 1 mac-address 4000.0000.0010
  standby 1 track 1 decrement 40
!
interface Ethernet0/1
```

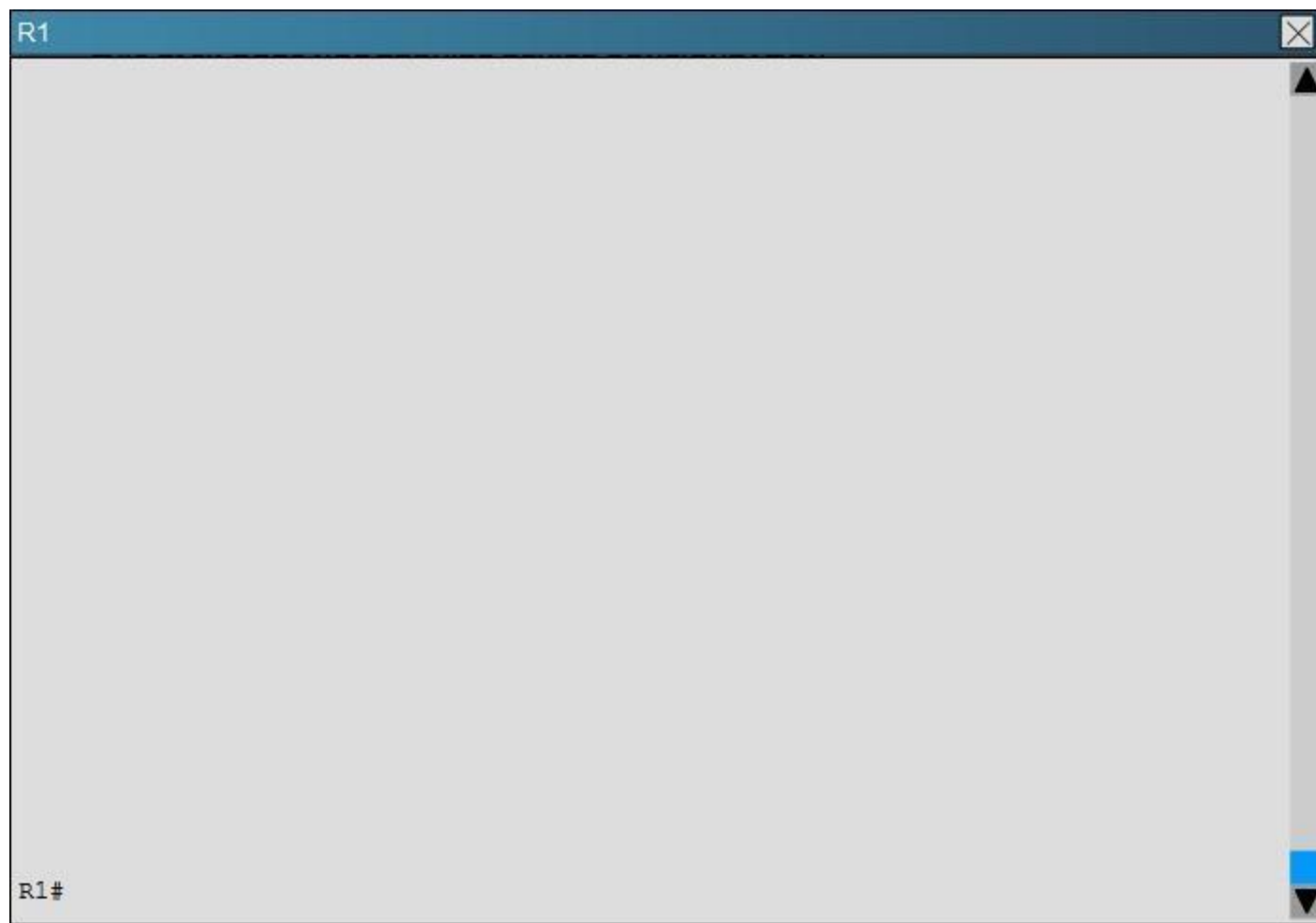
R1 should be tracking the Eth 0/1 link, not 0/0 to achieve the desired affect/

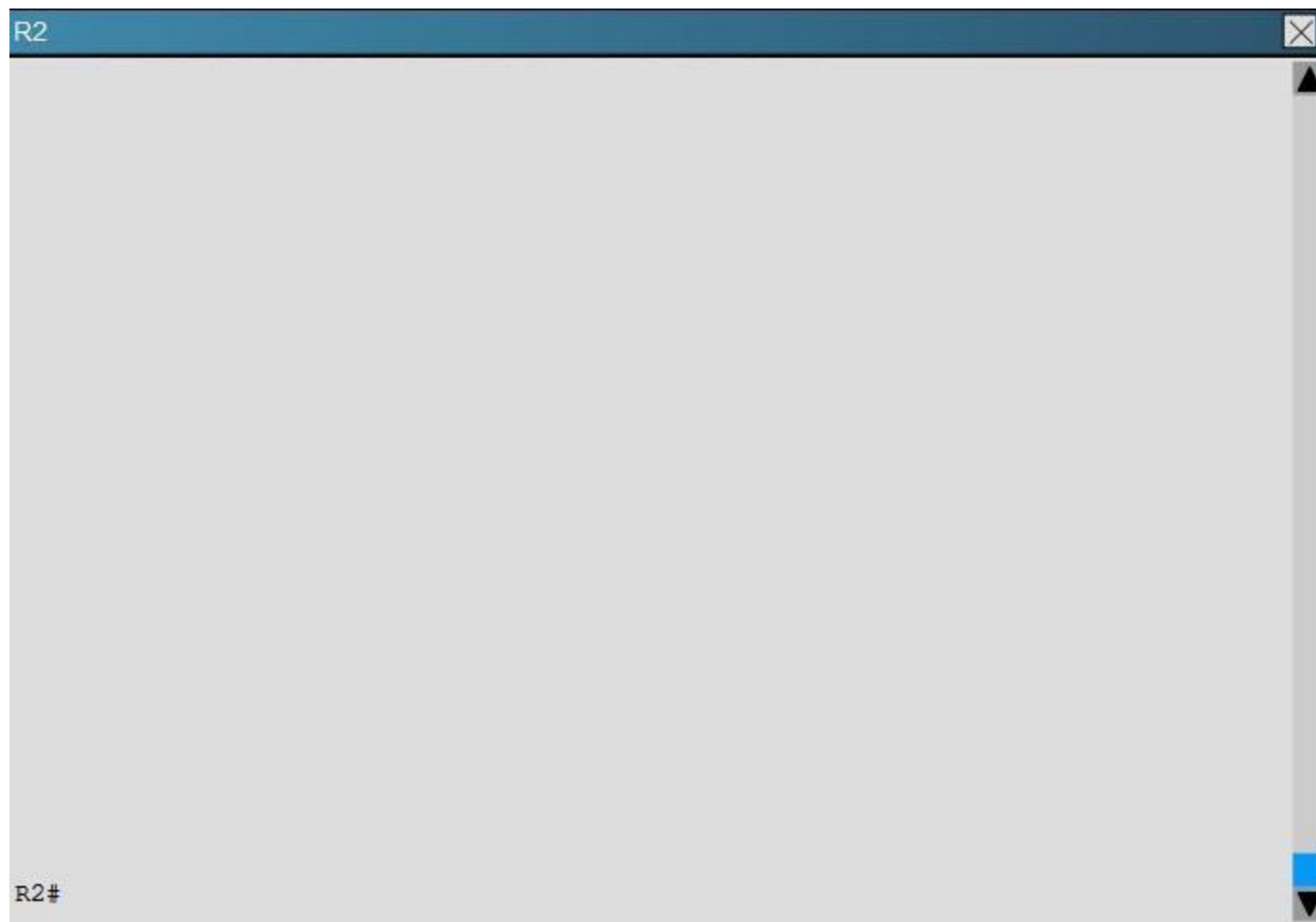
QUESTION 14

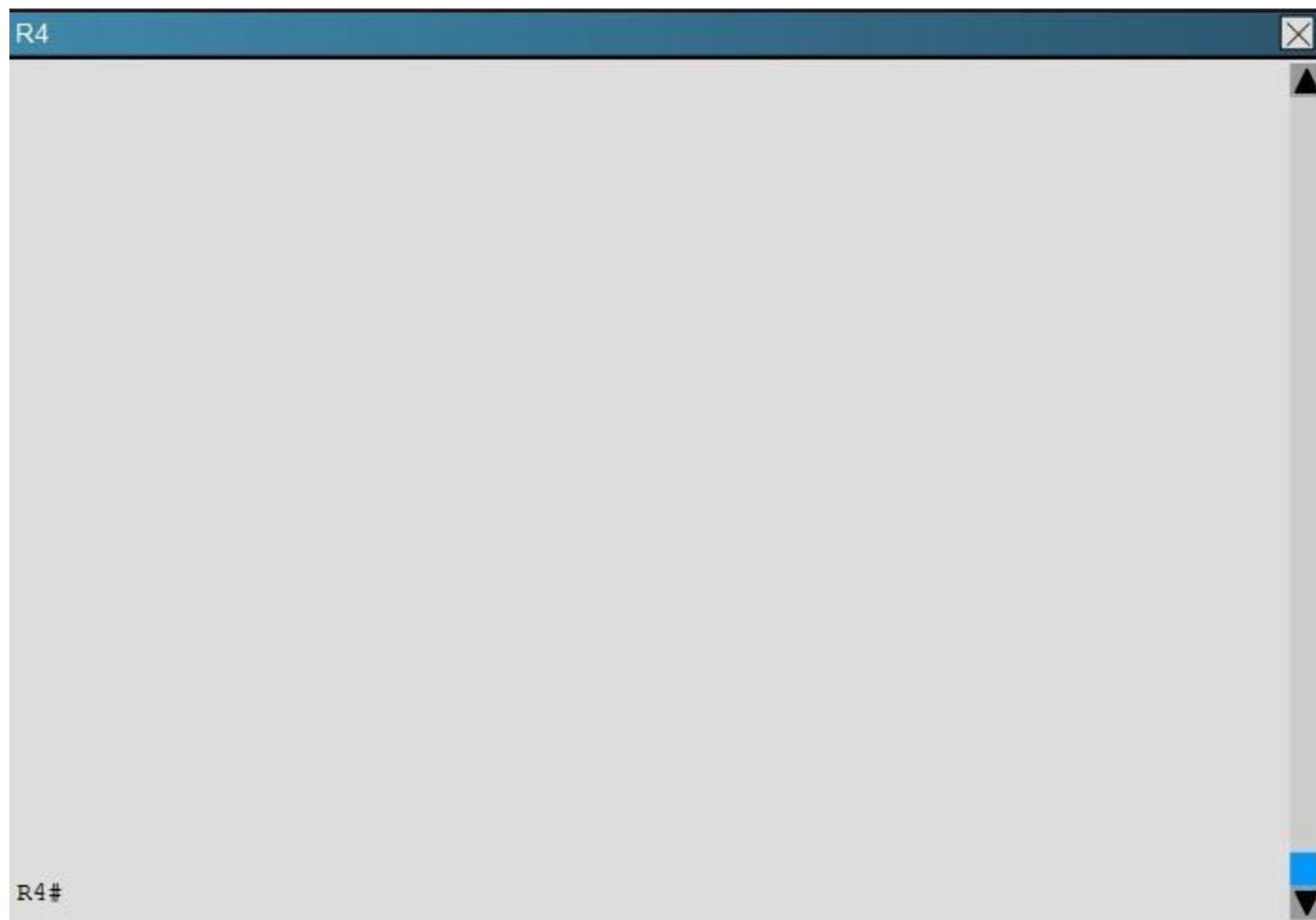
Scenario:

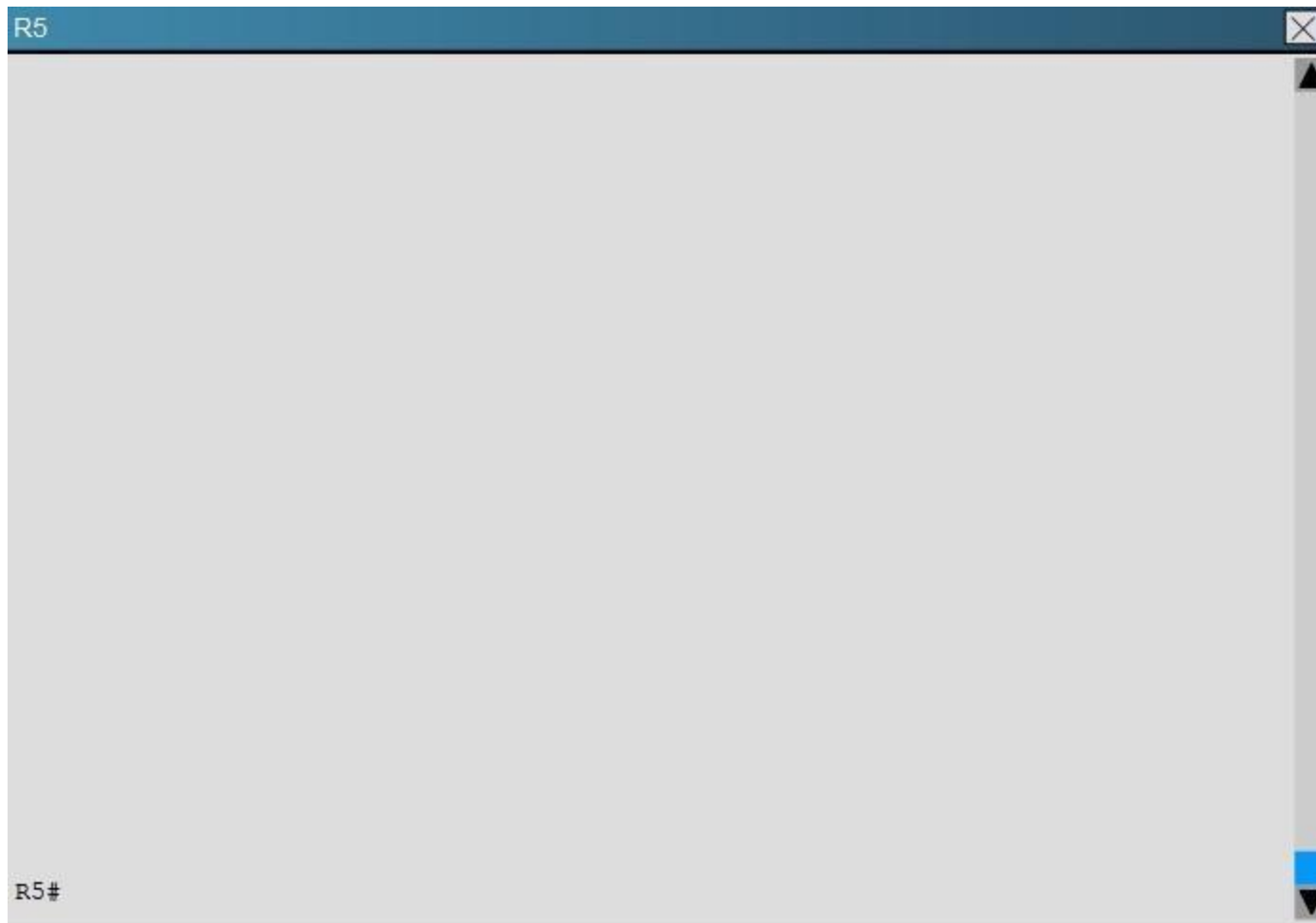
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.











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 pri130vIP 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

Correct Answer: E

Section: Troubleshooting HSRP

Explanation

Explanation/Reference:

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
```

!

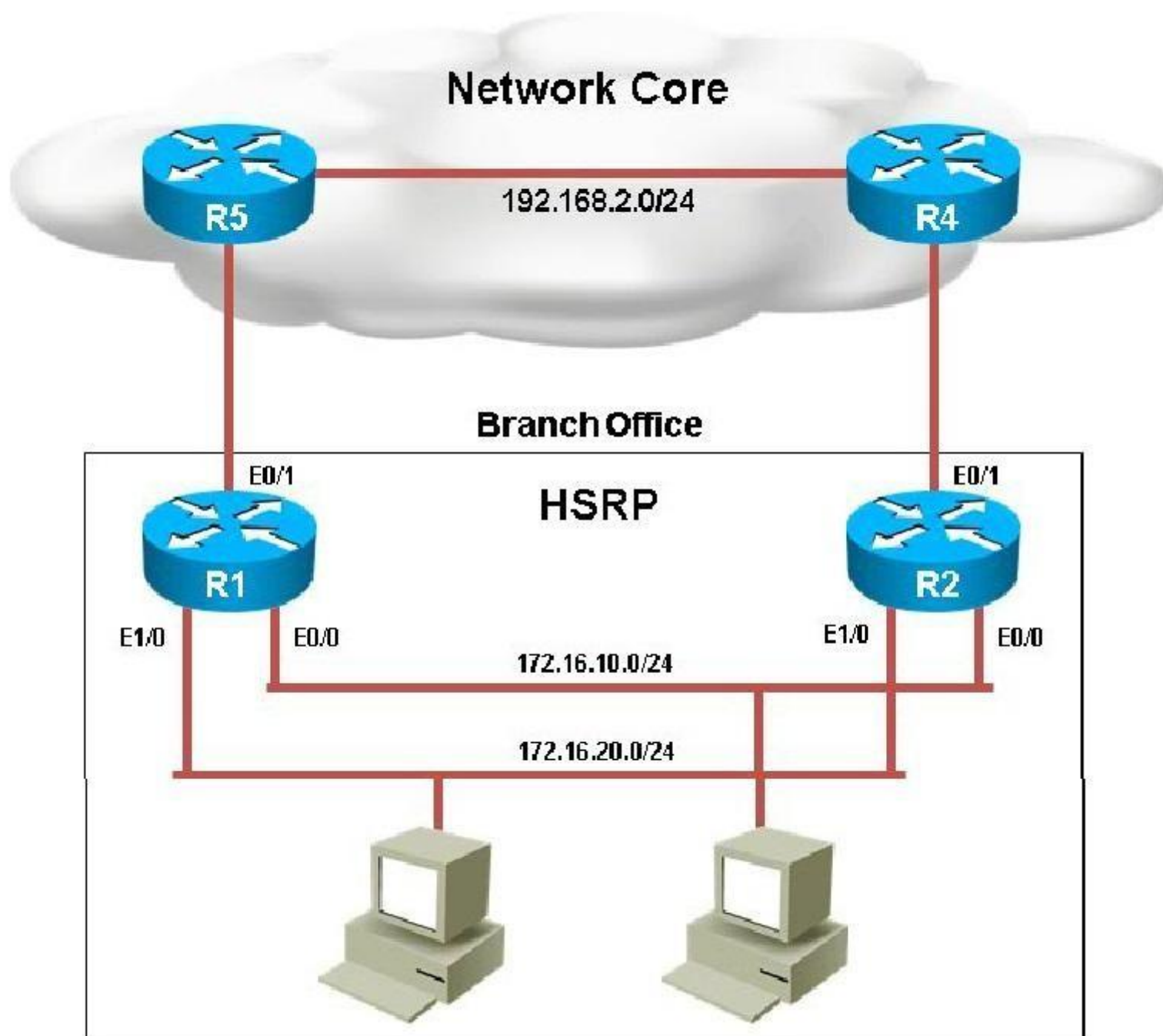
!

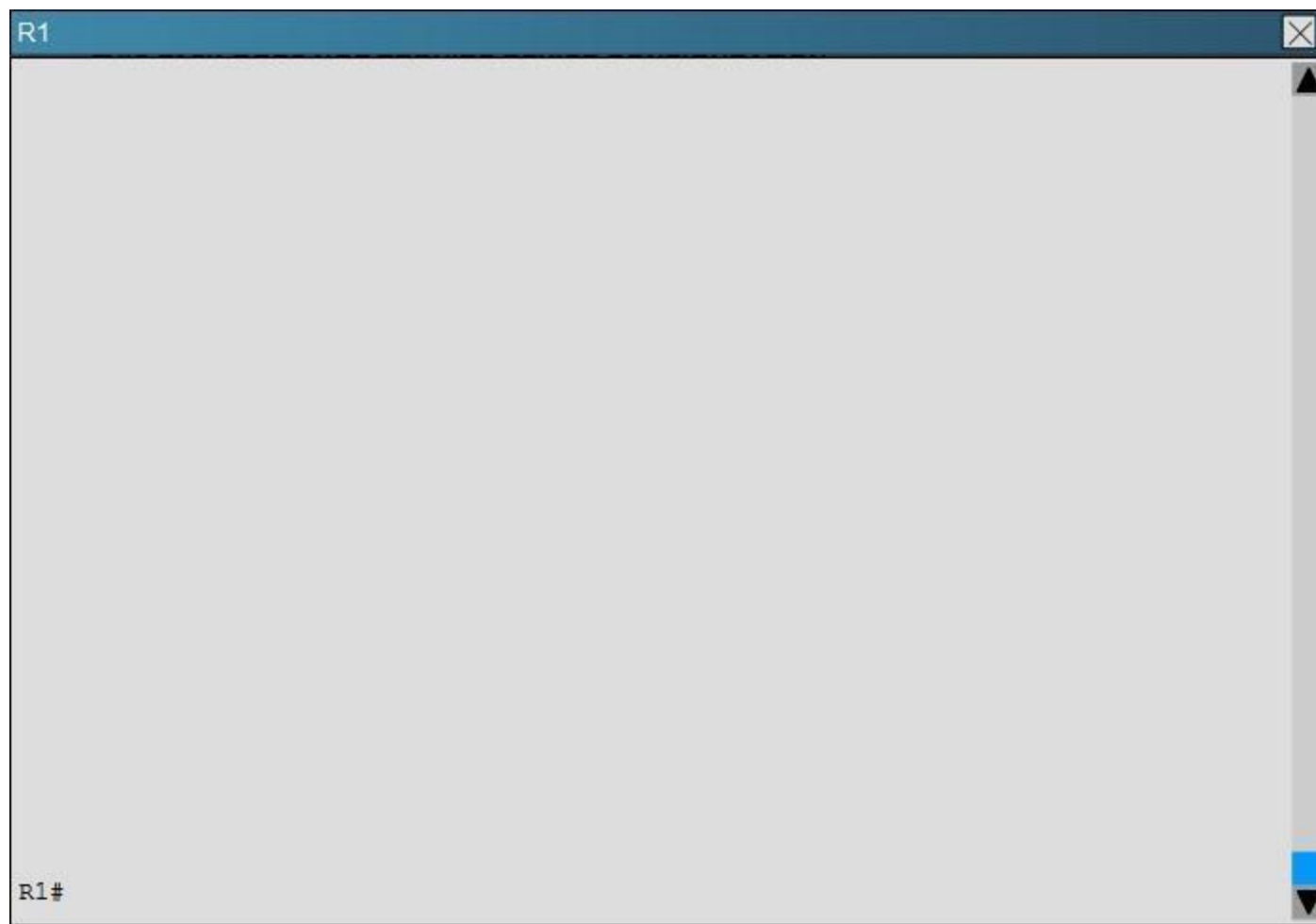
This access list is blocking all traffic to the 224.0.0.102 IP address, which is the multicast address used by HSRP.

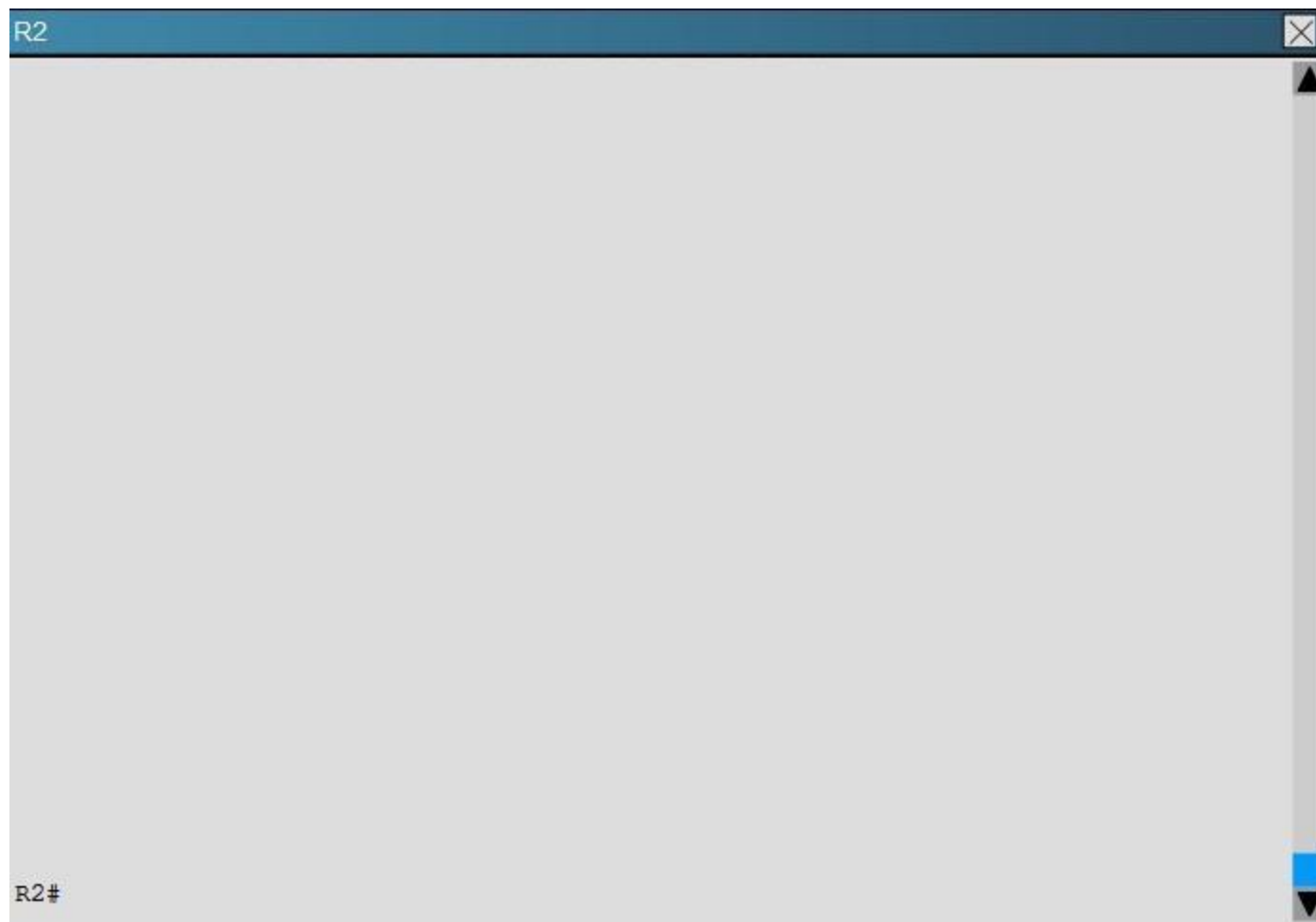
QUESTION 15

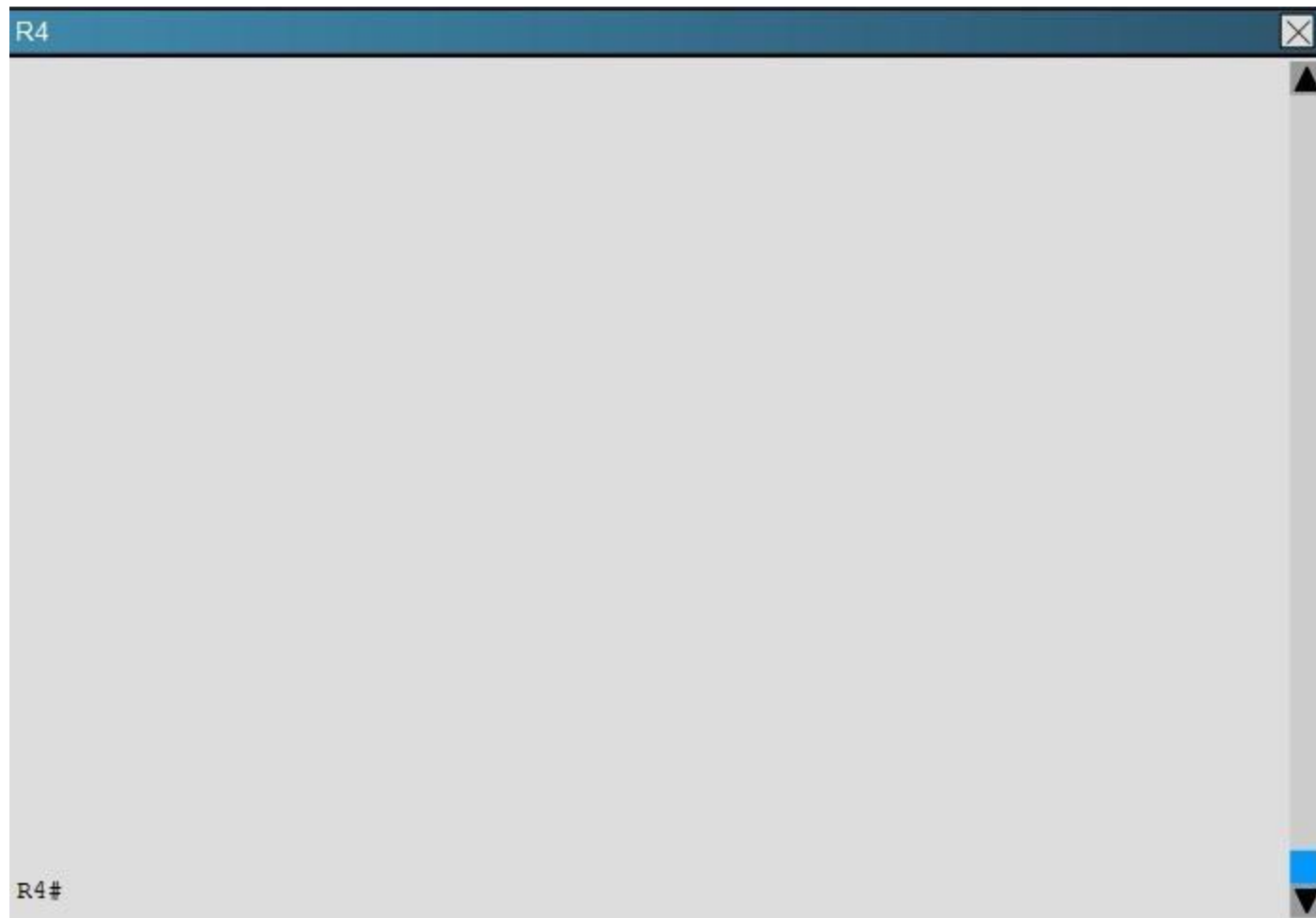
Scenario:

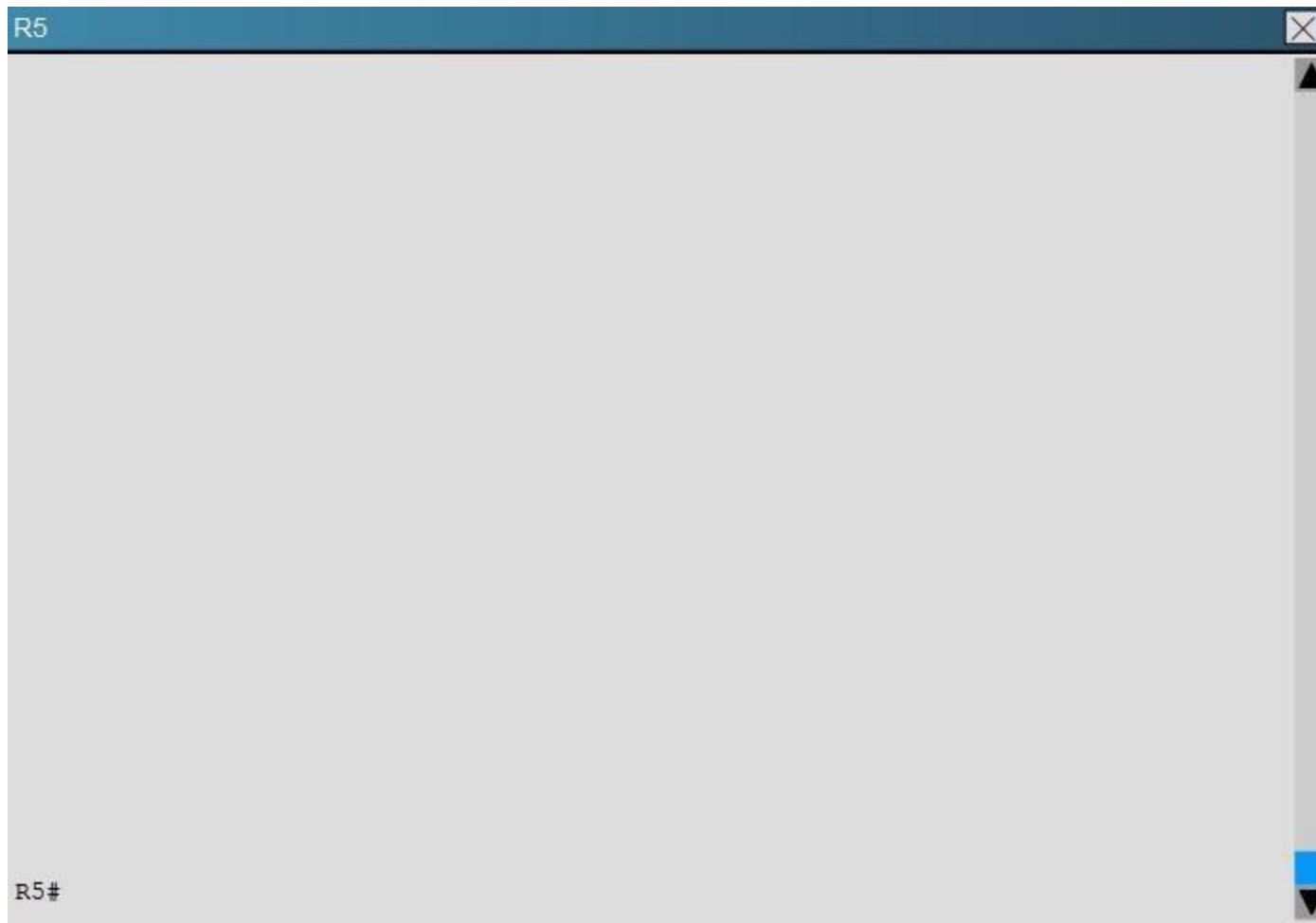
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.











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

- A. HSRP issue between R4 and R2
- B. This is an OSPF issue between R4 and R2
- C. This is a DHCP issue between R4 and R2
- D. The distribute-list configured on R4 is blocking route entries

E. The ACL configured on R4 is blocking inbound traffic on the interface connected to R2

Correct Answer: D

Section: Troubleshooting HSRP

Explanation

Explanation/Reference:

Explanation:

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

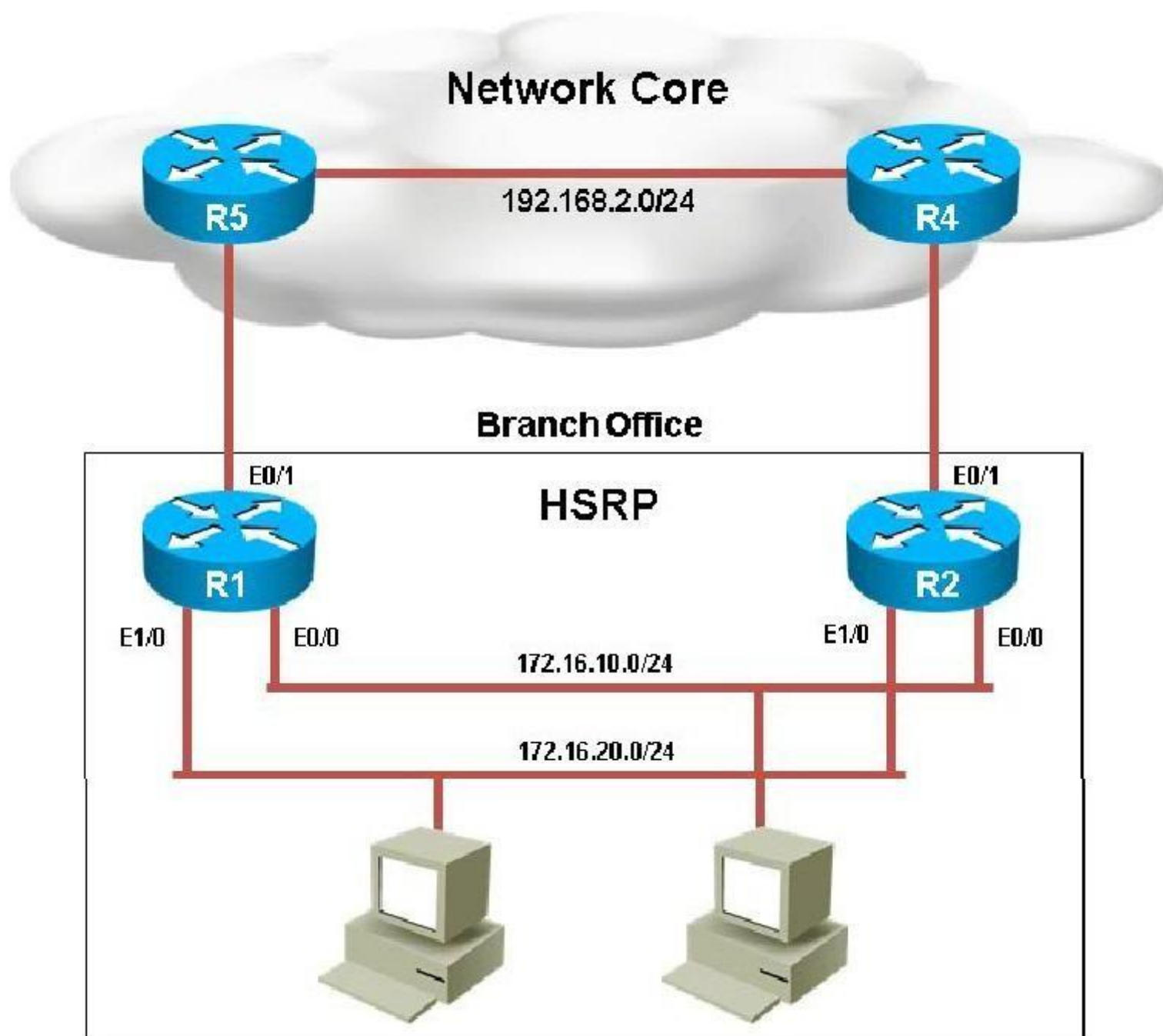
R4

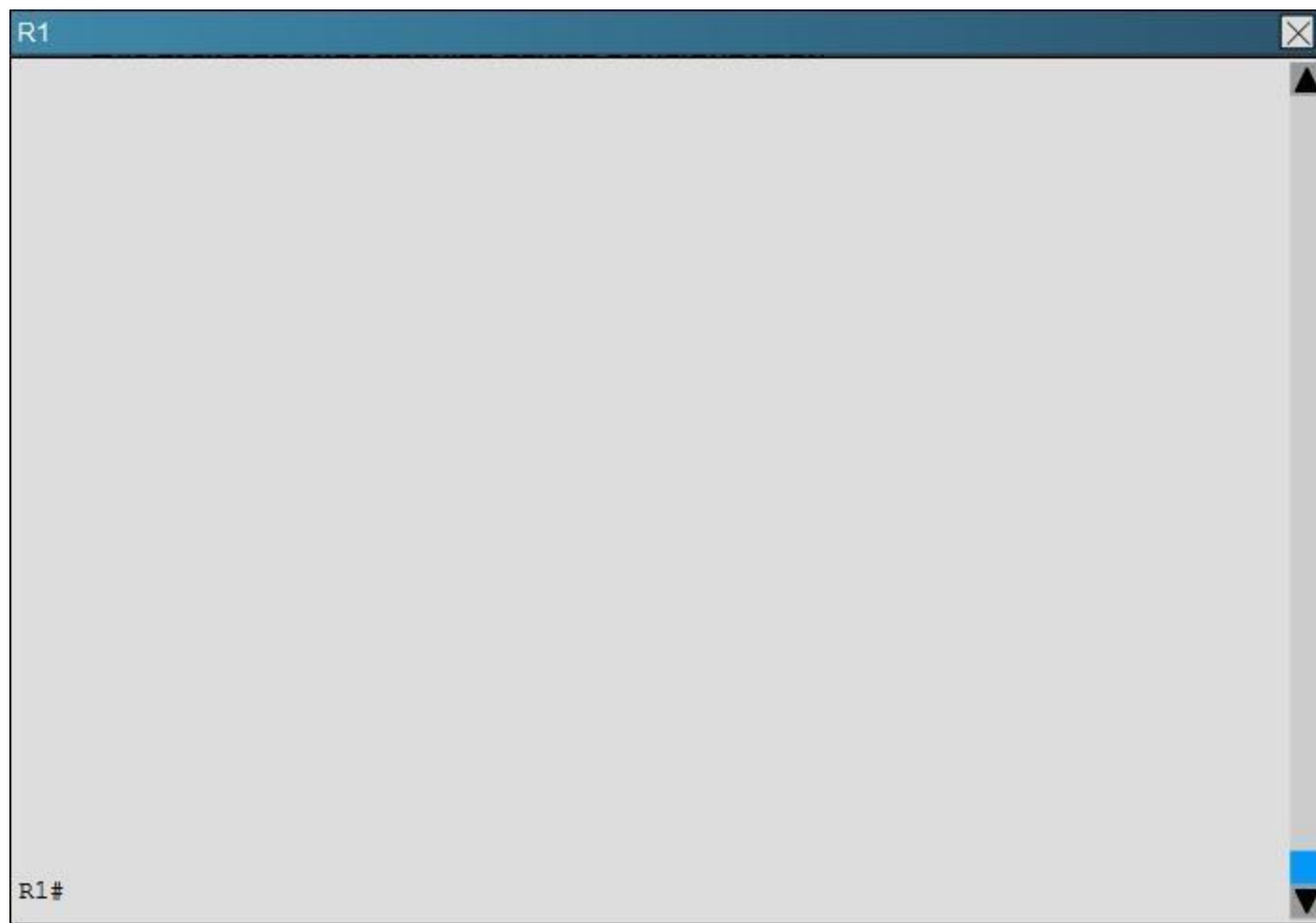
```
!  
router ospf 10  
  network 0.0.0.0 255.255.255.255 area 0  
  distribute-list 1 in  
!  
!  
!  
no ip http server  
!  
access-list 1 permit 172.18.30.0  
access-list 1 deny 172.16.20.0  
access-list 1 permit 172.18.20.0  
access-list 1 permit 172.18.10.0  
access-list 1 deny 172.16.10.0  
access-list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

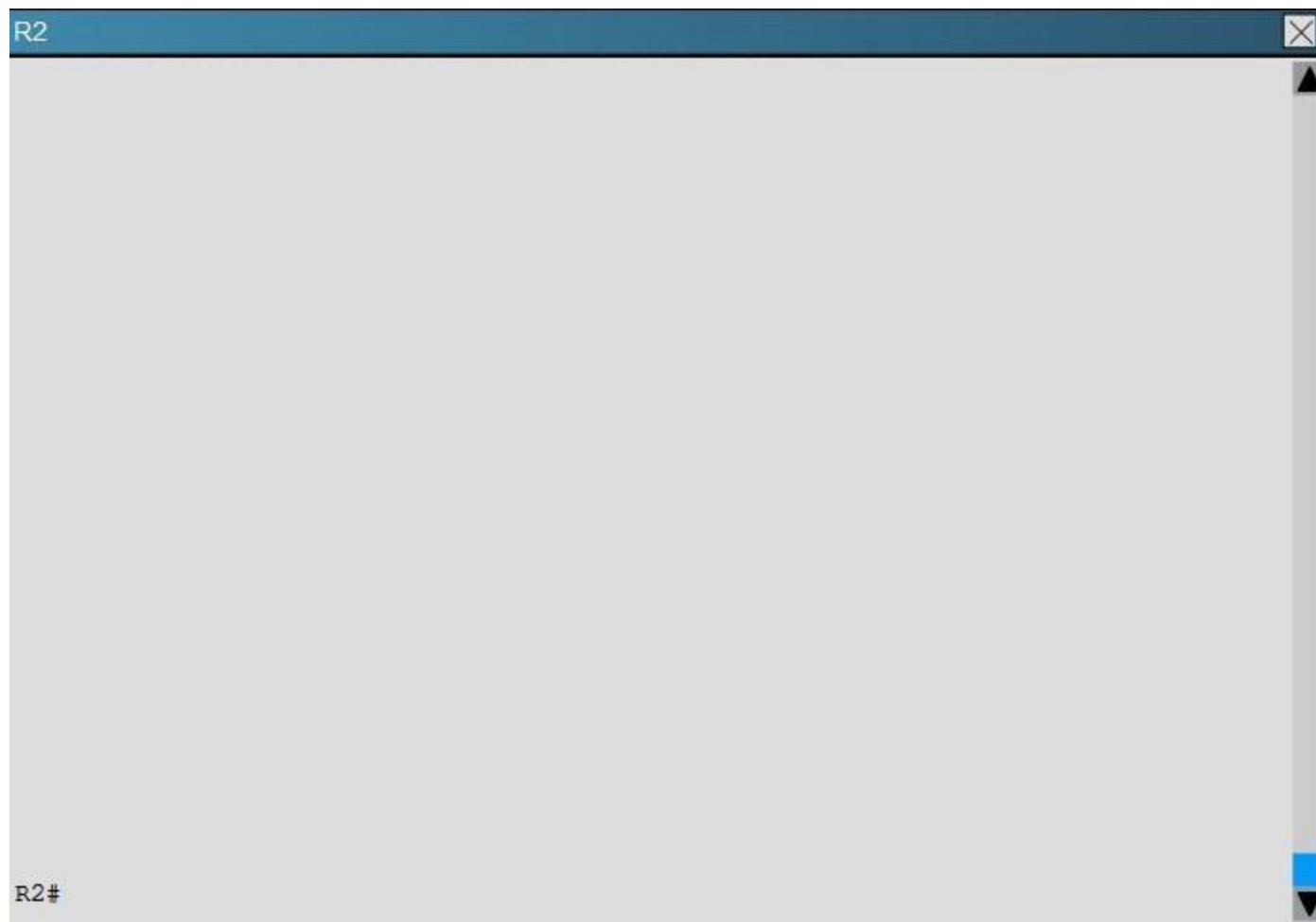
QUESTION 16

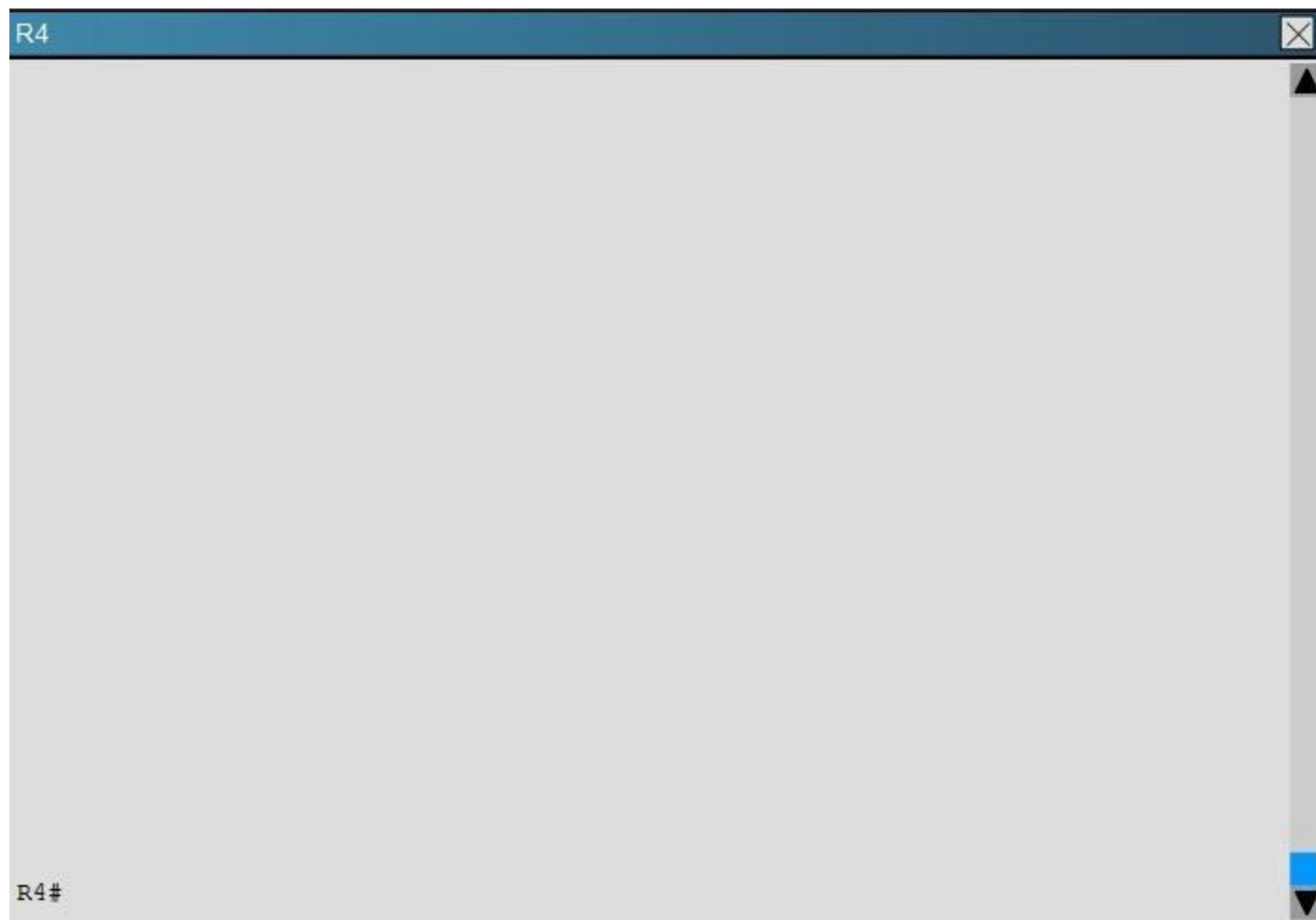
Scenario:

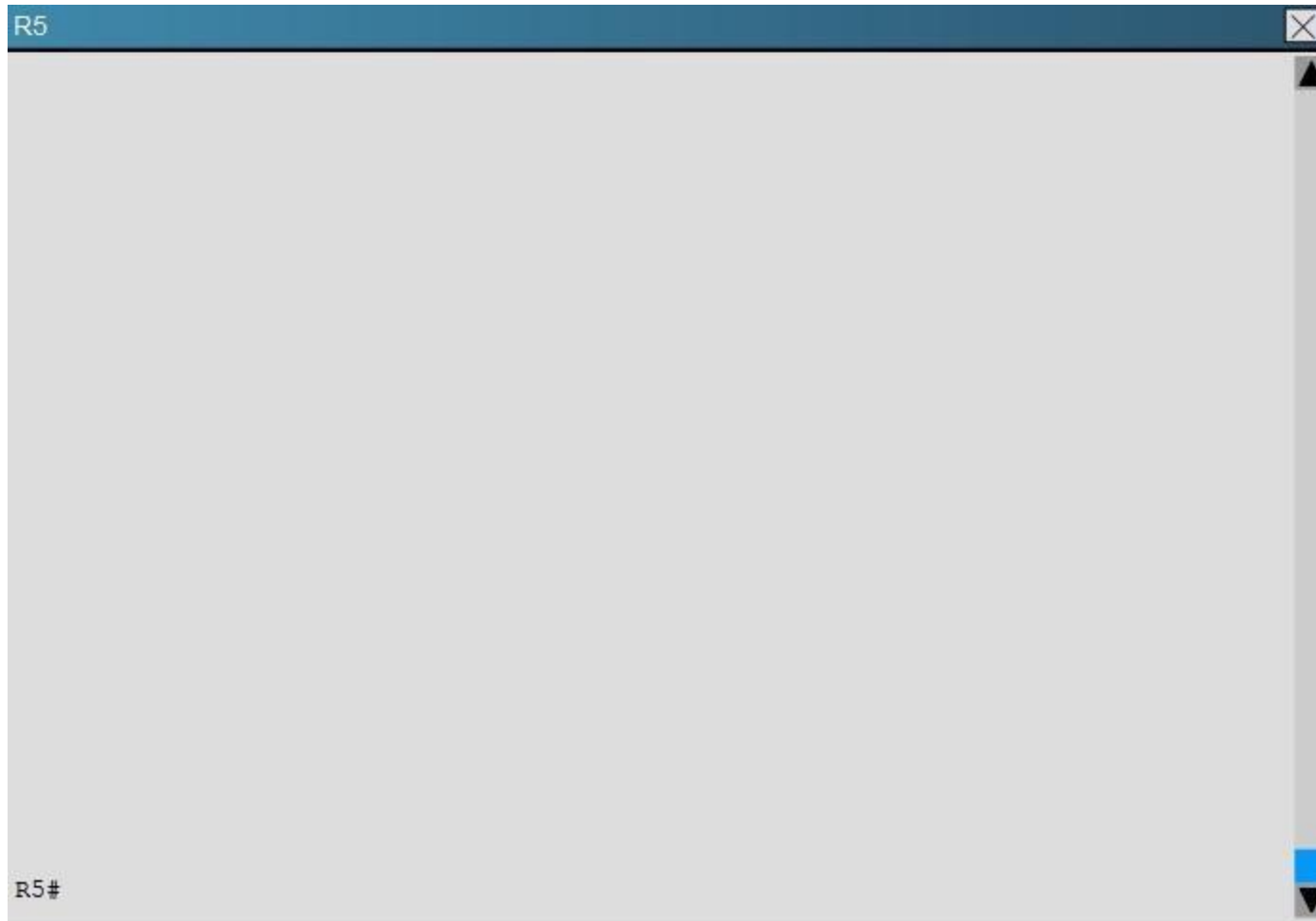
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.











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.

Correct Answer: B

Section: Troubleshooting HSRP

Explanation

Explanation/Reference:

Explanation:

If we issue the "show ip route" and "show ipospf neighbor" commands on R5, we see that there are no learned OSPF routes and he has no OSPF neighbors.

R5

R5#show ip route

R5#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
! - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.10.10.0/24 is directly connected, Loopback0

L 10.10.10.1/32 is directly connected, Loopback0

172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.18.40.0/24 is directly connected, Ethernet0/0

L 172.18.40.2/32 is directly connected, Ethernet0/0

R5#show ip ospf

R5#show ip ospf ne

R5#show ip ospf neighbor

R5#show ip ospf ncighbor

R5#

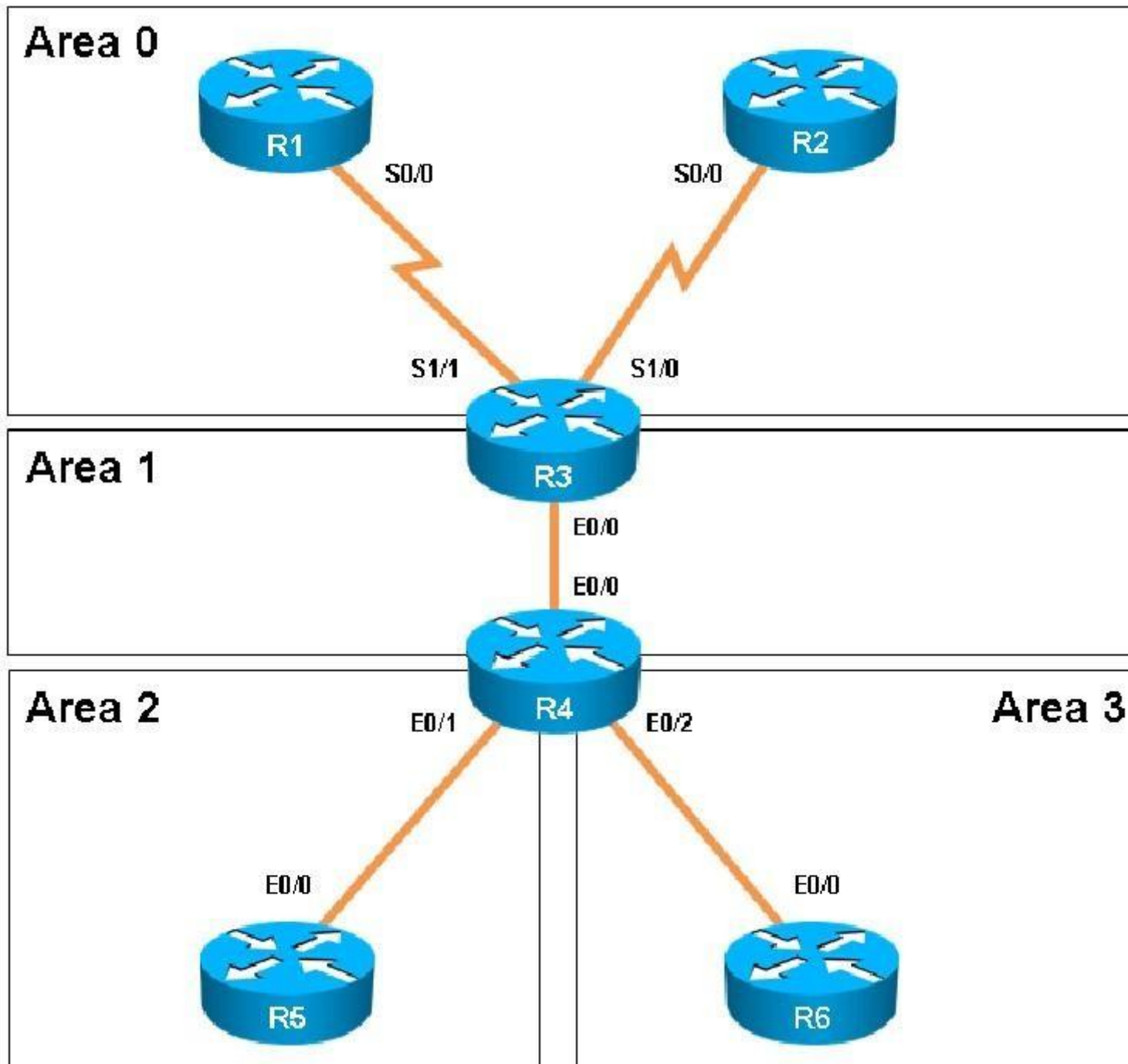
R5#

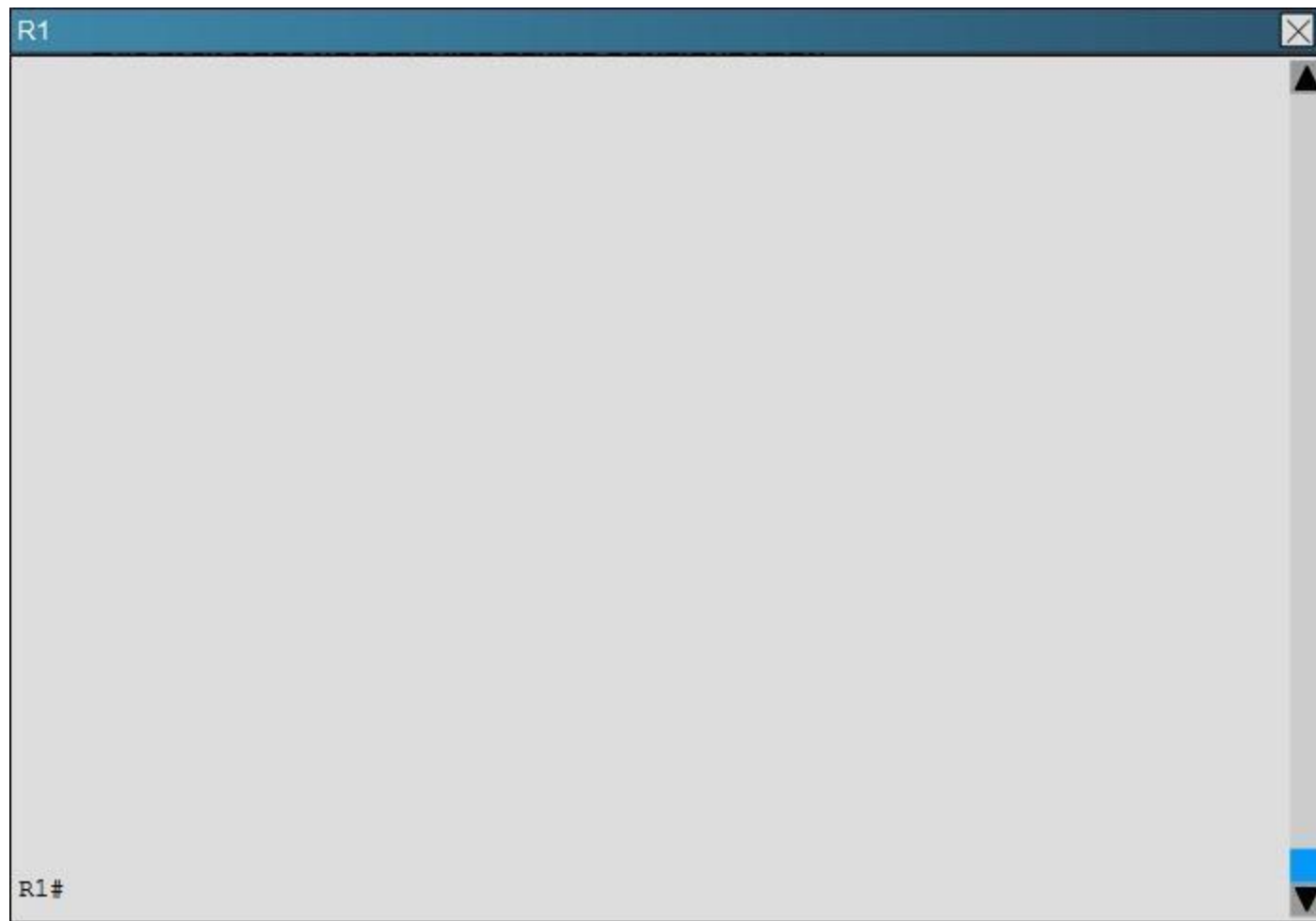
Topic 5, Troubleshooting OSPF

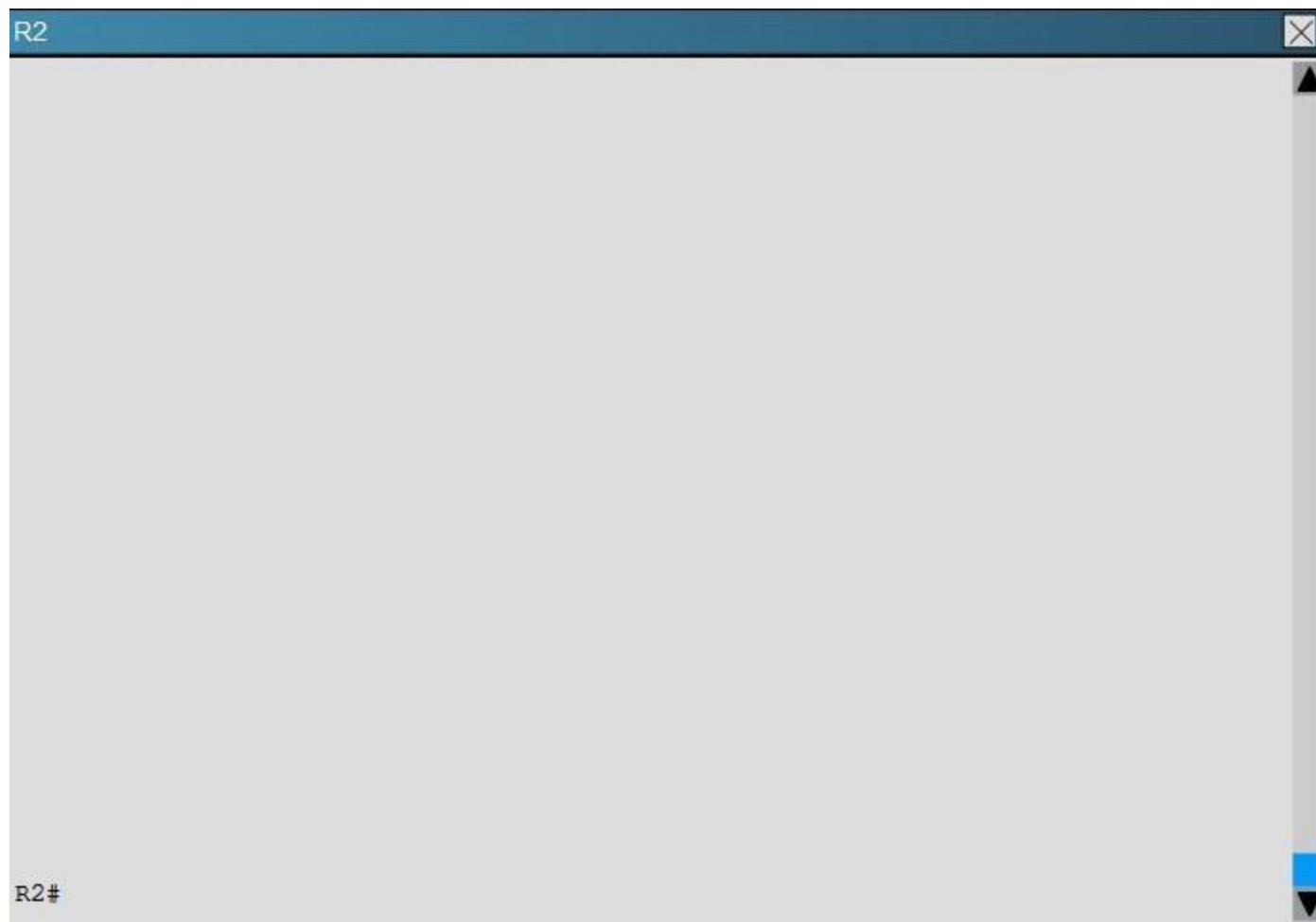
QUESTION 17

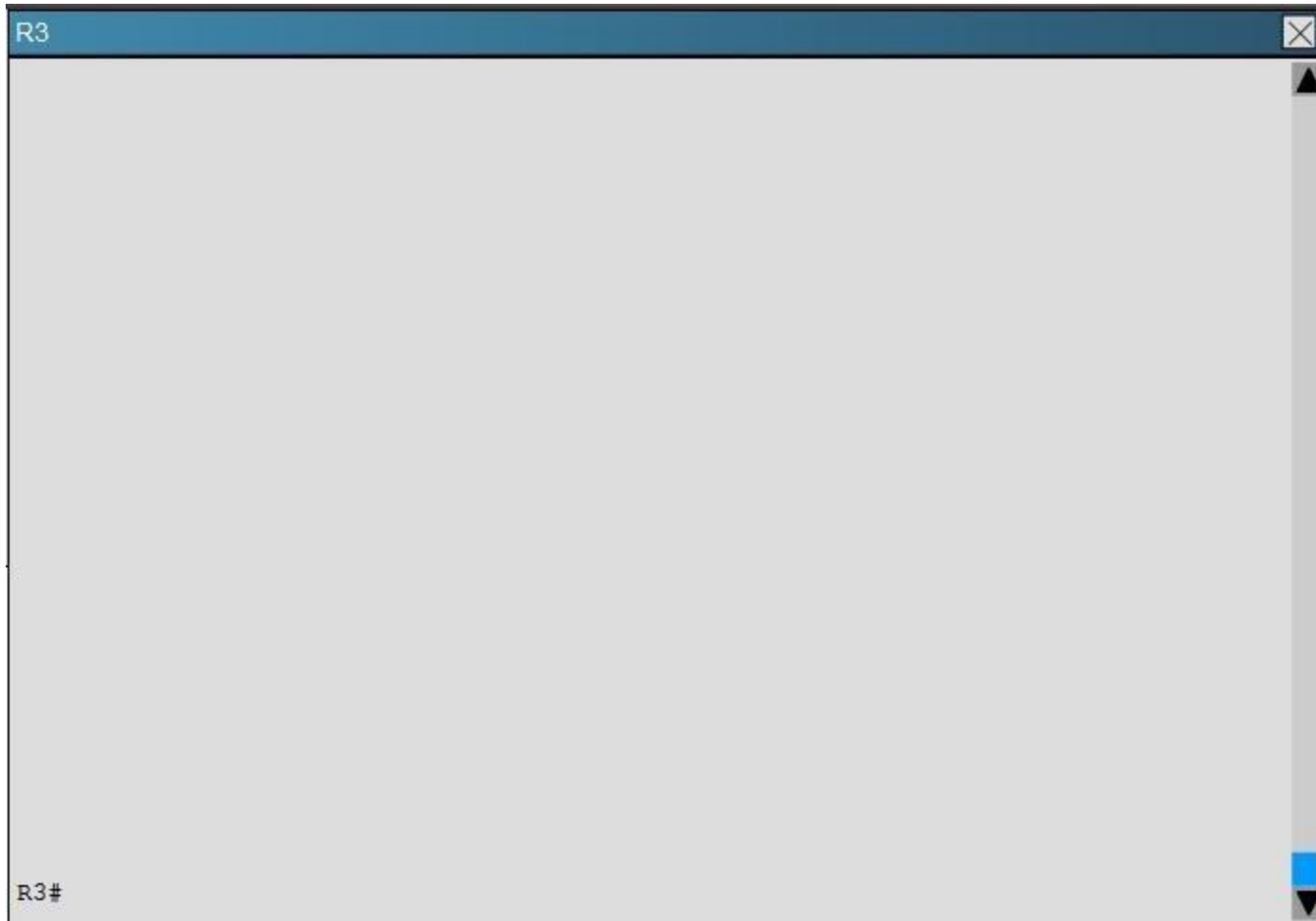
Scenario:

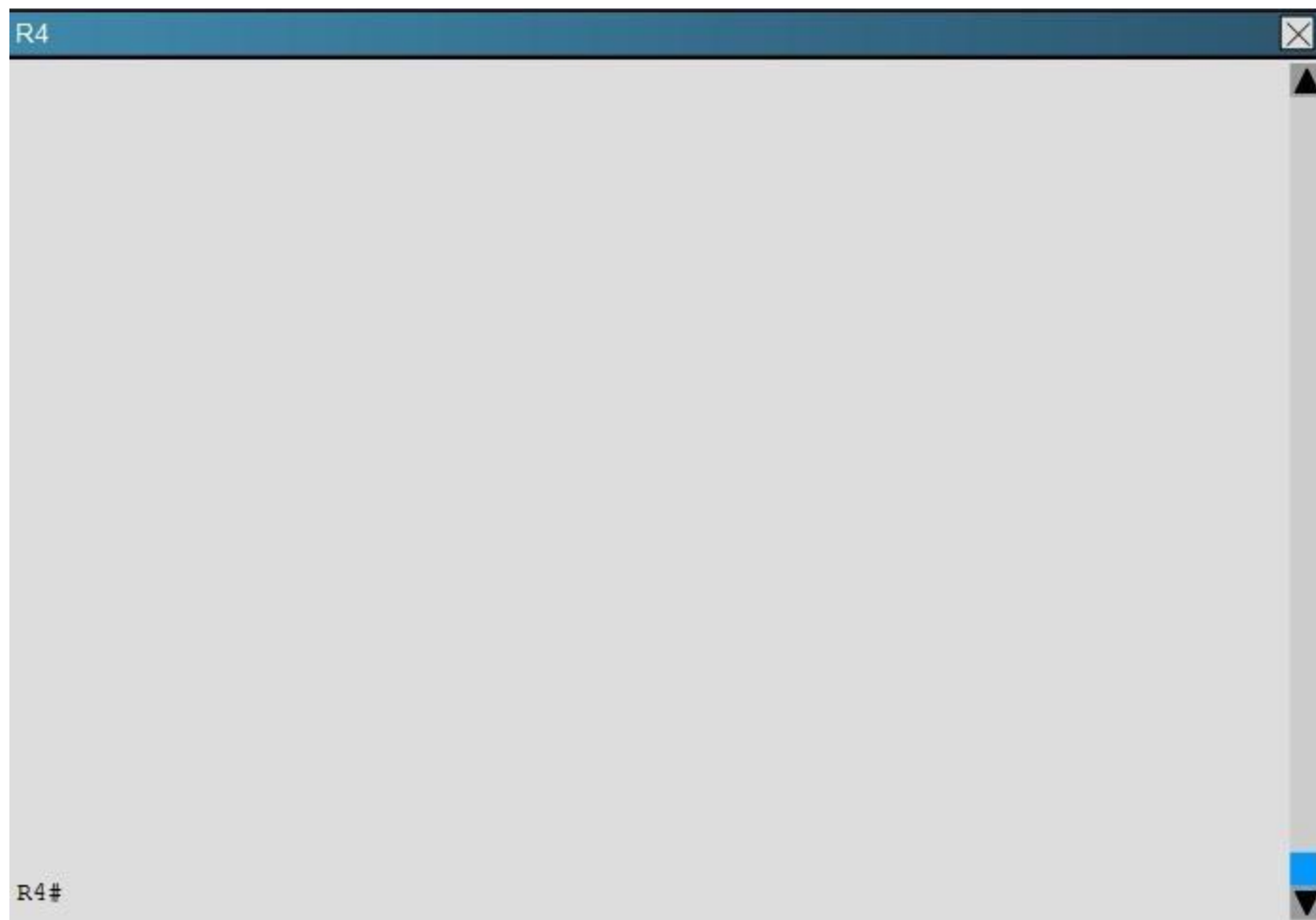
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.

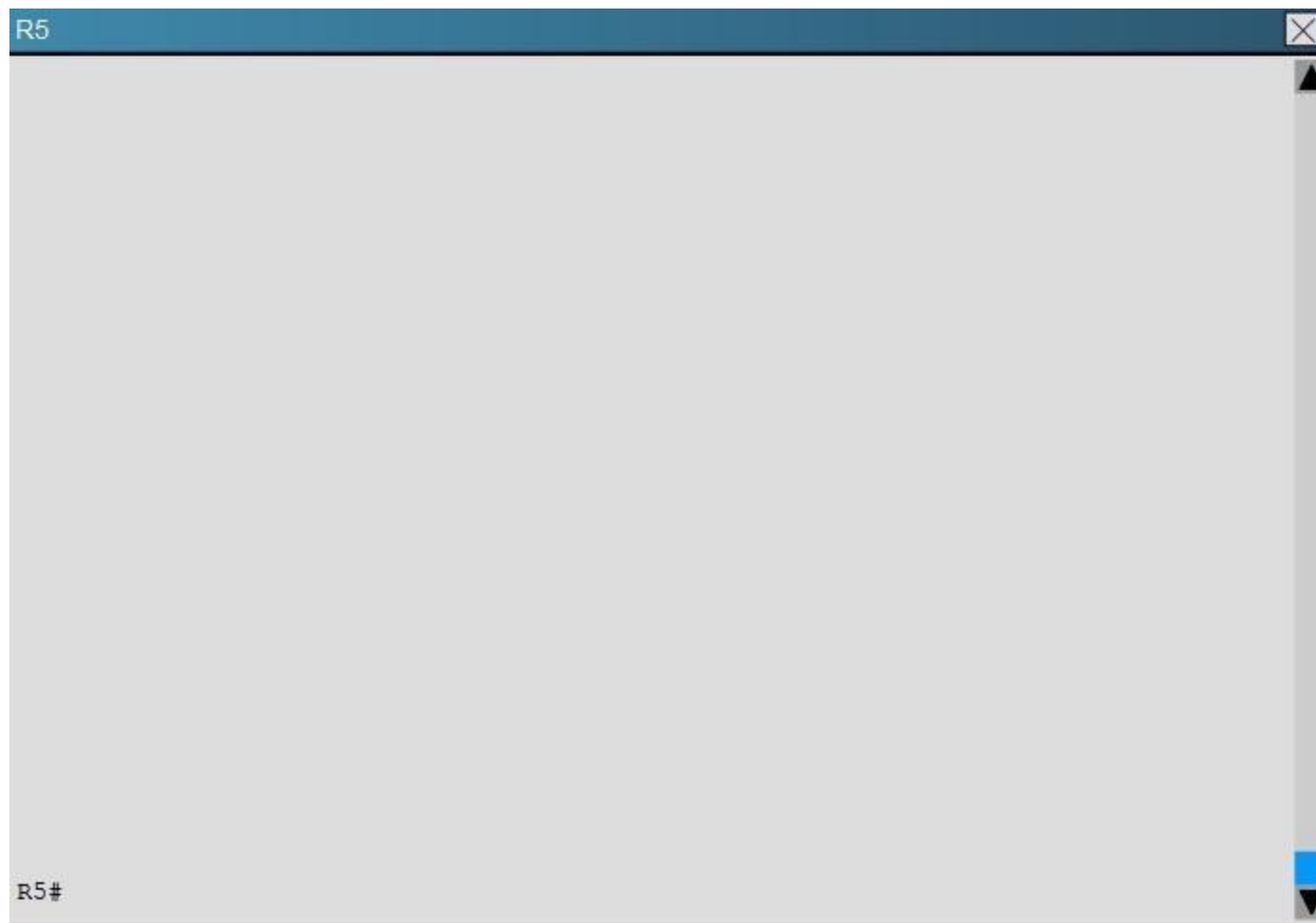


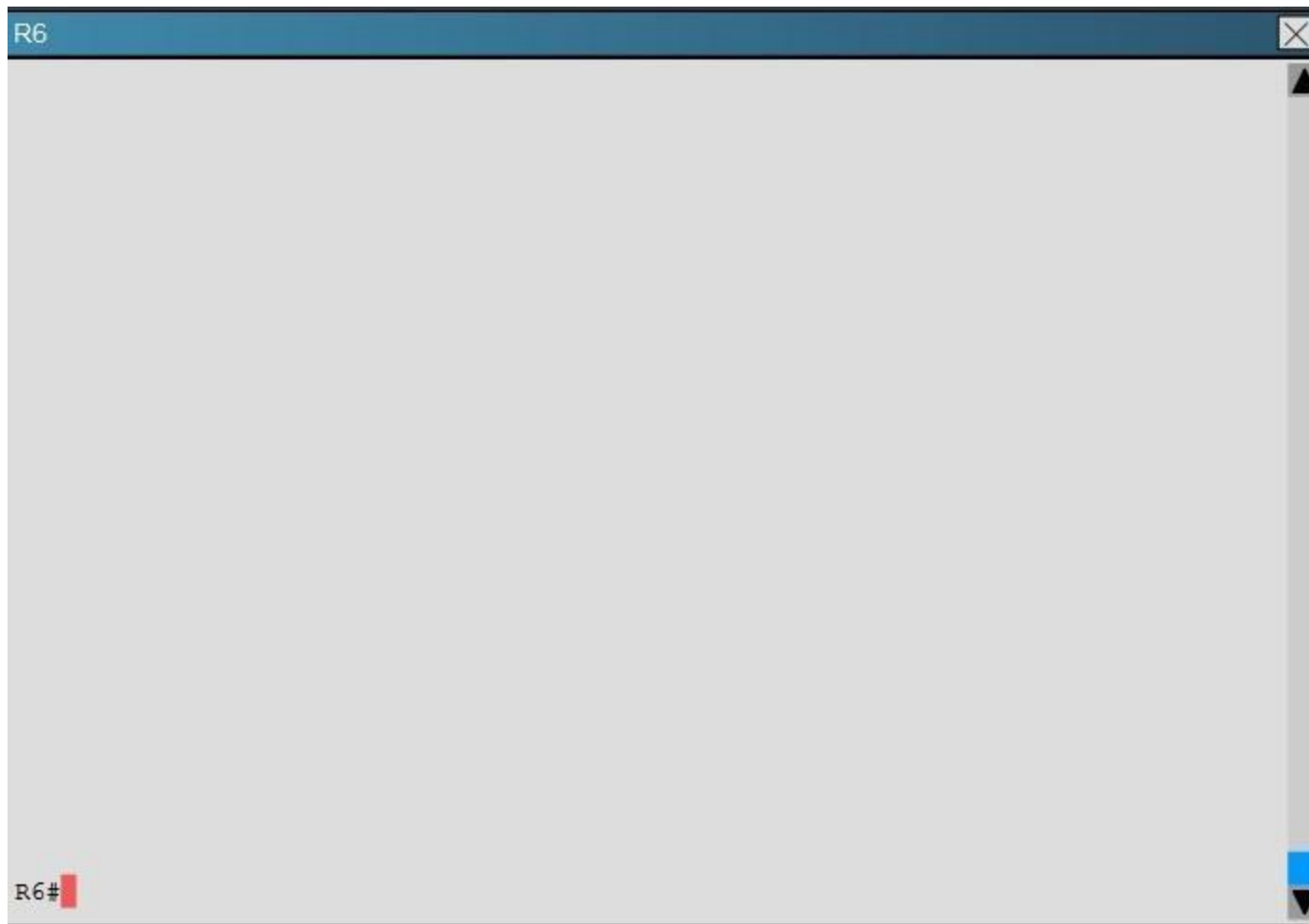












The OSPF neighbour relationship has been lost between R1 and R3. What is causing this problem?

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

Correct Answer: C

Section: Troubleshooting OSPF

Explanation

Explanation/Reference:

Explanation:

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

R1

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


R3

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

This can be seen by issuing the "show running-config" command on each router, or the "show ipospf interface" command:

R1

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

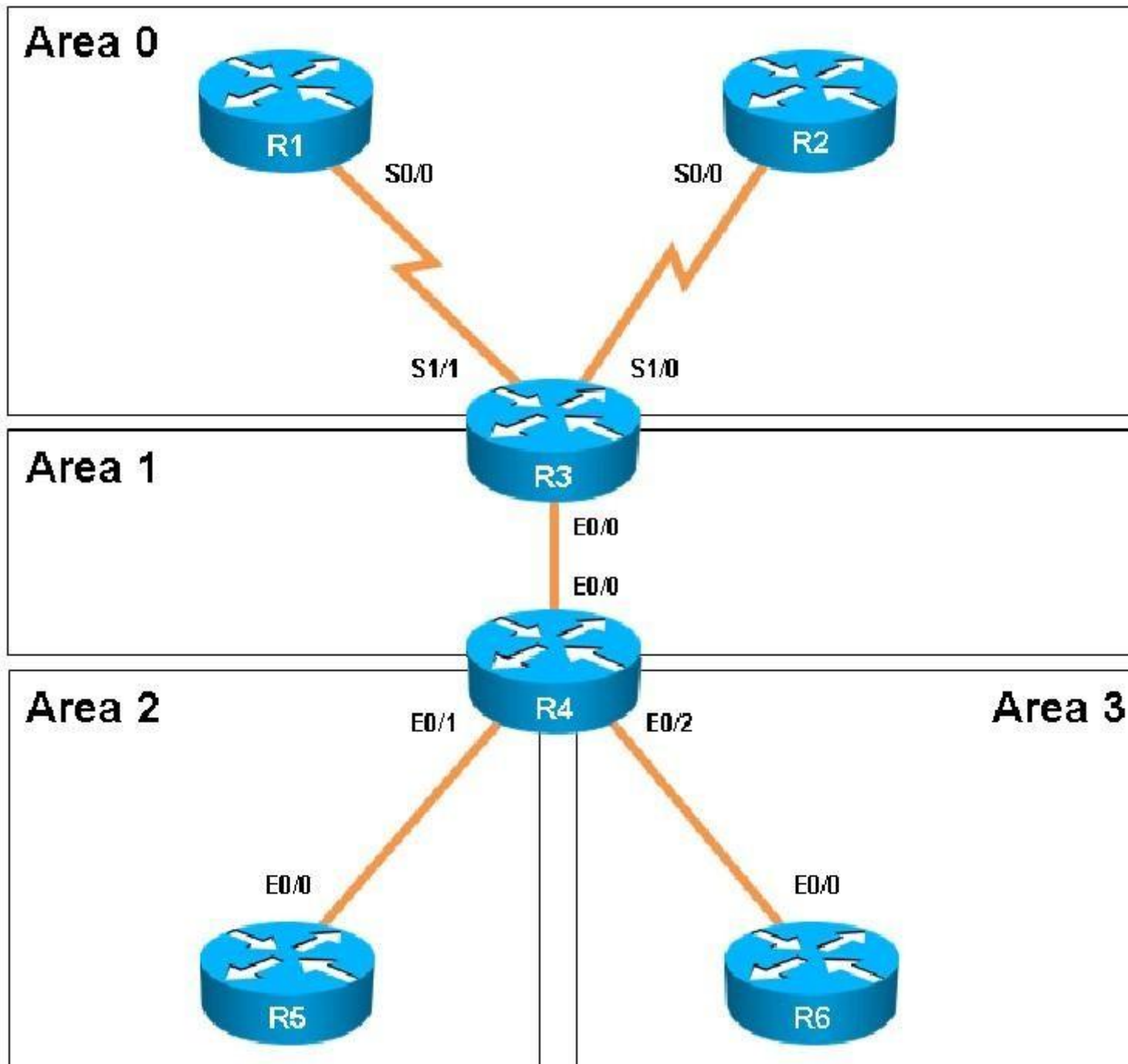
R3

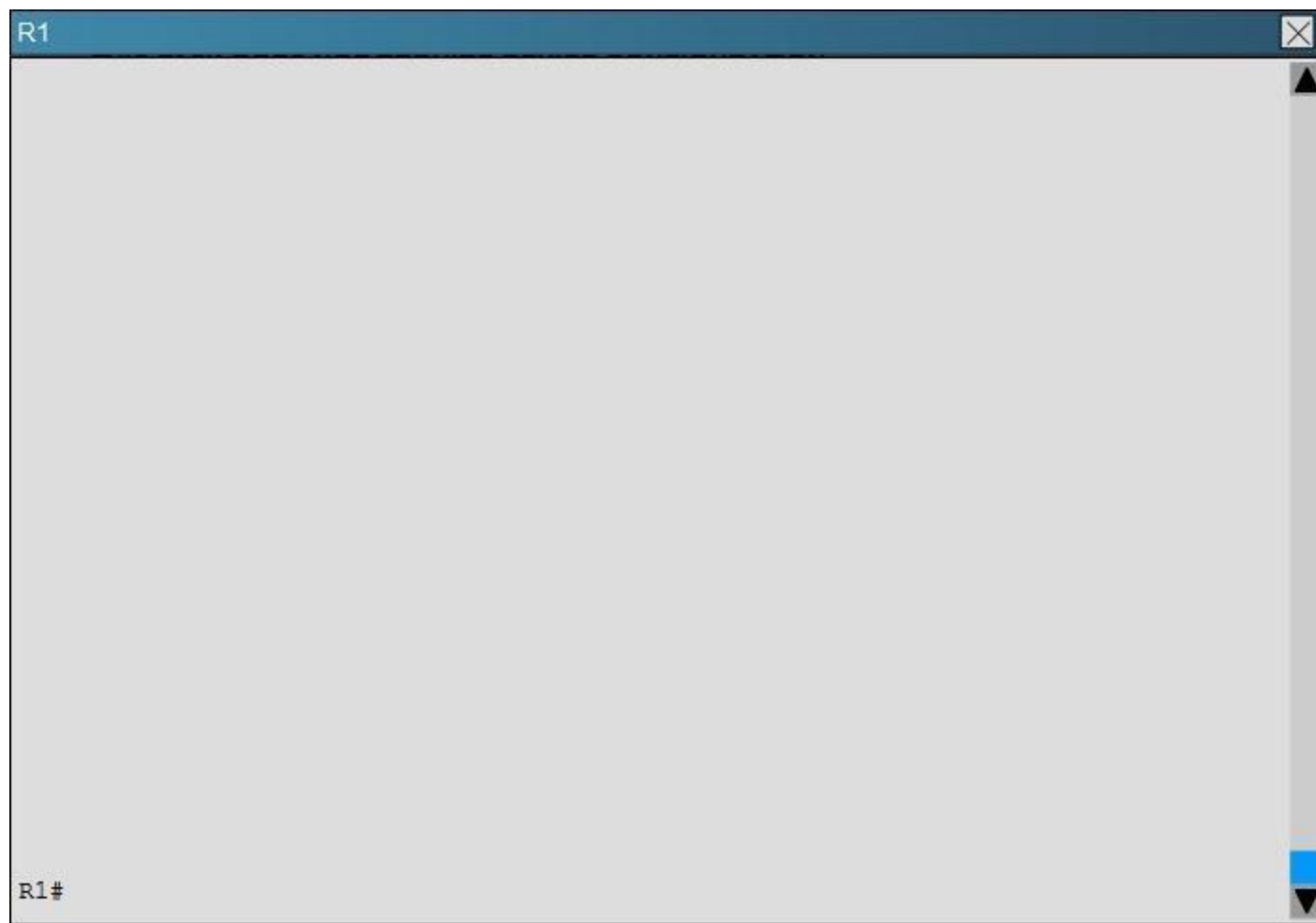
```
Serial1/0 is up, line protocol is up
  Internet Address 192.168.13.3/24, Area 0, Attached via Network Statement
  Process ID 100, Router ID 3.3.3.3, Network Type POINT_TO_MULTIPOINT, Cost: 64
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
            0          64      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

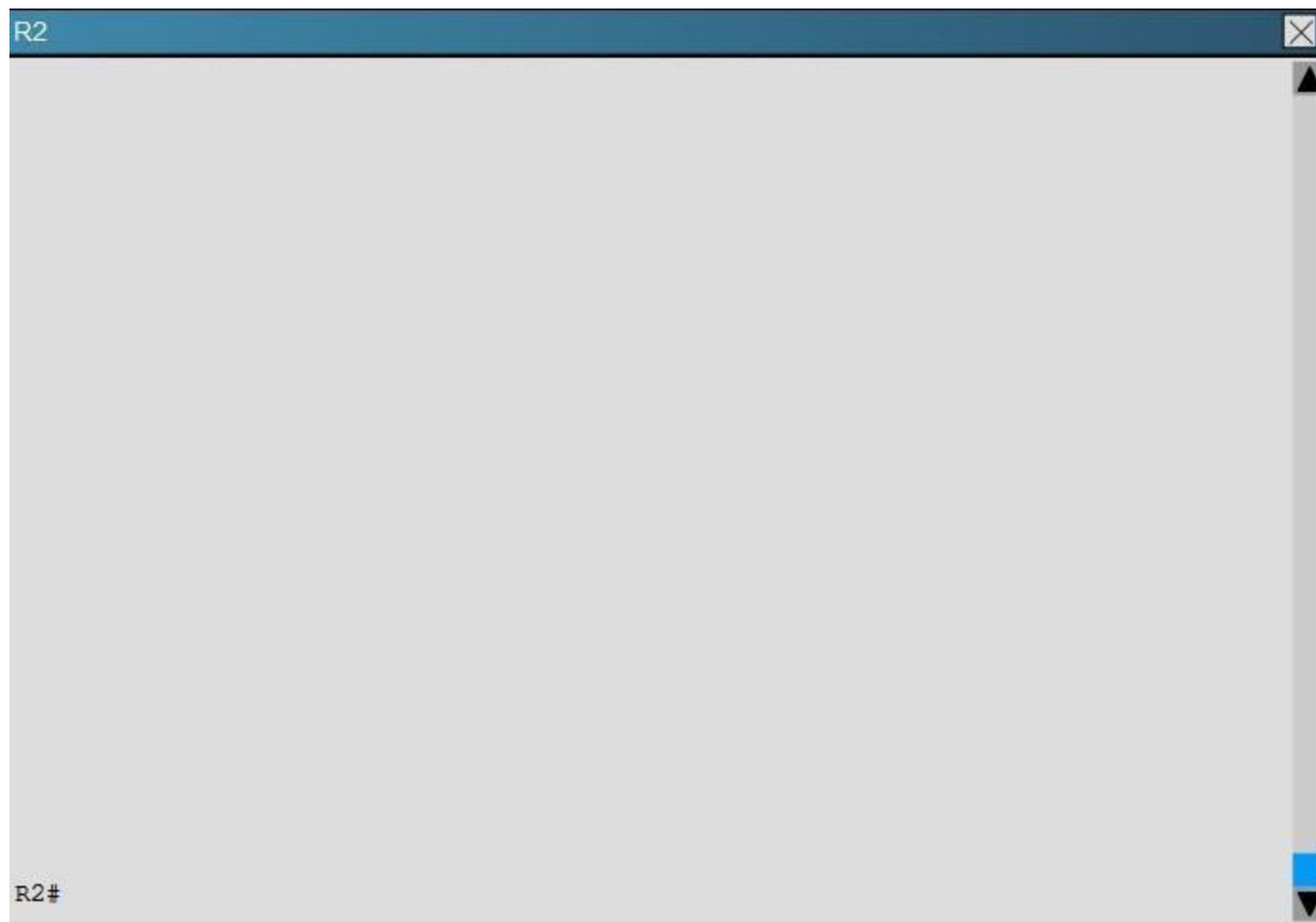
QUESTION 18

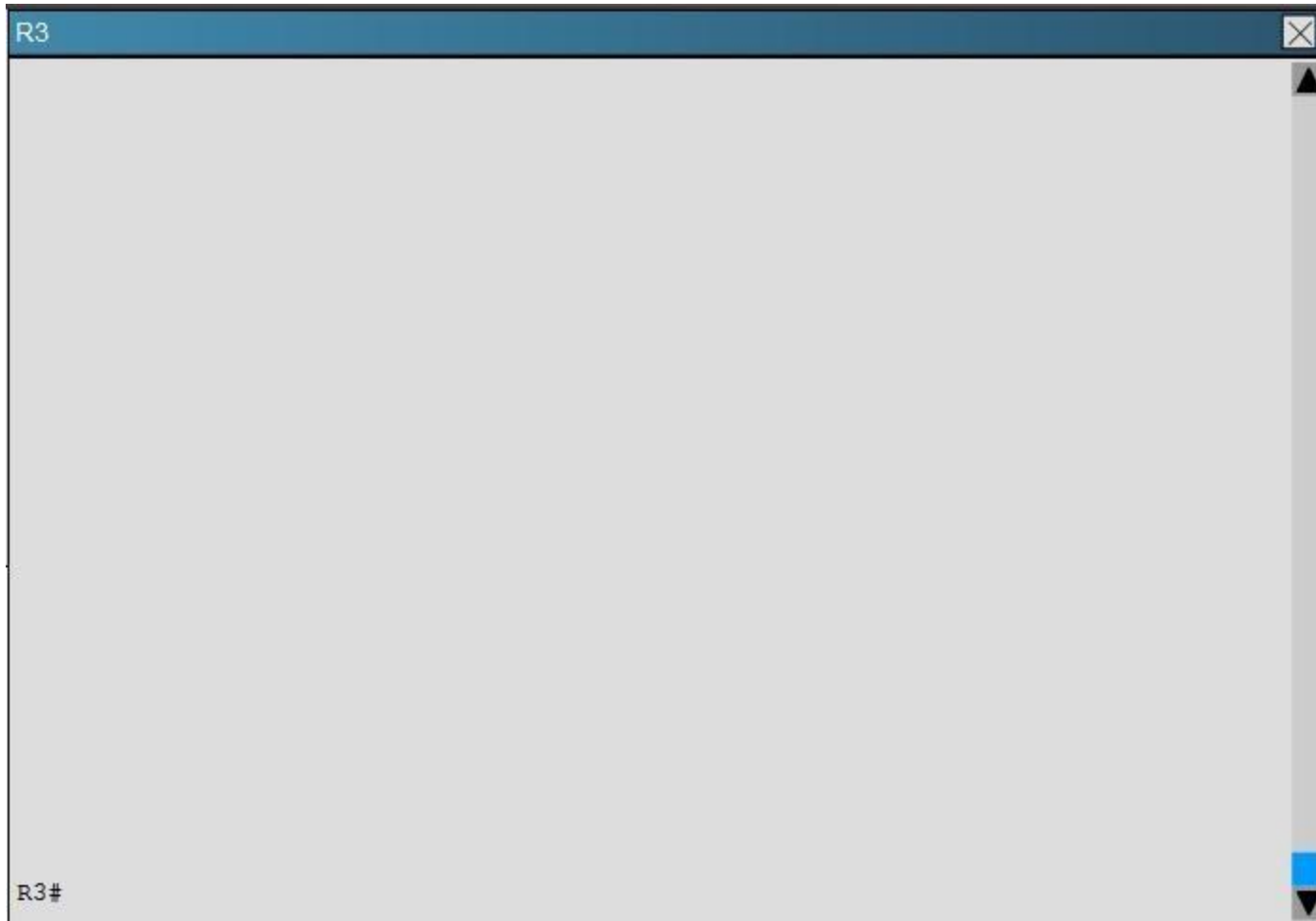
Scenario:

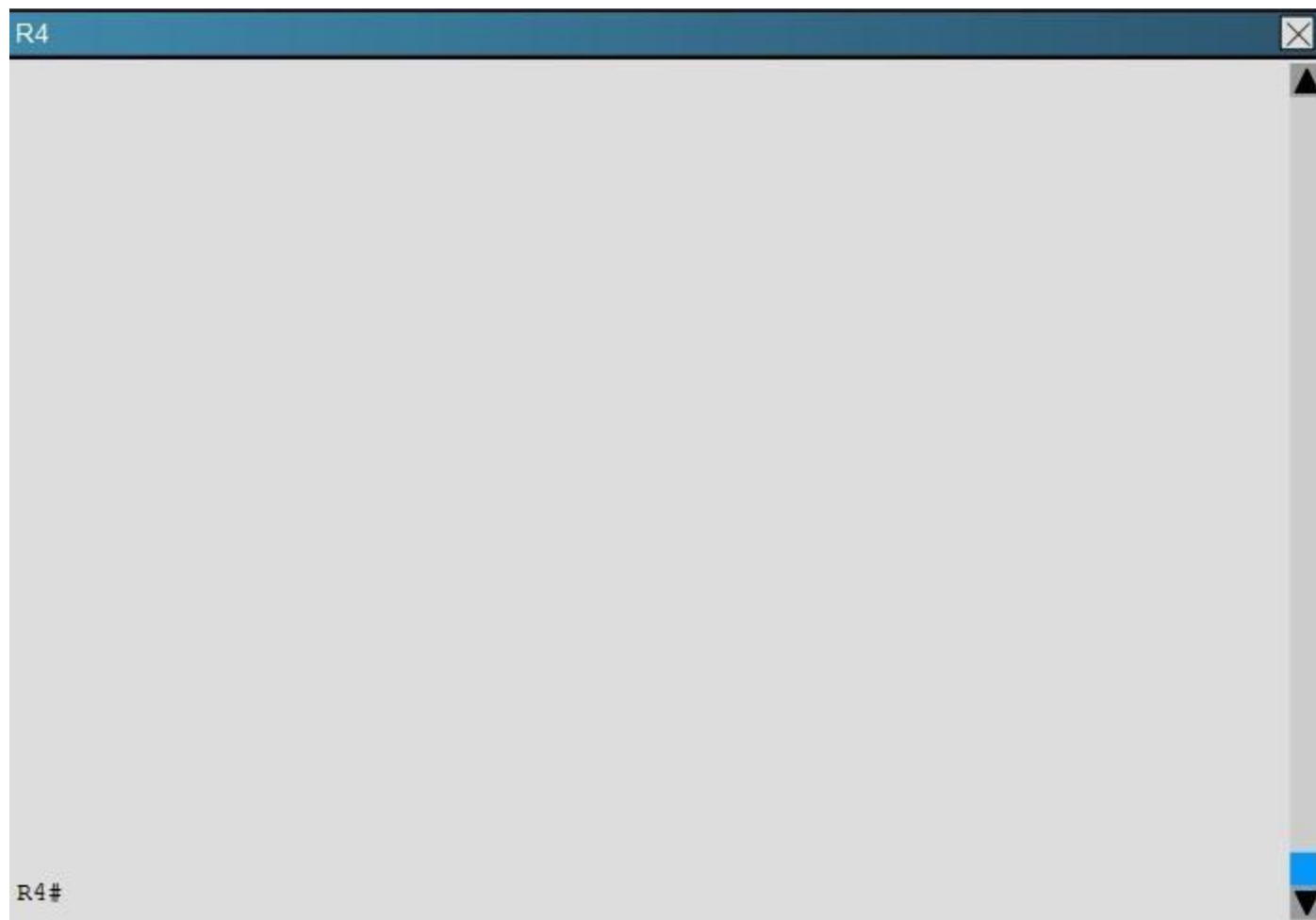
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.

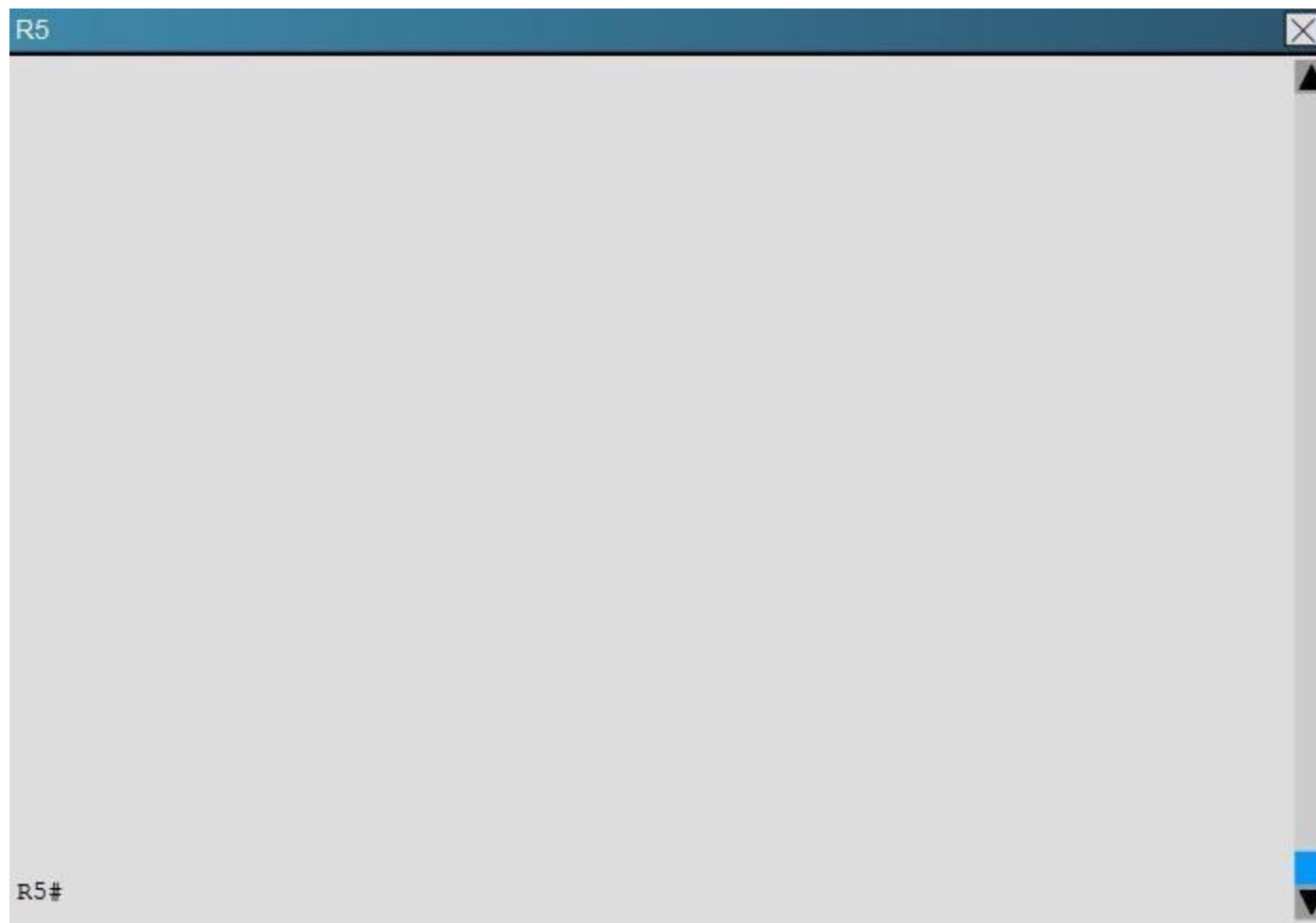














Connectivity from R3 to R4, R5 and R6 has been lost. How should connectivity be reestablished?

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

Correct Answer: E

Section: Troubleshooting OSPF

Explanation

Explanation/Reference:

Explanation:

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

Here, we see that the link to R4 is using the 192.168.34.0 network, but that this network has not been added to OSPF

```
R3
!
R3#show ip int brief
R3#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
Ethernet0/0              192.168.34.3    YES NVRAM    up          up
Ethernet0/1              unassigned      YES NVRAM    administratively down down
Ethernet0/2              unassigned      YES NVRAM    administratively down down
Ethernet0/3              unassigned      YES NVRAM    administratively down down
Serial1/0                192.168.13.3    YES NVRAM    up          up
Serial1/1                192.168.23.3    YES NVRAM    up          up
Serial1/2                unassigned      YES NVRAM    administratively down down
Serial1/3                unassigned      YES NVRAM    administratively down down
Loopback0                3.3.3.3         YES NVRAM    up          up
R3#
R3#
R3#
```

R3

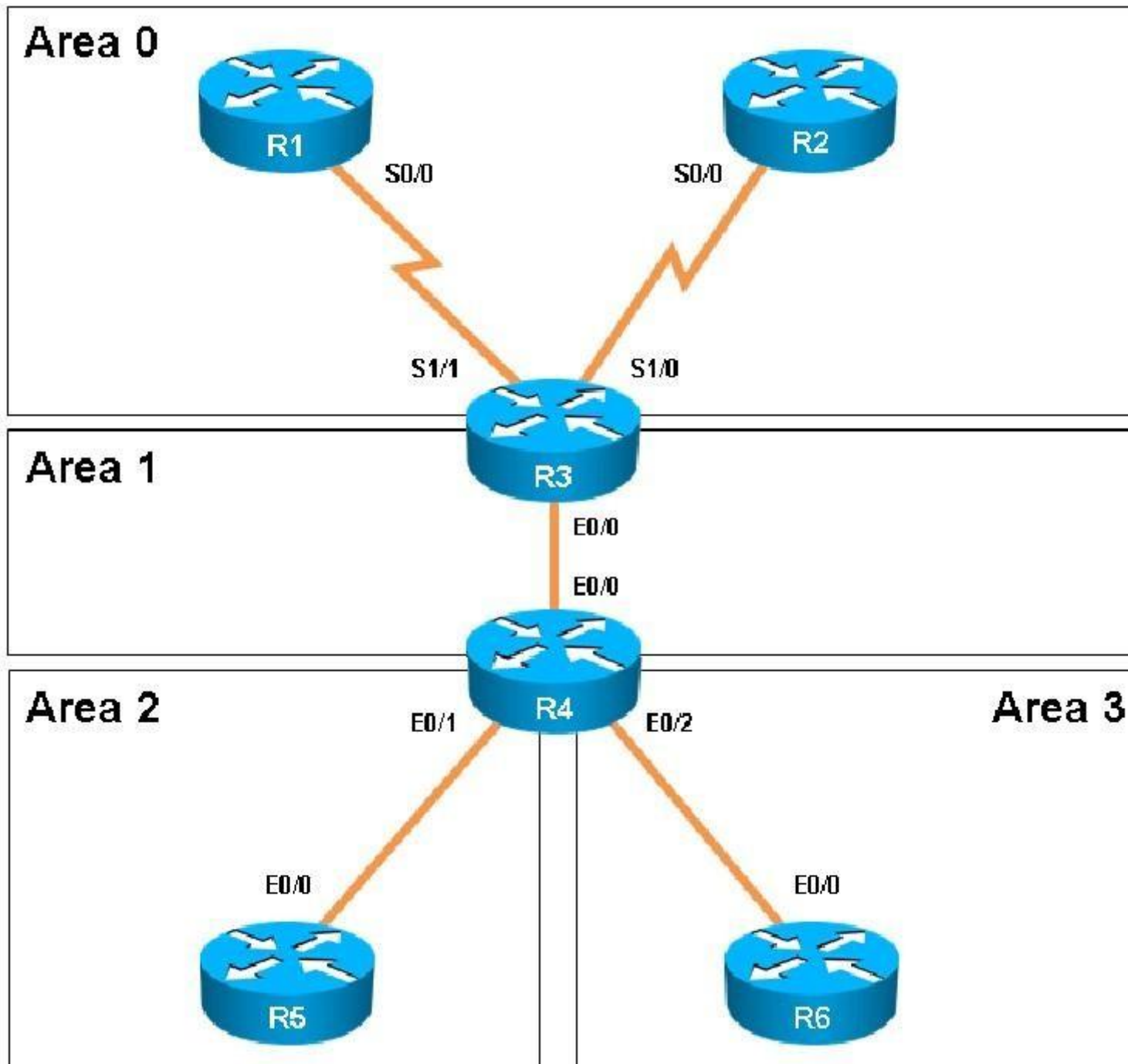
```
!  
router ospf 100  
  router-id 3.3.3.3  
  area 1 virtual-link 4.4.4.4  
  network 3.3.3.3 0.0.0.0 area 1  
  network 192.168.13.0 0.0.0.255 area 0  
  network 192.168.23.0 0.0.0.255 area 0  
  neighbor 192.168.13.1  
!  
!
```

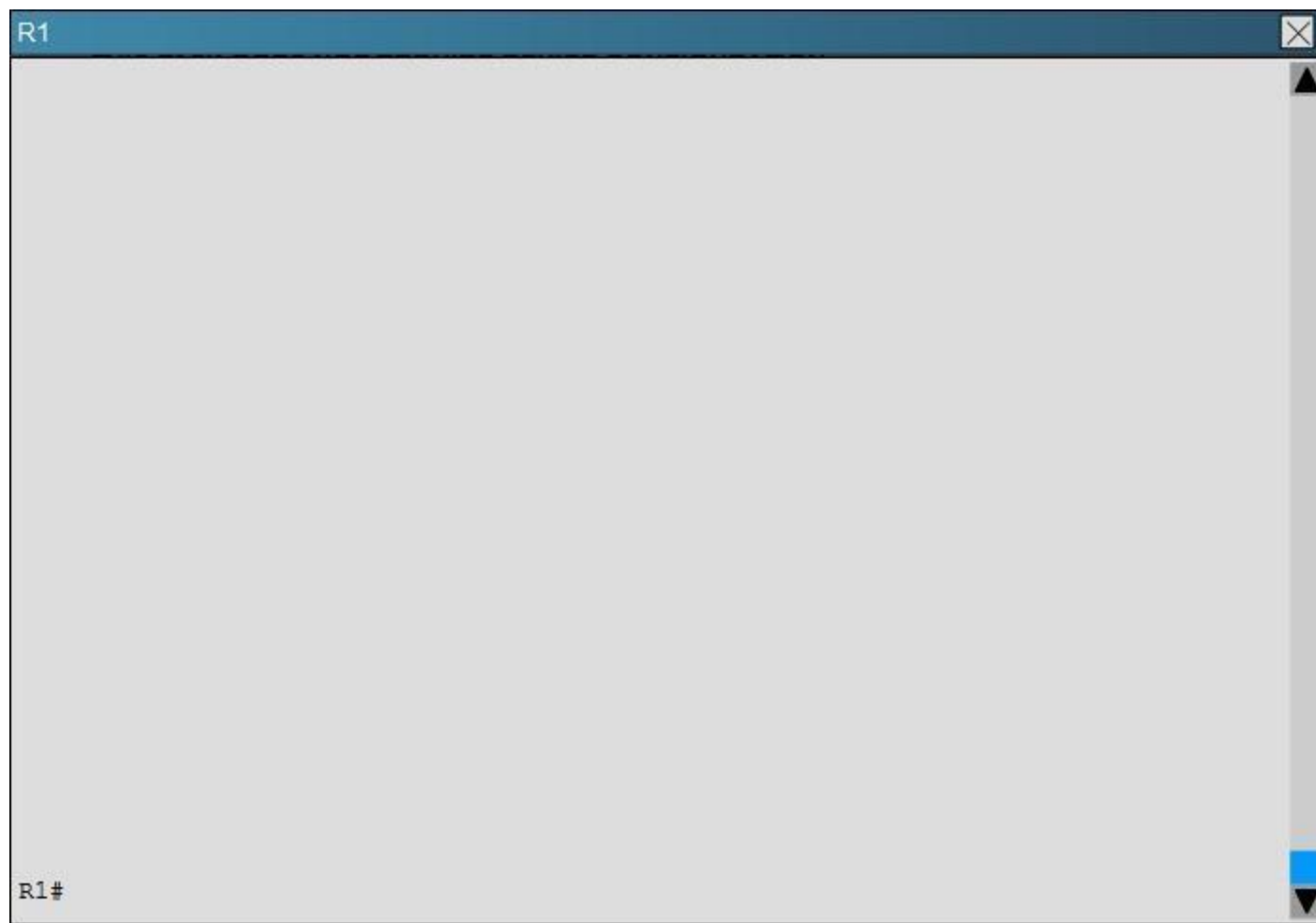
Based on the network diagram, this link should be added to Area 1, not Area 2.

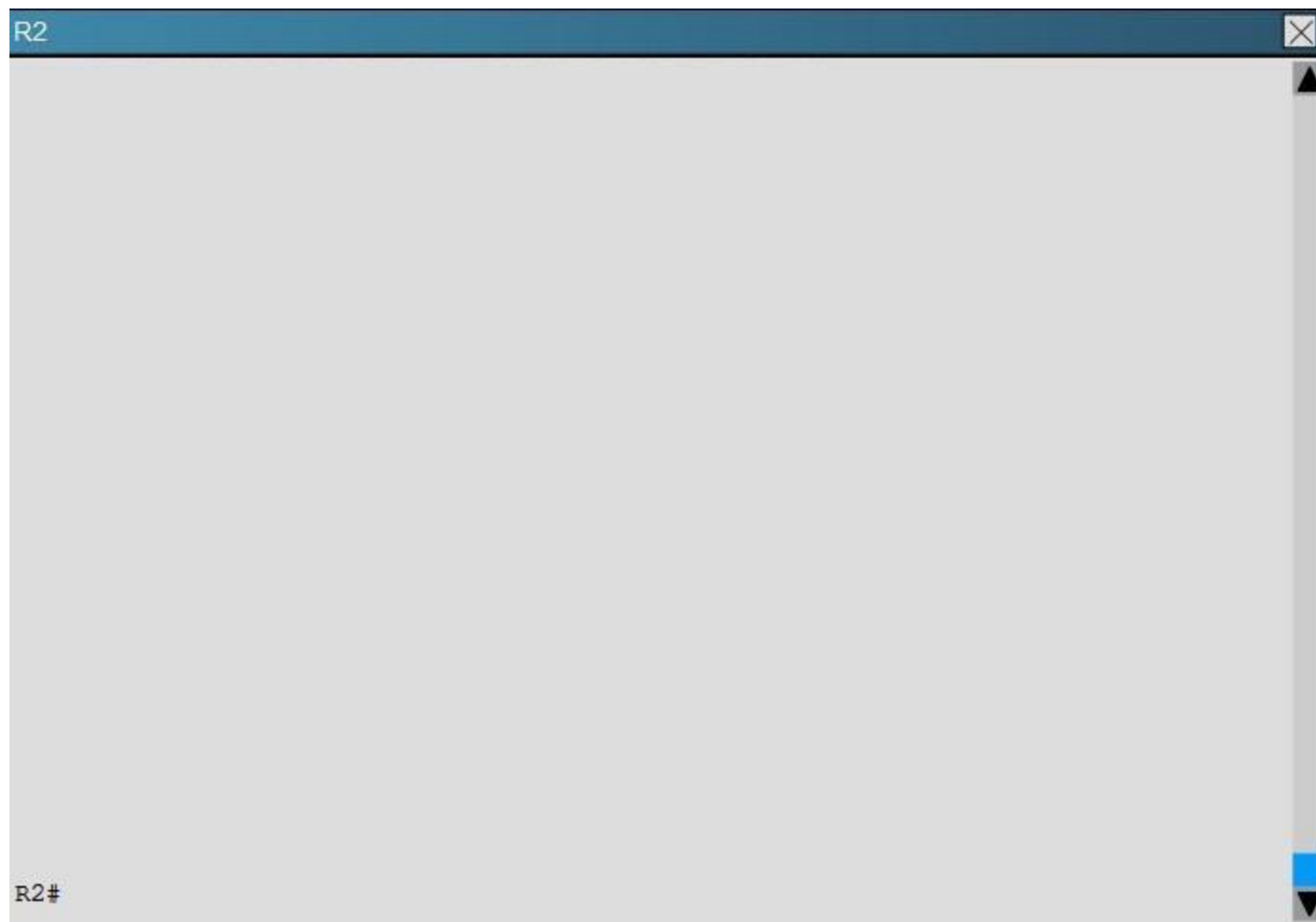
QUESTION 19

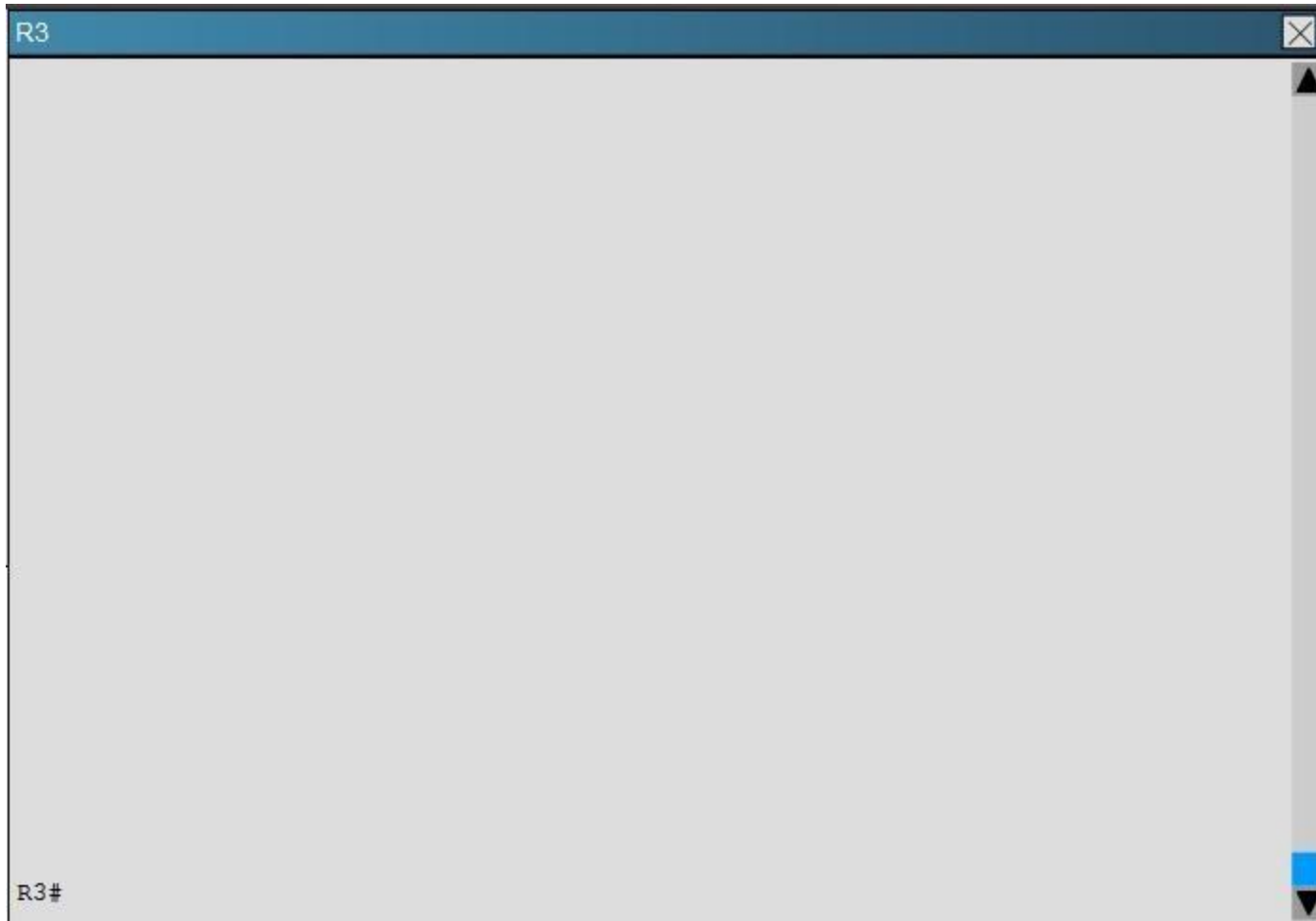
Scenario:

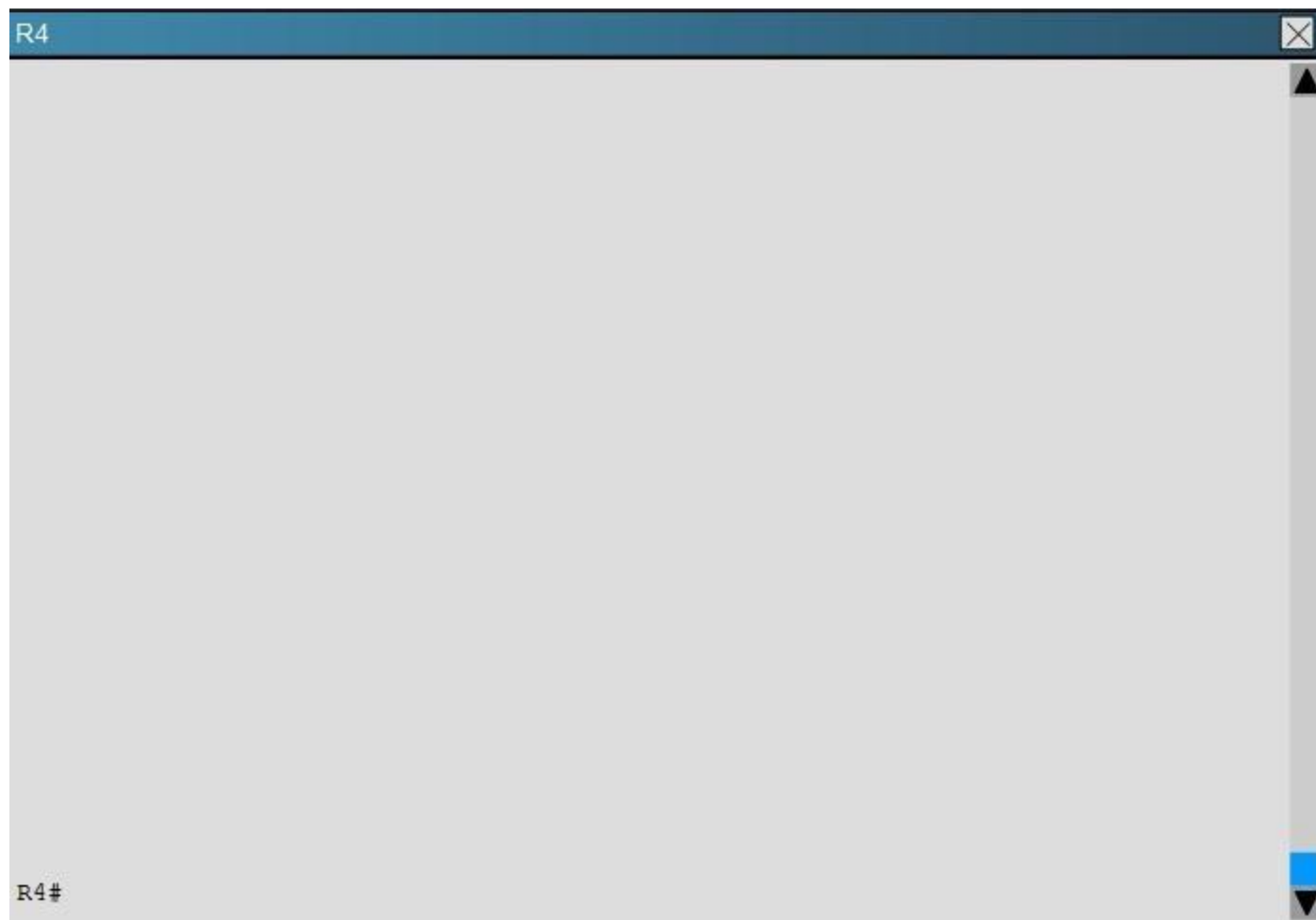
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.

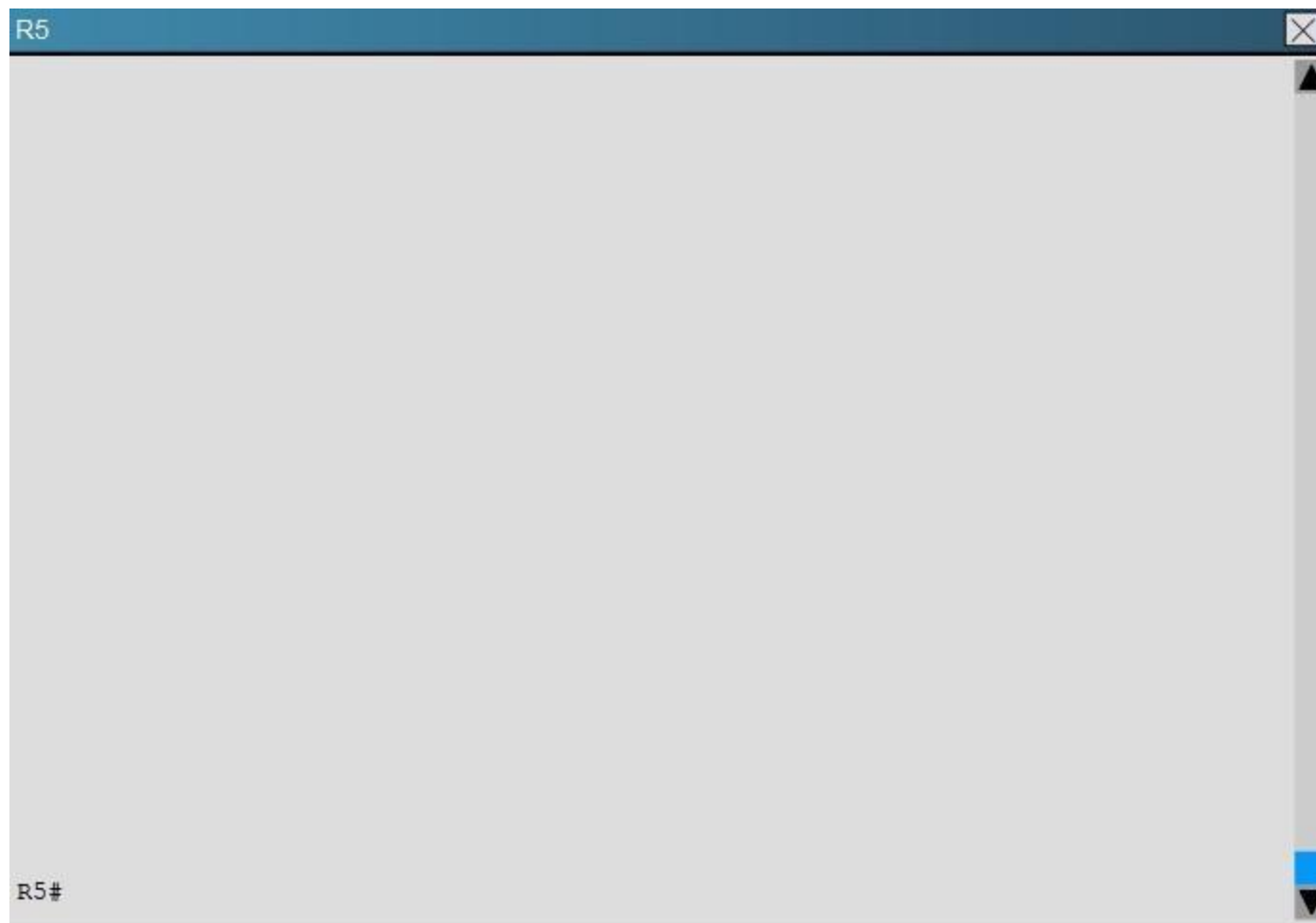


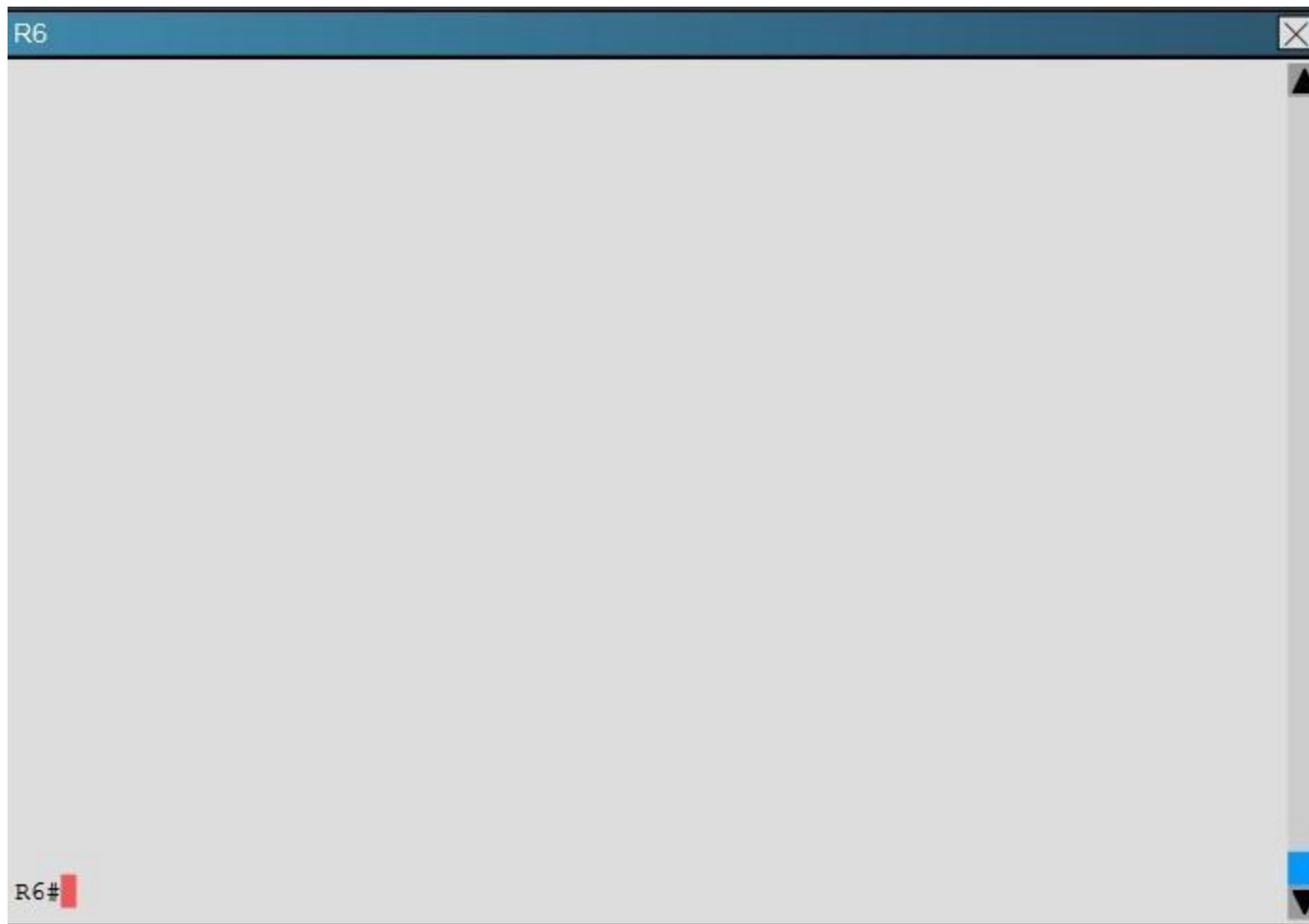












After resolving the issues between R3 and R4. Area 2 is still experiencing routing issues. Based on the current router configurations, what needs to be resolved for routes to the networks behind R5 to be seen in the company intranet?

- 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 ipospf authentication-key 7 BEST to the R4 Ethernet interface that connects to R5 and ipospf authentication-key 7 BEST to R5 Ethernet interface that connects to R4.

D. Add ipospf authentication-key CISCO to R4 Ethernet 0/1 and add area 2 authentication to the R4 OSPF routing process.

Correct Answer: D

Section: Troubleshooting OSPF

Explanation

Explanation/Reference:

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:

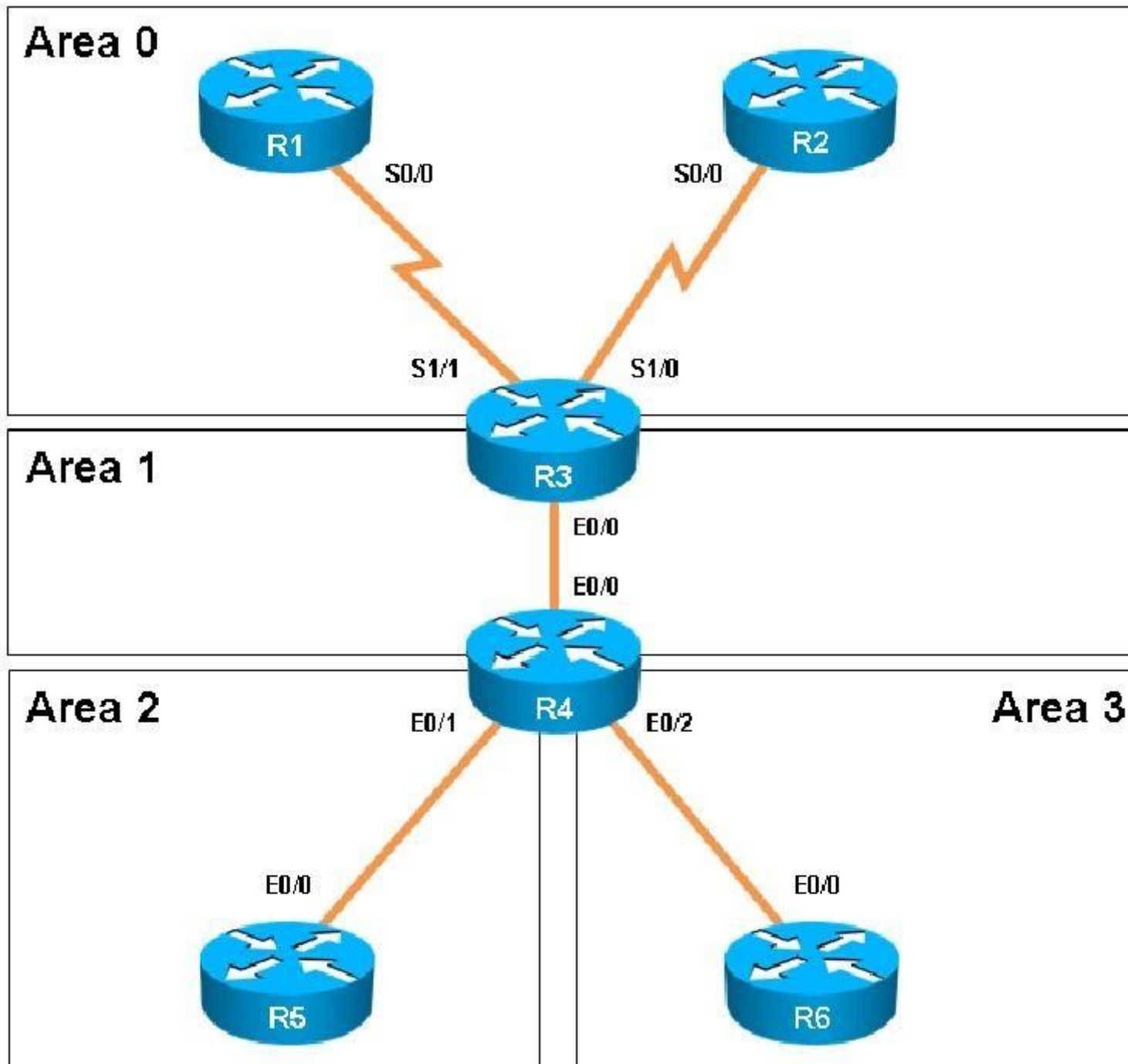
R4

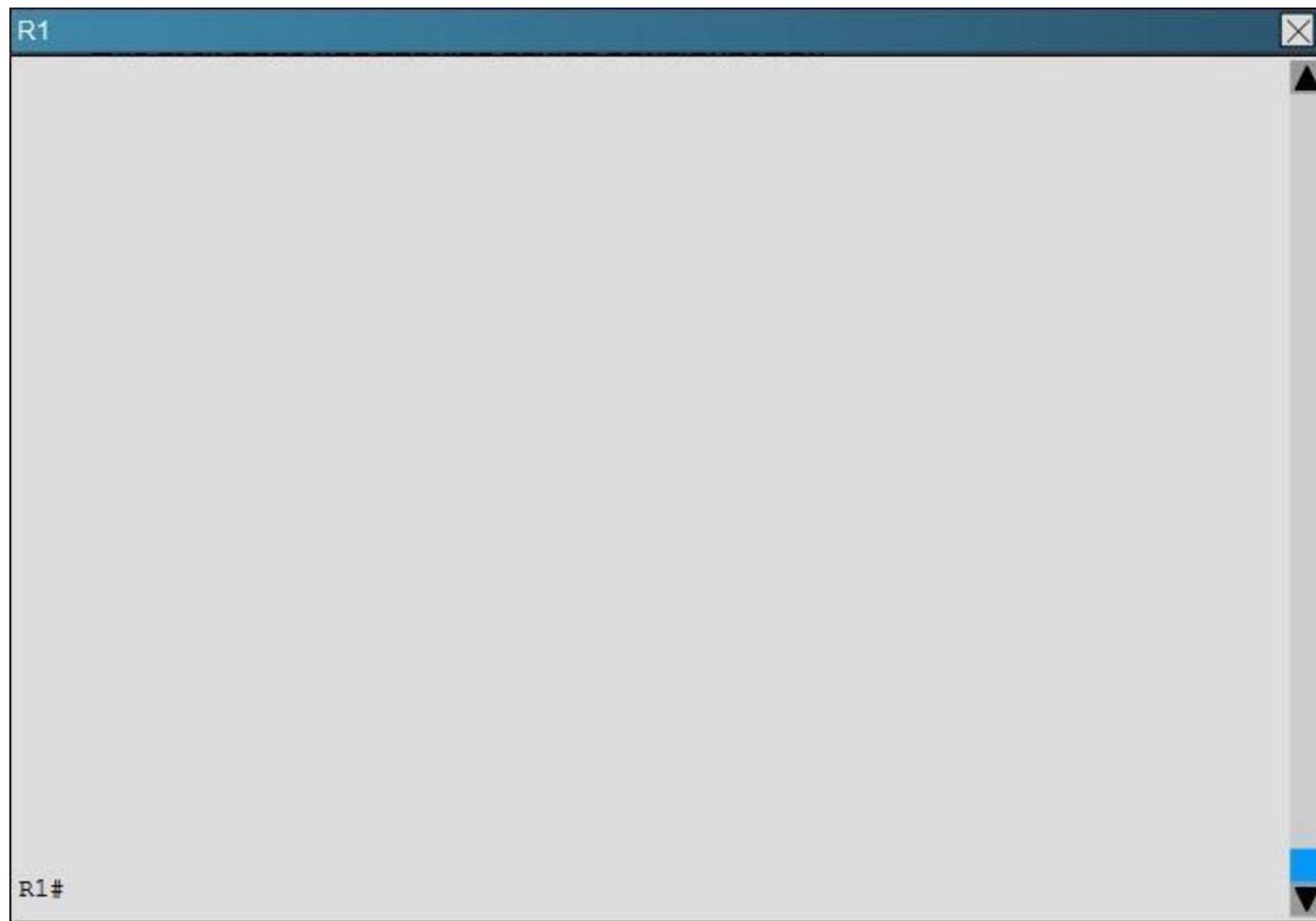
```
interface Ethernet0/1
 ip address 192.168.45.4 255.255.255.0
!
interface Ethernet0/2
 ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/3
 no ip address
 shutdown
!
router ospf 100
 router-id 4.4.4.4
 auto-cost reference-bandwidth 3000
 area 1 virtual-link 3.3.3.3
 area 2 nssa
 area 2 range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

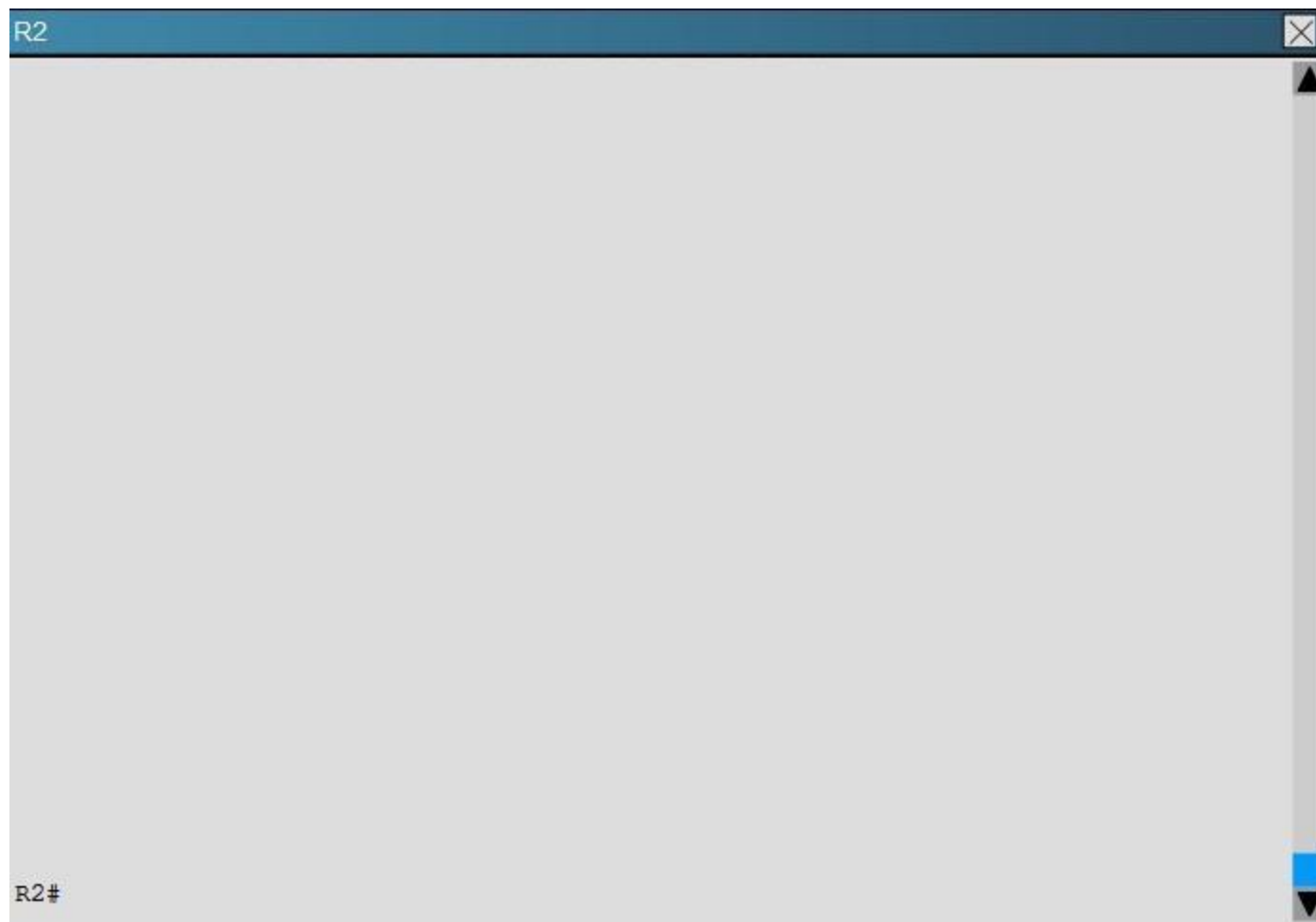

QUESTION 20

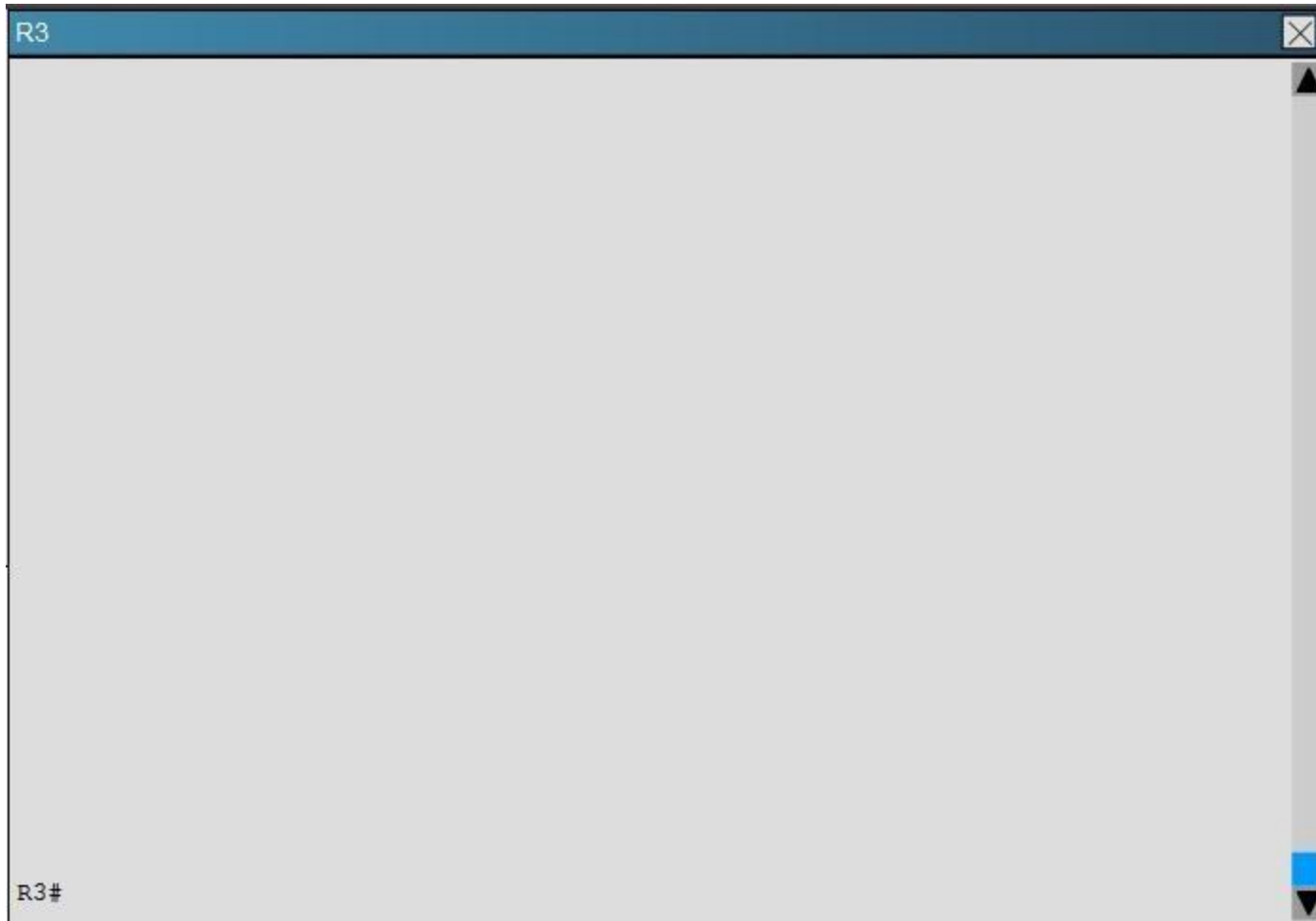
Scenario:

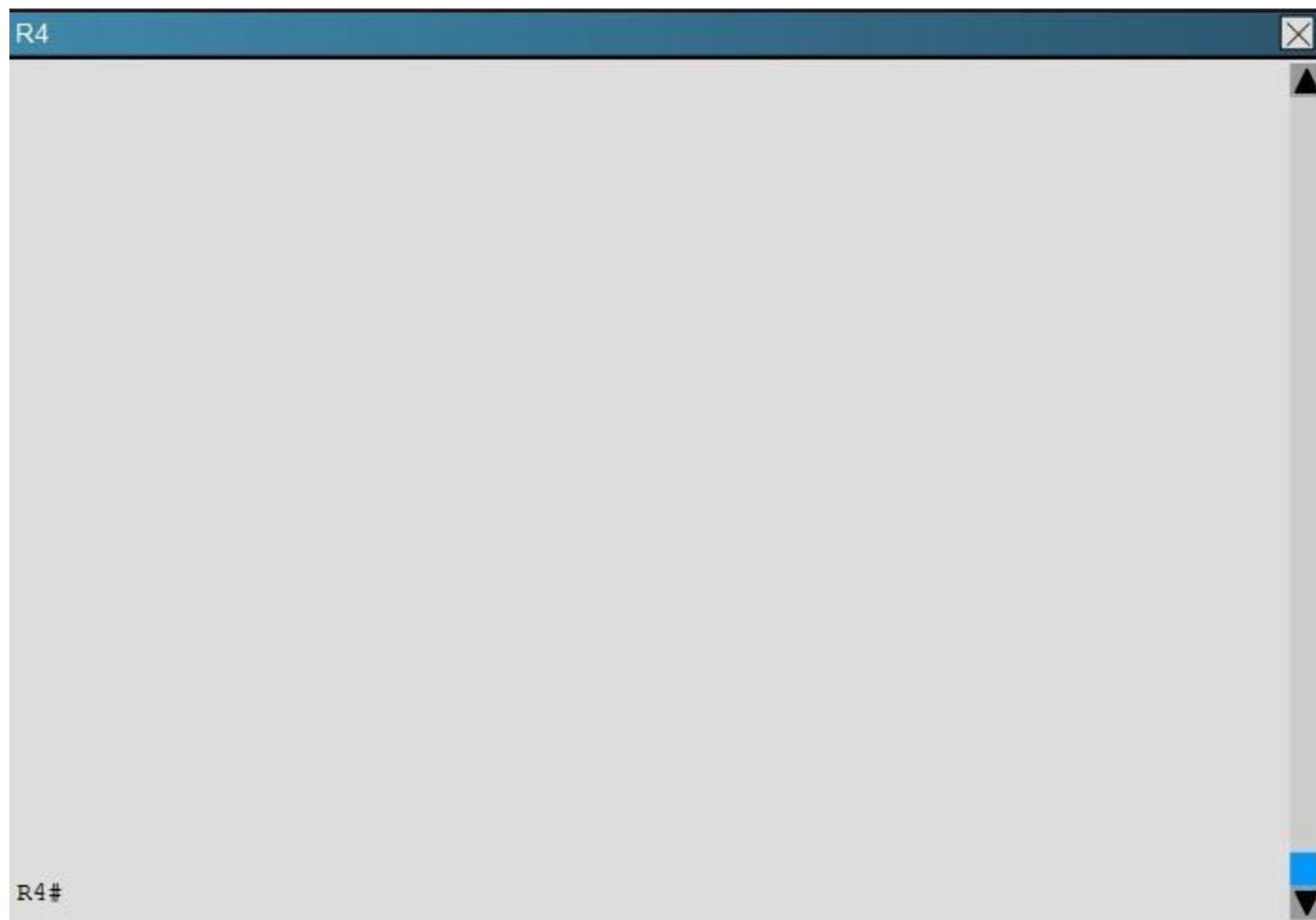
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.

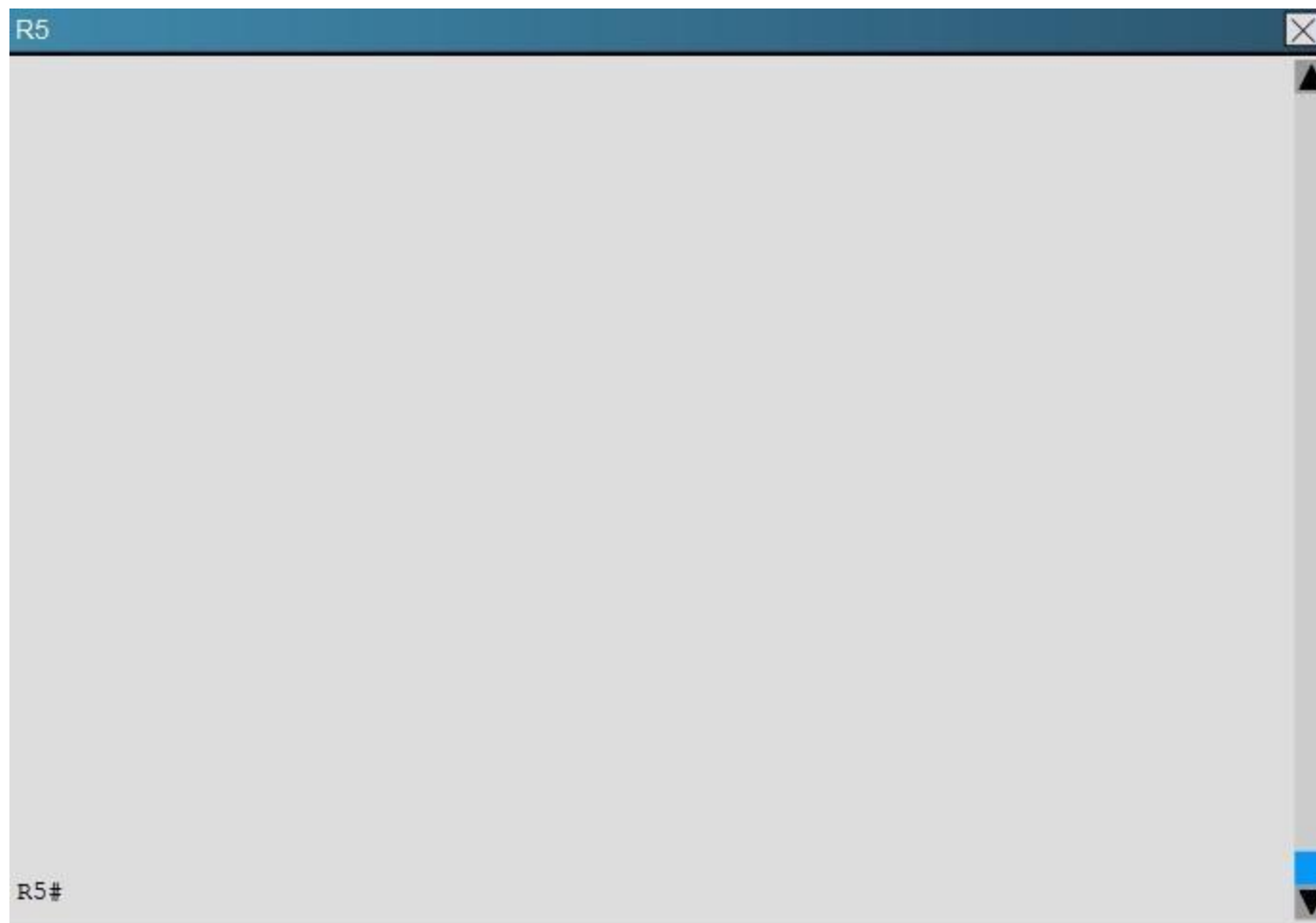














The 6.6.0.0 subnets are not reachable from R4. how should the problem be resolved?

- 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

Correct Answer: D

Section: Troubleshooting OSPF

Explanation

Explanation/Reference:

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.

Topic 6, Ticket 1: Switch Port Trunk

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

Client Should have IP 10.2.1.3

EIGRP 100 is running between switch DSW1 & DSW2

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

Network of OSPF is redistributed in EIGRP

BGP 65001 is configured on R1 with Webserver cloud AS 65002 HSRP is running between DSW1 & DSW2 Switches

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

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

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.

DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.

R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISPs network. Because the companys 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 R4s 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.

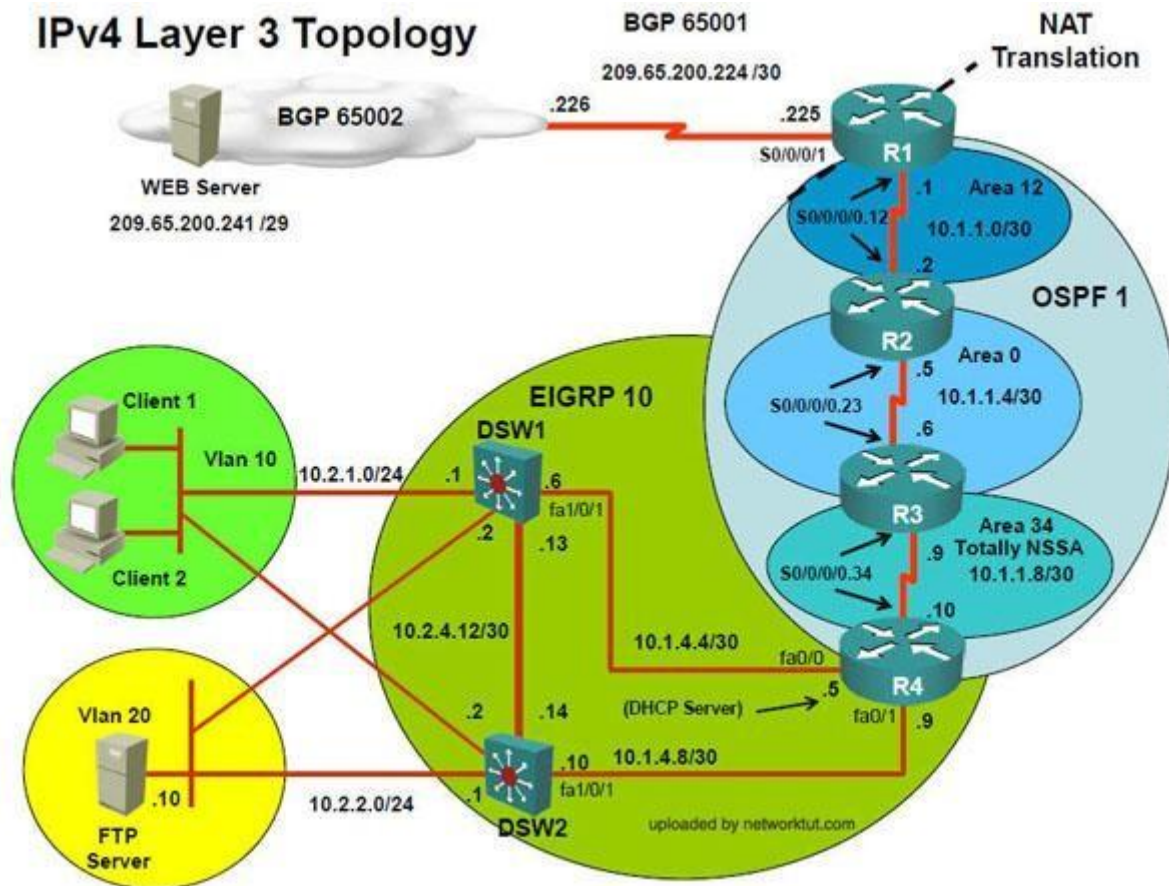
Question-1 Fault is found on which device,

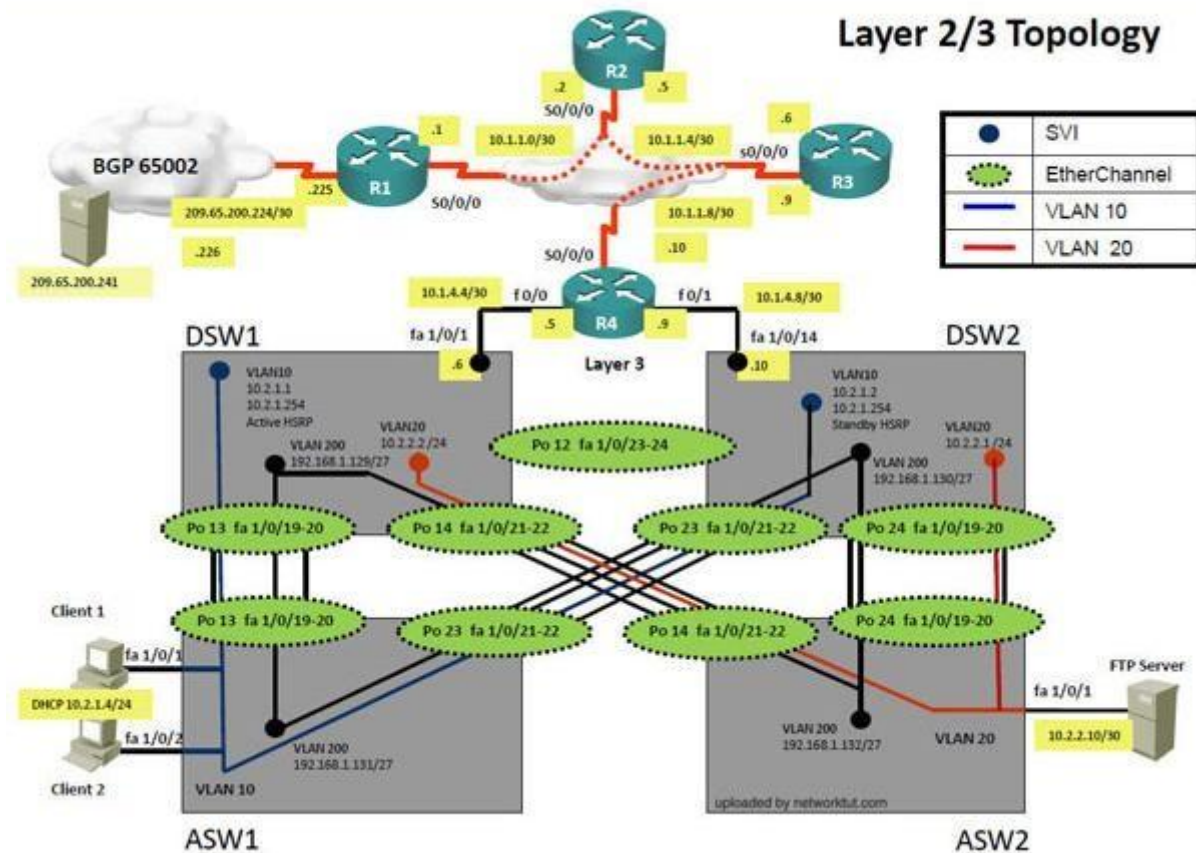
Question-2 Fault condition is related to,

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:-

1. 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
2. On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24
Sh run ----- & check for running config of int fa1/0/1 & fa1/0/2

```
=====
interface FastEthernet1/0/1
switchport mode access
switchport access vlan 10
```

```
interface FastEthernet1/0/2
switchport mode access
switchport access vlan 10
=====
```

3. We need to check on ASW 1 trunk port the trunk Po13 & Po23 were receiving VLAN 20 & 200 but not VLAN 10 so that switch could not get DHCP IP address and was failing to reach IP address of Internet

```
ASW1>sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Po13      on        802.1q         trunking    1
Po23      auto      802.1q         trunking    1

Port      Vlans allowed on trunk
Po13      20,200
Po23      20,200

Port      Vlans allowed and active in management domain
Po13      200
Po23      200

Port      Vlans in spanning tree forwarding state and not pruned
Po13      200
Po23      none
```

4. Change required: On ASW1 below change is required for switch-to-switch connectivity..

```
int range portchannel13,portchannel23
switchport trunk allowed vlan none
switchport trunk allowed vlan 10,200
```

QUESTION 21

The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, and FHRP services, a trouble ticket has been operated indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to Isolated the cause of this fault and answer the following questions.

On which device is the fault condition located?

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

Correct Answer: G

Section: Ticket 1: Switch Port Trunk

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 22

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

Correct Answer: B

Section: Ticket 1: Switch Port Trunk

Explanation

Explanation/Reference:

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.

QUESTION 23

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.

What is the solution to the fault condition?

- A. In Configuration mode, using the interface port-channel 13 command, then configureswitchport trunk allowed vlan none followed by switchport trunk allowed vlan 20,200 commands.
- B. In Configuration mode, using the interface port-channel 13, port-channel 23, then configure switchport trunk none allowed vlan none followed by switchport trunk allowed vlan 10,200 commands.
- C. In Configuration mode, using the interface port-channel 23 command, then configure switchport trunk allowed vlan none followed by switchport trunk allowed vlan 20,200 commands.
- D. In Configuration mode, using the interface port-channel 23, port-channel, then configure switchport trunk allowed vlan none followed by switchport trunk allowed vlan 10,20,200 commands.

Correct Answer: B

Section: Ticket 1: Switch Port Trunk

Explanation

Explanation/Reference:

Explanation:

We need to allow VLANs 10 and 200 on the trunks to restore full connectivity. This can be accomplished by issuing the "switchport trunk allowed vlan 10,200" command on the port channels used as trunks in DSW1.

Topic 7, Ticket 2 : ACCESS VLAN

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

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002 o
- o 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 ISPs network. Because the companys 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 R4s 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,

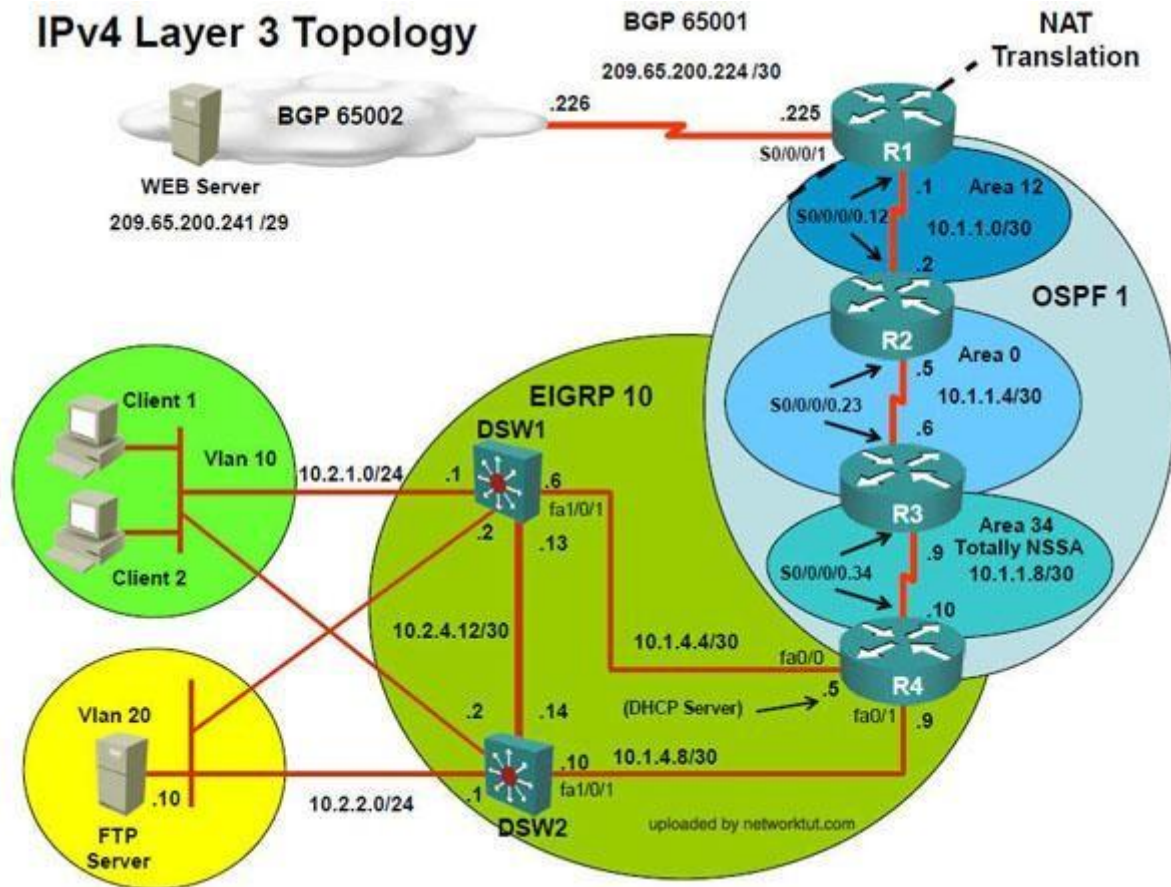
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

=====

IPv4 Layer 3 Topology




```
=====
interface FastEthernet1/0/1
description link to Client 1
switchport mode access
switchport nonegotiate
spanning-tree portfast

interface FastEthernet1/0/2
description link to Client 2
switchport mode access
switchport nonegotiate
spanning-tree portfast
=====
```

3. Here we are not able to see access Vlan10 configured for Port Fa1/0/1 & Fa1/0/2

4. Change required: On ASW1, for configuring Access Vlan under interface fa1/0/1 & 1/0/2 we have to enable command switchport access vlan 10

So in ticket Answer to the fault condition will be as:

QUESTION 24

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

Correct Answer: G

Section: Ticket 2 : ACCESS VLAN

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 25

The implementations group has been using the test bed to do a „proof-of-concept that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to isolated the cause of this fault and answer the following questions.

The fault condition is related to switch technology?

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

Correct Answer: D

Section: Ticket 2 : ACCESS VLAN

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 26

The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to isolated the cause of this fault and answer the following questions.

What is the solution to the fault condition?

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

Correct Answer: D

Section: Ticket 2 : ACCESS VLAN

Explanation

Explanation/Reference:

Explanation:

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

Topic 8, Ticket 3 : OSPF Authentication

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

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002
- o 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 ISPs network. Because the companys 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 R4s DHCP server.

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

In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.

DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.

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

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

Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution. Each ticket has 3 sub questions that need to be answered & topology remains same.

Question-1 Fault is found on which device,

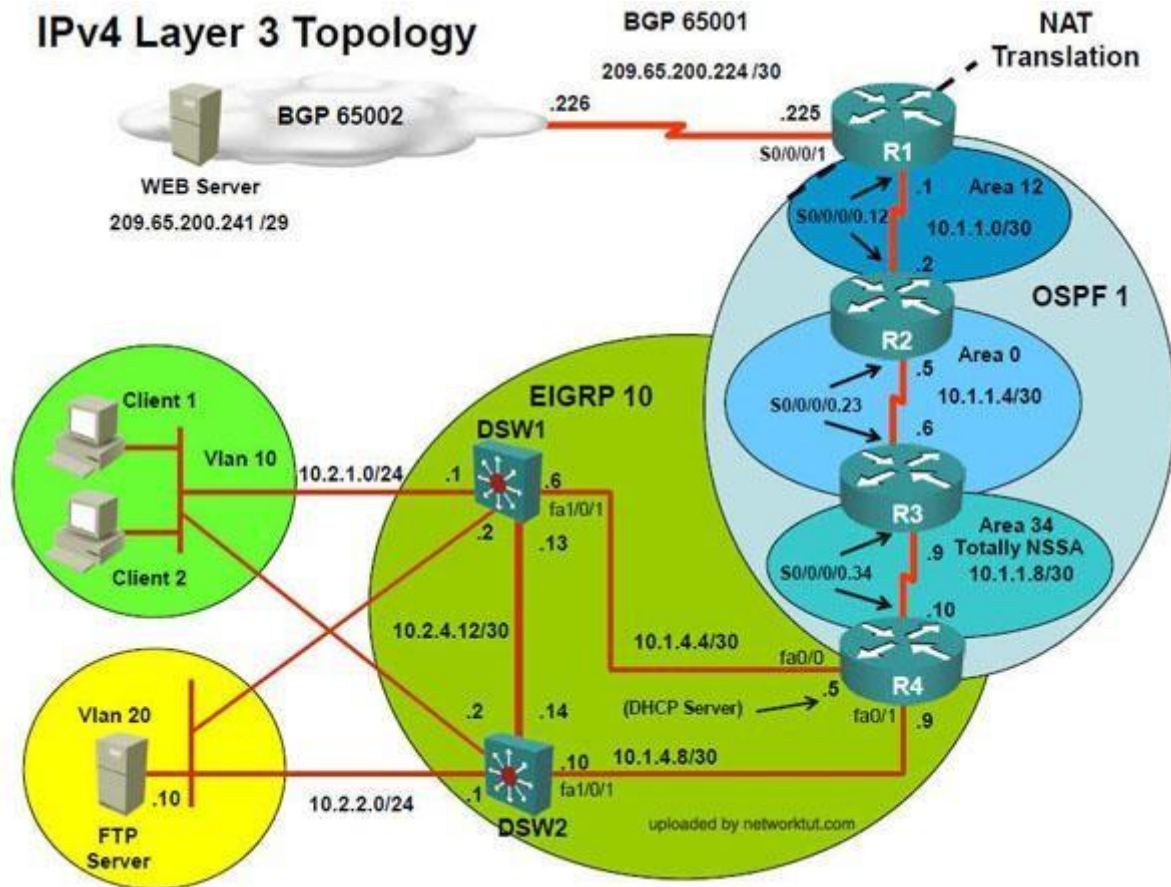
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

=====

IPv4 Layer 3 Topology



<pre> R1> R1>ping 10.2.1.3 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 0 percent (0/5) </pre>	<pre> R2>ping 10.2.1.3 Type escape sequence to a Sending 5, 100-byte ICMP !!!! Success rate is 100 perce </pre>
---	---

3. Check for neighborship of ospf
 shipospfnei ----- Only one neighborship is forming with R2 & i.e. with R3

Since R2 is connected to R1 & R3 with routing protocol ospf than there should be 2 neighbors seen but only one is seen

4. Need to check running config of R2 & R3 for interface Sh run ----- Interface Serial0/0/0/0.12 on R2

```

R1
duplex auto
speed auto
!
interface Serial0/0/0
description Link to R2
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly
encapsulation frame-relay
ip ospf message-digest-key 1 md5 TSHOOT
ip ospf network point-to-point
ip ospf priority 0
ip ospf 1 area 12
ipv6 address 2026::12:1/122
ipv6 ospf network point-to-point
ipv6 ospf 6 area 12
frame-relay map ipv6 FE80::2 403
frame-relay map ip 10.1.1.1 403 broadcast
frame-relay map ip 10.1.1.2 403
frame-relay map ipv6 2026::12:1 403 broadcast
frame-relay map ipv6 2026::12:2 403
no frame-relay inverse-arp
!

R2
speed auto
!
interface Serial0/0/0
no ip address
encapsulation frame-relay
no frame-relay inverse-arp
!
interface Serial0/0/0.12 point-to-point
description Link to R1
ip address 10.1.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 TSHOOT
ipv6 address 2026::12:2/122
ipv6 address FE80::2 link-local
ipv6 ospf 6 area 12
frame-relay interface-dlci 304
!
interface Serial0/0/0.23 point-to-point
description Link to R3
ip address 10.1.1.5 255.255.255.252
ipv6 address 2026::1:1/123
ipv6 ospf 6 area 0
frame-relay interface-dlci 302

```

Sh run ----- Interface Serial0/0/0/0 on R1

5. Change required: On R1, for IPV4 authentication of OSPF command is missing and required to configure----- ipospf authentication message-digest

QUESTION 27

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

Correct Answer: A

Section: Ticket 3 : OSPF Authentication

Explanation

Explanation/Reference:

Explanation:

On R1, for IPV4 authentication of OSPF the command is missing and required to configure----- ipospf authentication message-digest

QUESTION 28

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

Correct Answer: D

Section: Ticket 3 : OSPF Authentication**Explanation****Explanation/Reference:**

Explanation:

On R1, for IPV4 authentication of OSPF the command is missing and required to configure----- ipospf authentication message-digest

QUESTION 29

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 ipospf 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.

Correct Answer: A

Section: Ticket 3 : OSPF Authentication**Explanation****Explanation/Reference:**

Explanation:

On R1, for IPV4 authentication of OSPF the command is missing and required to configure----- ipospf authentication message-digest

Topic 9, Ticket 4 : BGP Neighbor

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

o

Client Should have IP 10.2.1.3

o

EIGRP 100 is running between switch DSW1 & DSW2

o

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

o

Network of OSPF is redistributed in EIGRP

o

BGP 65001 is configured on R1 with Webserver cloud AS 65002 o

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 ISPs network. Because the companys 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 R4s 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.

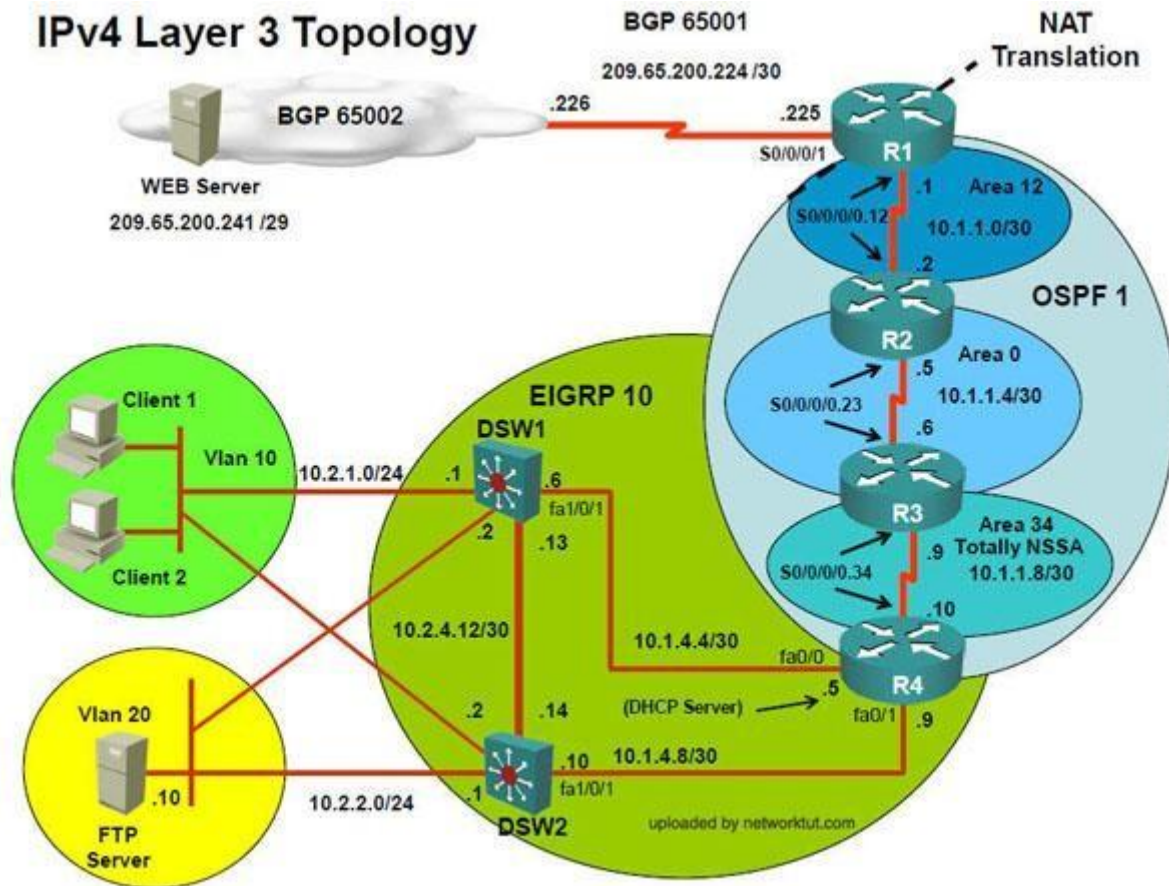
Question-1 Fault is found on which device,

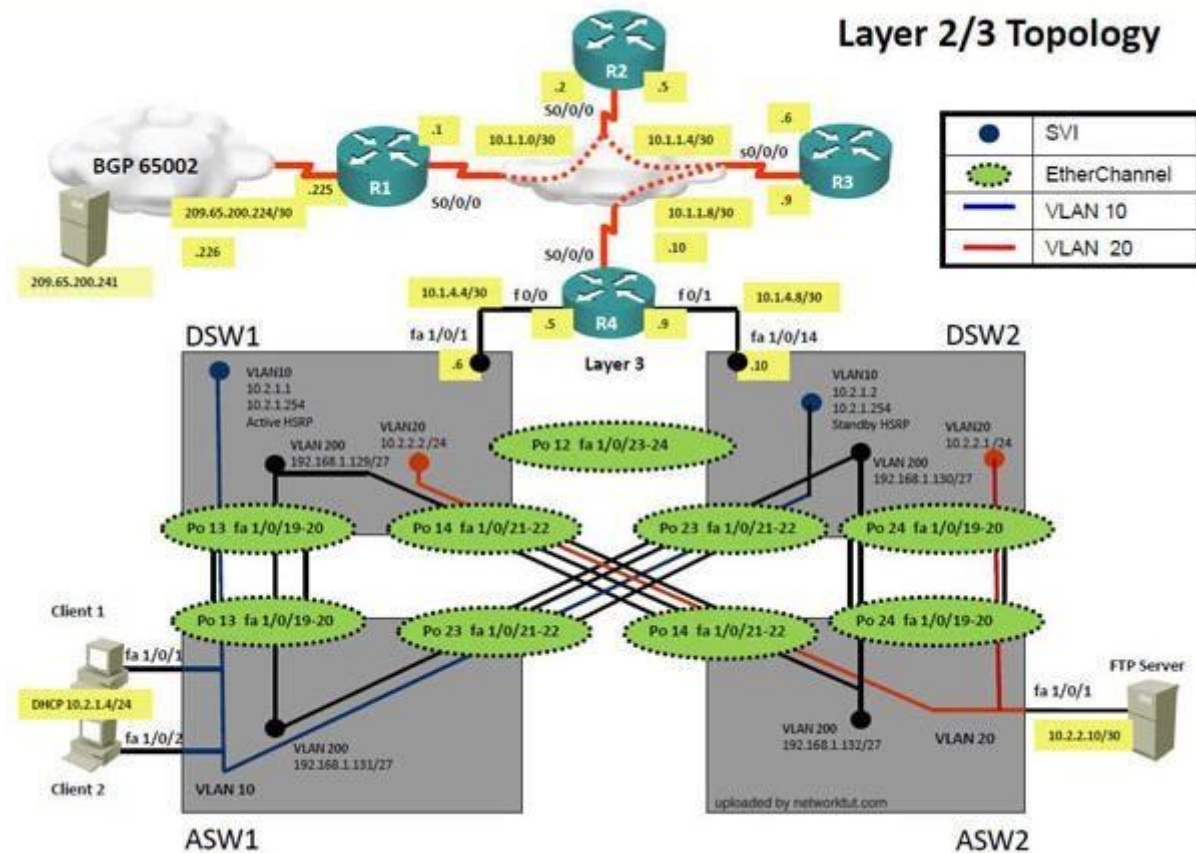
Question-2 Fault condition is related to,

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:-

- 1) 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
- 2) IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1
- 3) Look for BGP Neighbourship

Shippbgp summary ----- No O/P will be seen

4) Check for interface IP & ping IP 209.65.200.225 ---- Reply will be received from Webserver interface

5) Look for peering IP address via sh run on R1 interface serial 0/0/1

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

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

6) 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.

7) 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

QUESTION 30

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

Correct Answer: A

Section: Ticket 4 : BGP Neighbor

Explanation

Explanation/Reference:

Explanation:

The BGP neighbor statement is wrong on R1.

QUESTION 31

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

Correct Answer: A

Section: Ticket 4 : BGP Neighbor

Explanation

Explanation/Reference:

Explanation:

On R1 under router the BGP process Change neighbor 209.56.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65002

QUESTION 32

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 65001 command.
- 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.

Correct Answer: D

Section: Ticket 4 : BGP Neighbor

Explanation

Explanation/Reference:

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

Topic 10, Ticket 5 : NAT ACL

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

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002
- o 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.

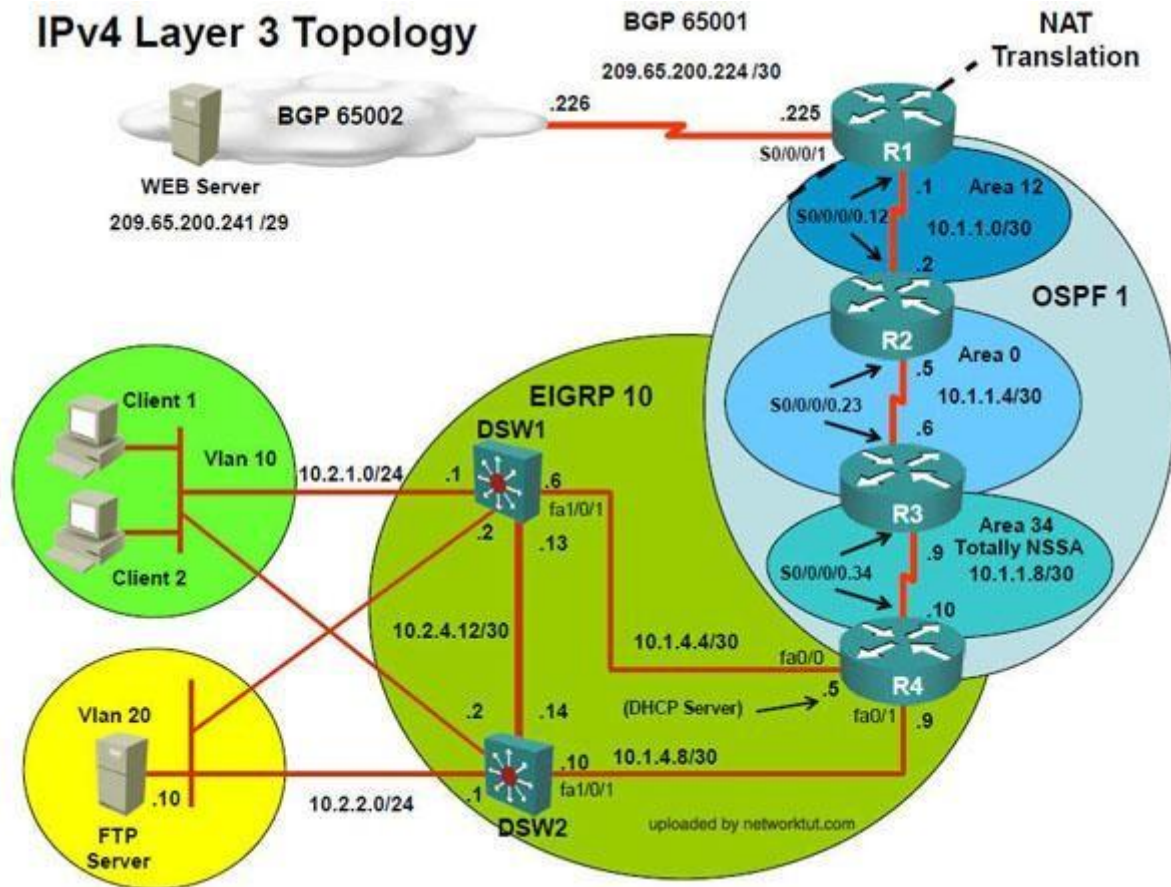
Question-1 Fault is found on which device,

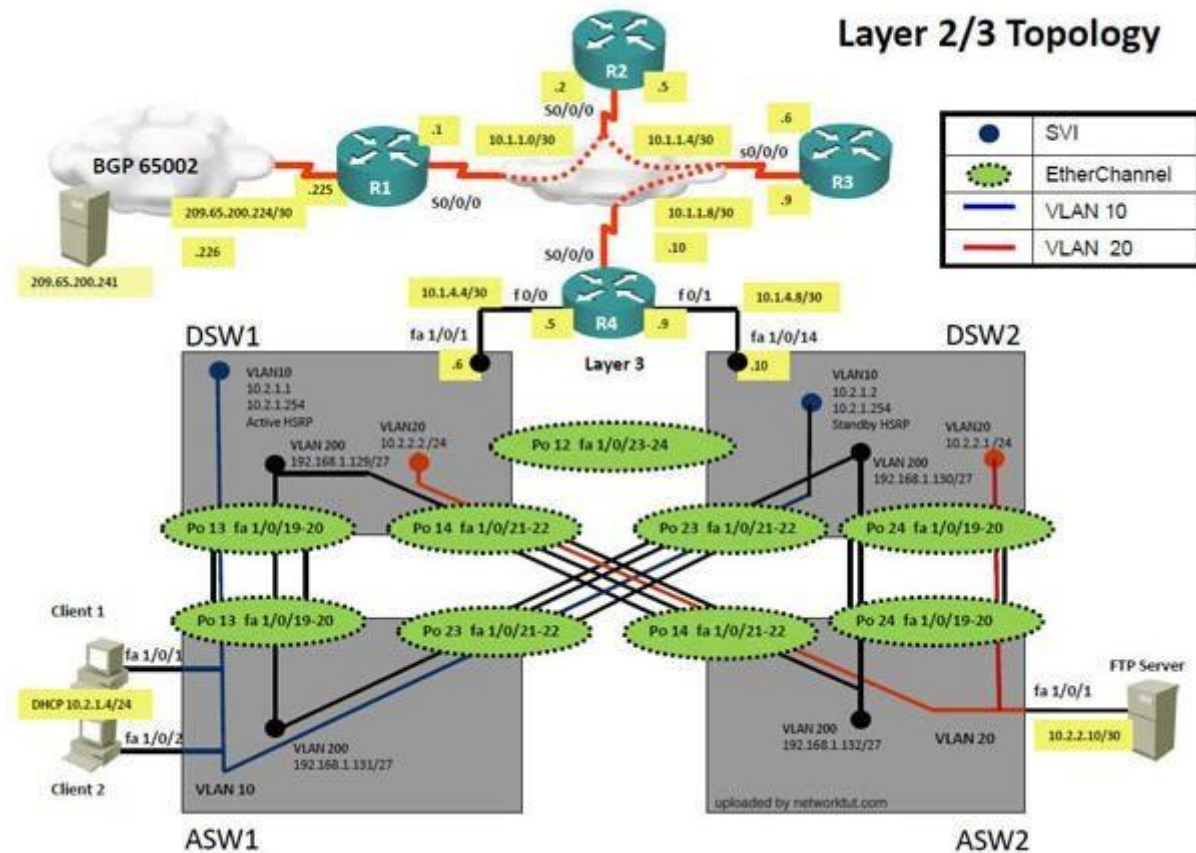
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology





Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

- 1) 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
- 2) IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1
- 3) Look for BGP Neighbourship
Shippbgp summary ----- State of BGP will be in established state & will be able to receive I prefix (209.65.200.241)

- 4) As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of webserver & we are able to ping the same from R1. Further troubleshooting needs to be done on R1 on serial 0/0/1
- 5) Check for running config. i.esh run for interface serial 0/0/1..

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

!

```
ip http server
no ip http secure-server
ip nat inside source list nat_traffic interface Serial0/0/1 overload
!
ip access-list standard nat_traffic
permit 10.1.0.0 0.0.255.255
!
ipv6 router ospf 6
log-adjacency-changes
```

!

From above snapshot we are able to see that IP needs to be PAT to serial 0/0/1 to reach web server IP

(209.65.200.241). But in access-list of NAT IP allowed IP is 10.1.0.0/16 is allowed & need 10.2.0.0 /16 to

6) As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of web server & we are able to ping the same from R1. Its should be checked further for running config of interface for stopping

7) Change required: 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.

QUESTION 33

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

Correct Answer: A

Section: Ticket 5 : NAT ACL

Explanation

Explanation/Reference:

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.

QUESTION 34

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

Correct Answer: C

Section: Ticket 5 : NAT ACL

Explanation

Explanation/Reference:

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.

QUESTION 35

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

Correct Answer: C

Section: Ticket 5 : NAT ACL

Explanation

Explanation/Reference:

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)

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002
- o 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.

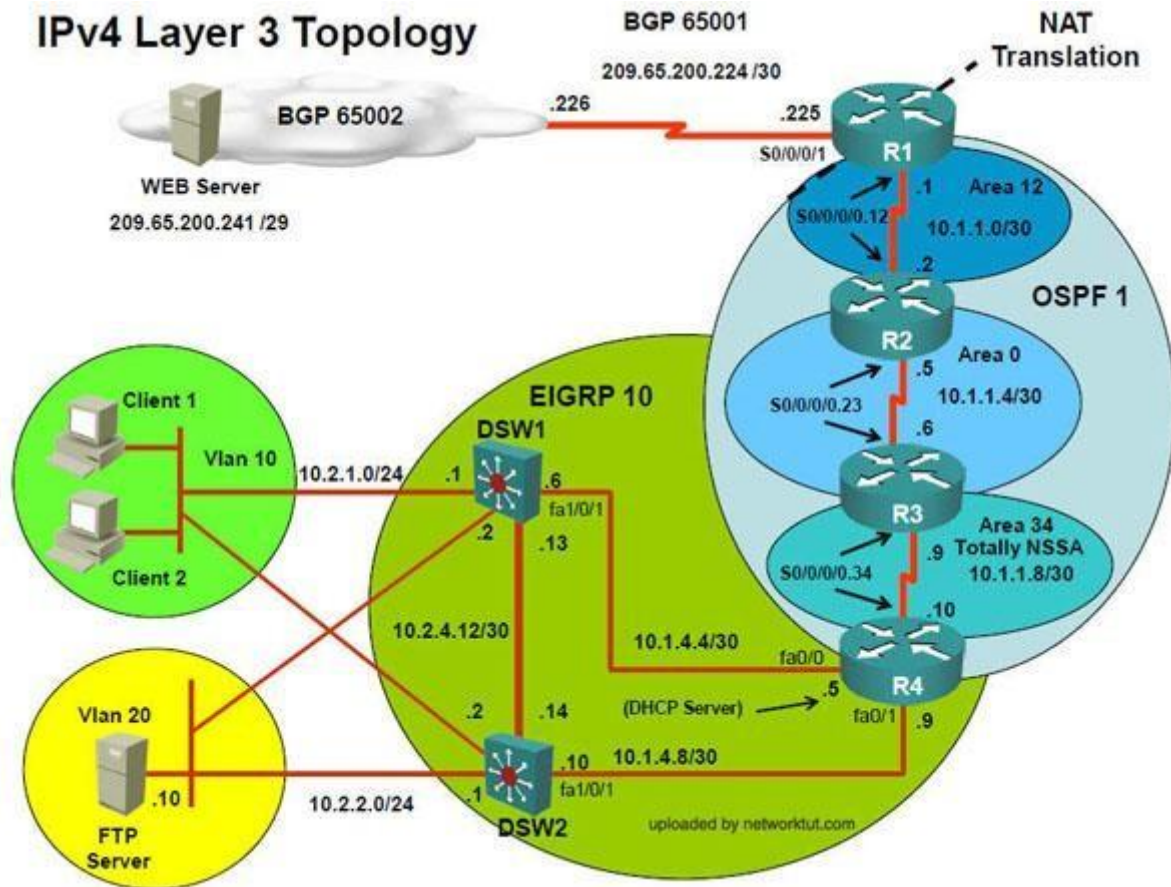
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology



5) Shipbgp summary ----- State of BGP will be in active state. This means connectivity issue between serial

6) Check for running config. i.esh 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)

```
interface Serial0/0/1
description Link to ISP
ip address 209.65.200.225 255.255.255.252
ip access-group edge_security in
ip nat outside
ip virtual-reassembly
ntp broadcast client
ntp broadcast key 1
no cdp enable
```

```
ip nat inside source list nat_traffic interface Serial0/0/1 overload
!
ip access-list standard nat_traffic
permit 10.1.0.0 0.0.255.255
permit 10.2.0.0 0.0.255.255
!
ip access-list extended edge_security
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
permit ip host 209.65.200.241 any
!
```

7) In above snapshot we can see that access-list of edge_security on R1 is not allowing wan IP network

8) Change required: On R1, we need to permit IP 209.65.200.222/30 under the access list.

QUESTION 36

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

Correct Answer: A

Section: Ticket 6 : R1 ACL

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 37

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

Correct Answer: G

Section: Ticket 6 : R1 ACL

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 38

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 0.255.255.255 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.

Correct Answer: B

Section: Ticket 6 : R1 ACL

Explanation

Explanation/Reference:

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)

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002 o
- o 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.

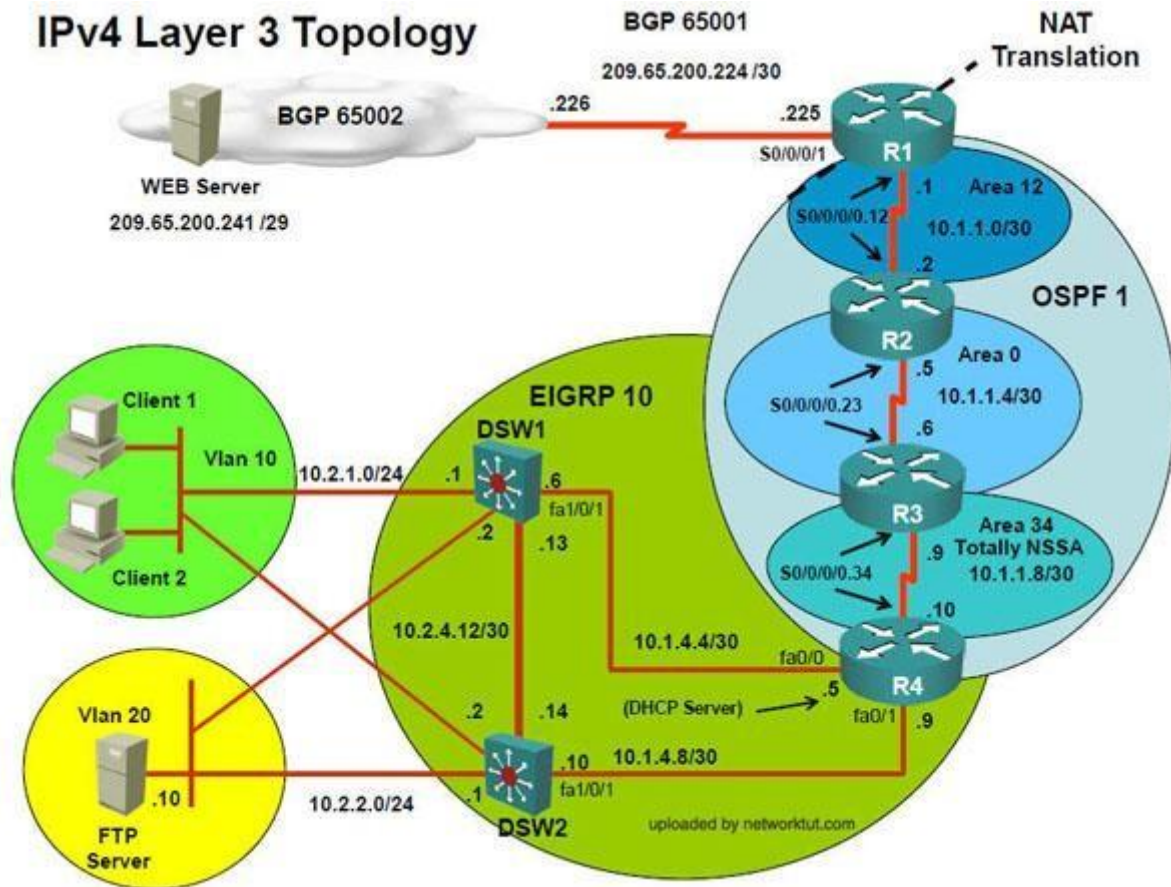
Question-1 Fault is found on which device,

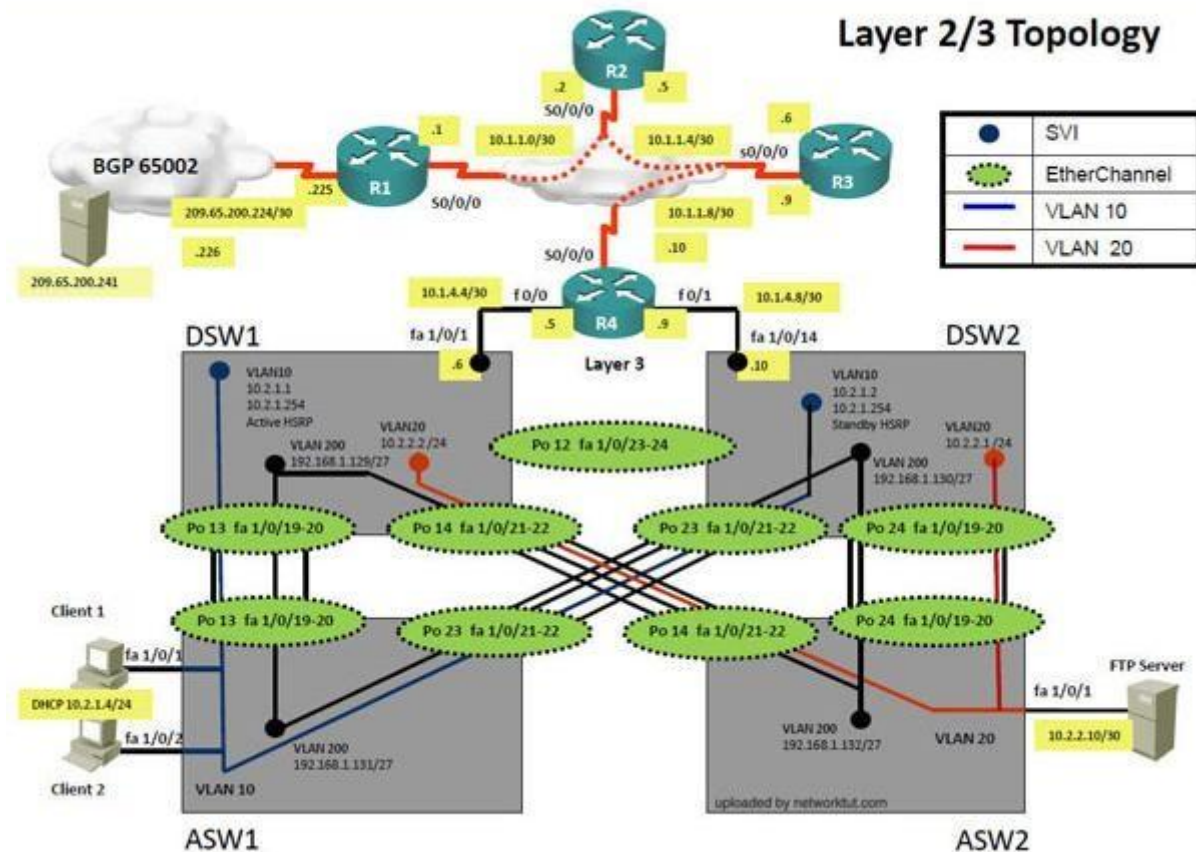
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology





Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

- 1) 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
- 2) 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

Shint fa1/0/1 &shint fa1/0/2

```
ASW1
FastEthernet1/0/1 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 001b.90ab.bc83 (bia 001b.90ab.bc83)
Description: link to Client 1
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

```
ASW1
FastEthernet1/0/2 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 001b.90ab.bc84 (bia 001b.90ab.bc84)
Description: link to Clint 2
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

3) As seen on interface the port is in err-disable mode so need to clear port.

4) Change required: On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2.

QUESTION 39

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

Correct Answer: G

Section: Ticket 7 : Port Security

Explanation

Explanation/Reference:

Explanation:

port security needs is configured on ASW1.

QUESTION 40

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 Vlan
- D. Port Security
- E. VLAN ACL / Port ACL
- F. Switch Virtual Interface

Correct Answer: D

Section: Ticket 7 : Port Security

Explanation

Explanation/Reference:

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

QUESTION 41

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

Correct Answer: B

Section: Ticket 7 : Port Security

Explanation

Explanation/Reference:

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

=====

Topic 13, Ticket 8 : Redistribution of EIGRP to OSPF

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

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP

o
BGP 65001 is configured on R1 with Webserver cloud AS 65002 o
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.

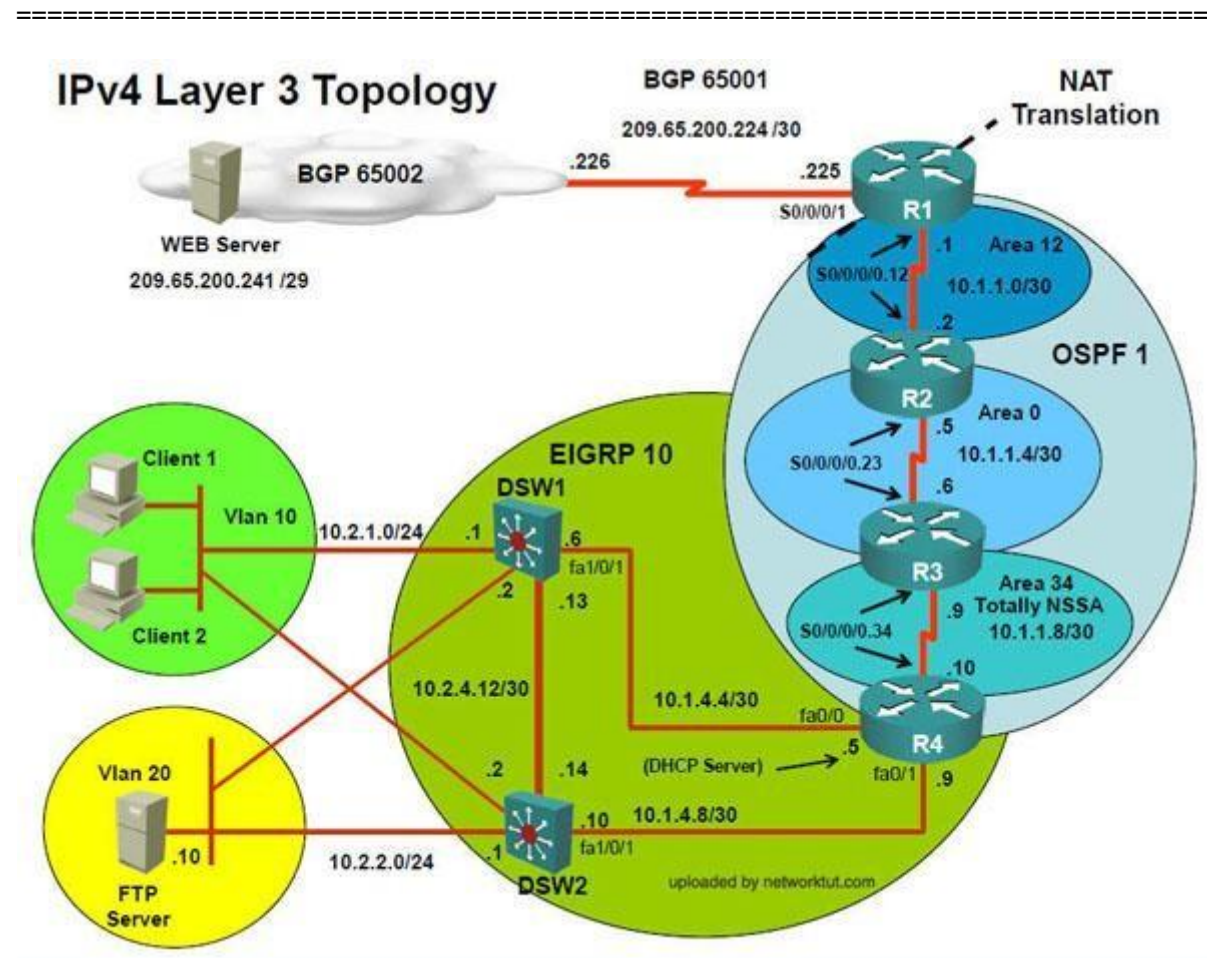
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.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

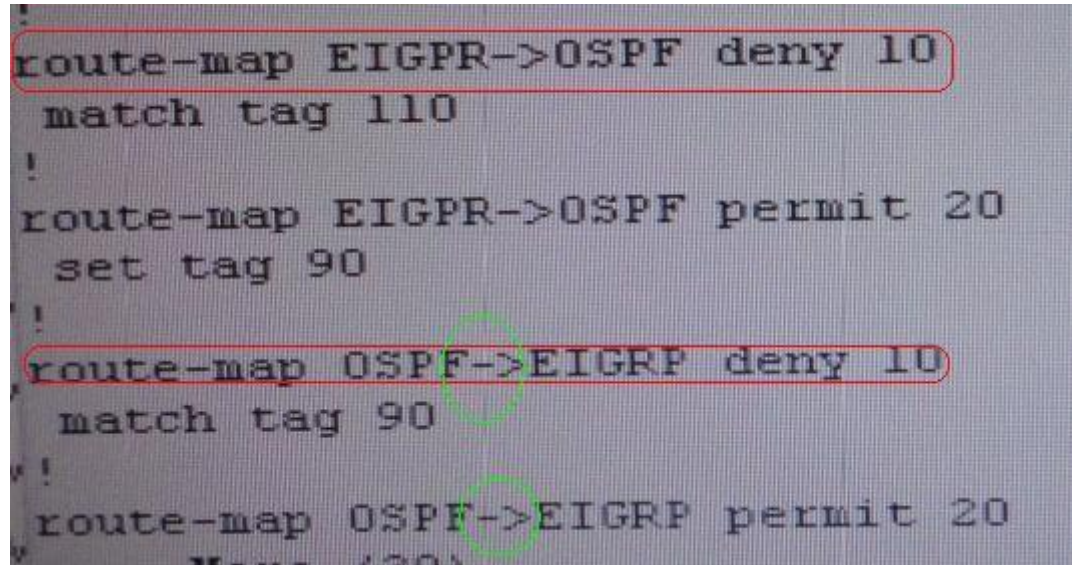
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution



- 4) 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.
5) Need to check the routes are being advertised properly or not in OSPF & EIGRP vice-versa.

```
!
router eigrp 10
 redistribute ospf 1 route-map OSPF_to_EIGRP
 network 10.1.4.0 0.0.0.255
 network 10.1.10.0 0.0.0.255
 network 10.1.21.128 0.0.0.3
 default-metric 100000 100 100 1 1500
 auto-summary
!
router ospf 1
 log-adjacency-changes
 area 34 nssa
 summary-address 10.2.0.0 255.255.0.0
 redistribute eigrp 10 subnets route-map EIGRP->OSPF
 network 10.1.1.0 0.0.0.255 area 34
 network 10.1.2.0 0.0.0.255 area 34
```

```
!
route-map EIGRP->OSPF deny 10
  match tag 110
!
route-map EIGRP->OSPF permit 20
  set tag 90
!
route-map OSPF->EIGRP deny 10
  match tag 90
!
route-map OSPF->EIGRP permit 20
```

6) 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.

7) 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.

QUESTION 42

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

Correct Answer: D

Section: Ticket 8 : Redistribution of EIGRP to OSPF

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 43

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

Correct Answer: E

Section: Ticket 8 : Redistribution of EIGRP to OSPF

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 44

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.

Which is the solution to the fault condition?

- A. Under the EIGRP process, delete the redistribute ospf 1 route-map OSPF_ to_ EIGRP command and enter the redistribute ospf 1 route-map OSPF - > EIGRP command.
- B. Under the EIGRP process, delete the redistribute ospf 1 route-map OSPF_ to_ EIGRP command and enter the redistribute ospf 6 metric route-map OSPF - > EIGRP command.
- C. Under the OSPF process, delete the redistribute eigrp10 subnets route-map EIGPR ->OSPF command and enter the redistribute eigrp10 subnets route-map OSPF - > EIGRP command.
- D. Under the OSPF process, delete the redistribute eigrp10 subnets route-map EIGPR ->OSPF command and enter the redistribute eigrp10 subnets route-map EIGPR - > OSPF command.
- E. Under the EIGRP process, delete the redistribute ospf 1 route-map OSPF _to_ EIGRP command and enter redistribute ospf 1 metric 100000 100 100 1 15000 route_ map OSPF _to_ _EIGRP command

Correct Answer: A

Section: Ticket 8 : Redistribution of EIGRP to OSPF

Explanation

Explanation/Reference:

Explanation:

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

===== Topic 14, Ticket 9 : EIGRP AS number

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

o

Client Should have IP 10.2.1.3

o

EIGRP 100 is running between switch DSW1 & DSW2

o

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

o

Network of OSPF is redistributed in EIGRP

o

BGP 65001 is configured on R1 with Webserver cloud AS 65002 o

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.

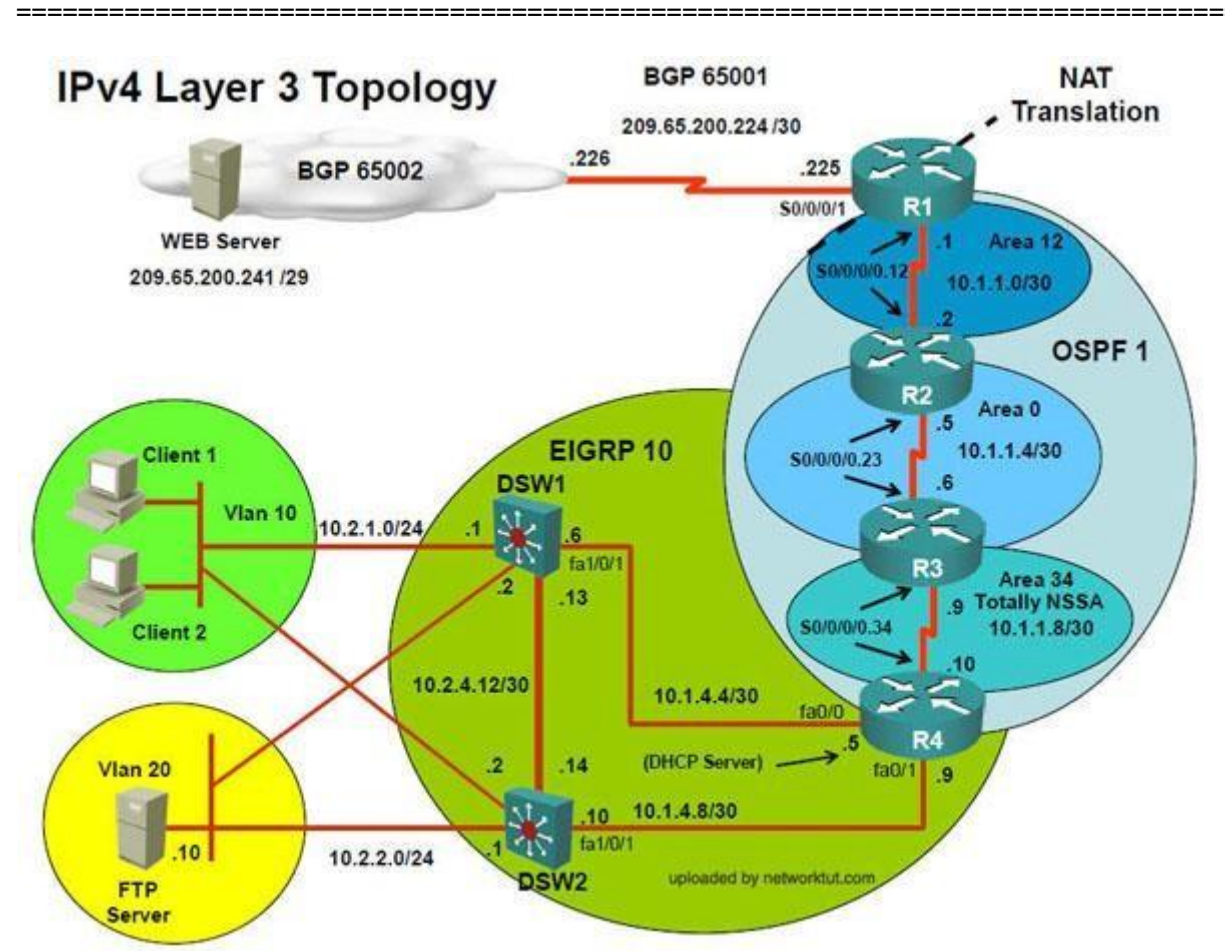
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

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



4) This clearly shows problem at R4 Kindly check routes in EIGRP there are no routes of eigrp.

5) Check the neighborship of EIGRP on R4; there are no neighbor seen from DSW1 & DSW2 check the running config of EIGRP protocol it shows EIGRP AS 1 process.... Now check on DSW1 & DSW2 On DSW1 only one Eigrpneighbour is there with DSW2 but its not with R4...

```
DSW1#sh ip eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H   Address                Interface    Hold Uptime    SRTT    RT0    Q    Seq
                               (sec)              (ms)          Cnt Num
1   10.2.4.14              Po12        13 2w0d        2      200    0    73
DSW1#sh ip route
```

6) From above snapshot & since R4 has EIGRP AS number 1 due to which neighbour is not happening.

7) Change required: 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.

QUESTION 45

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

Correct Answer: D

Section: Ticket 9 : EIGRP AS number

Explanation

Explanation/Reference:

Explanation:

The EIGRP AS number configured on R4 is wrong.

QUESTION 46

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

Correct Answer: D

Section: Ticket 9 : EIGRP AS number

Explanation

Explanation/Reference:

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.

QUESTION 47

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. Disable auto summary on the EIGRP process
- B. Enable EIGRP on the FastEthernet0/0 and FastEthernet0/1 interface using the no passive- interface command.
- C. Change the AS number on the EIGRP routing process from 1 to 10 to much the AS number used on DSW1 and DSW2.
- D. Under the EIGRP process, delete the network 10.1.4.0 0.0.0.255 command and enter the network 10.1.4.4 0.0.0.252 and 10.1.4.8 0.0.0.252 commands.

Correct Answer: C

Section: Ticket 9 : EIGRP AS number

Explanation

Explanation/Reference:

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)

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002 o
- o 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.

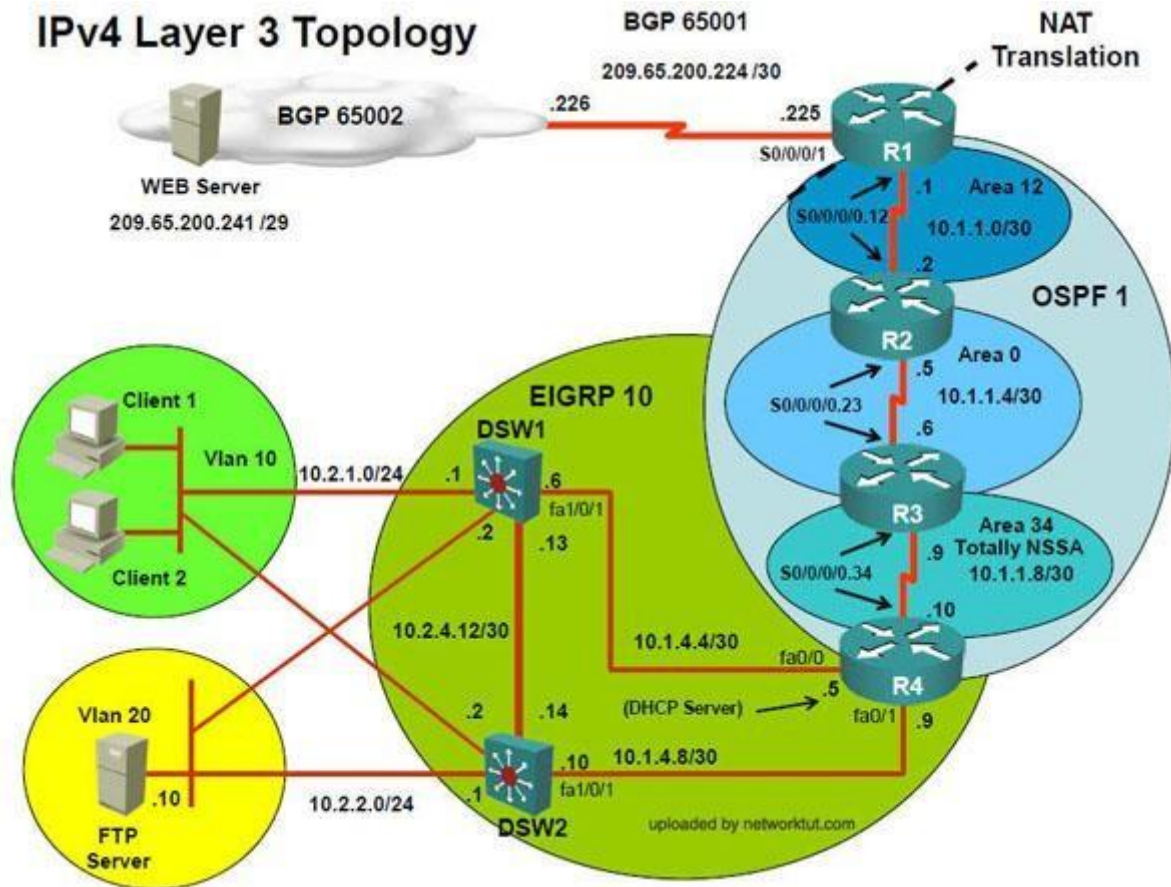
Question-1 Fault is found on which device,

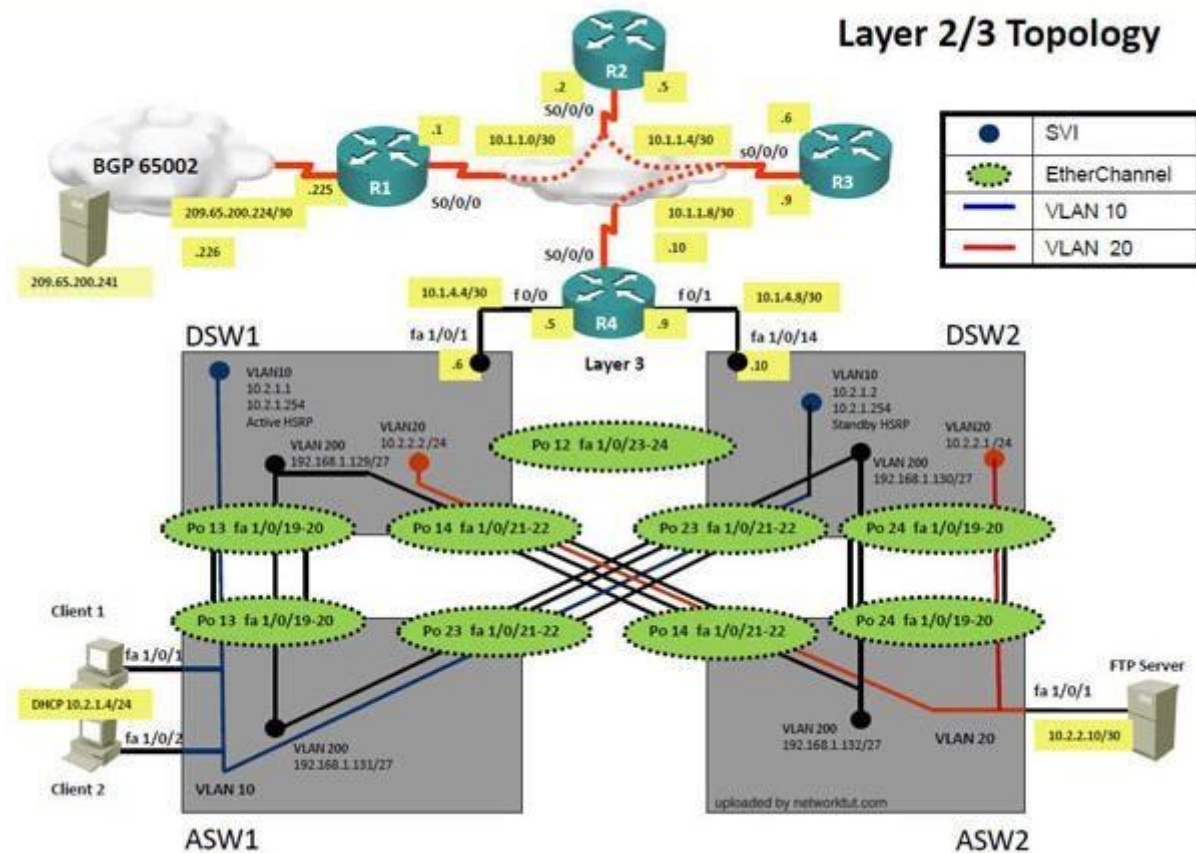
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology





Client 1 is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

- 1) 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
- 2) From Client PC we can ping 10.2.1.254....
- 3) But IP 10.2.1.3 is not able to ping from R4, R3, R2, R1


```
DSW1
vlan access-map test1 10
  action drop
  match ip address 10
vlan access-map test1 20
  action drop
  match ip address 20
vlan access-map test1 30
  action forward
  match ip address 30
vlan access-map test1 40
  action forward
!
vlan filter test1 vlan-list 10
vlan internal allocation policy ascending
```

```
!
access-list 10 permit 10.2.1.3
access-list 20 permit 10.2.1.4
access-list 30 permit 10.2.1.0 0.0.0.255
```

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

QUESTION 48

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 isolate 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

Correct Answer: E

Section: Ticket 10 : VLAN Access Map

Explanation

Explanation/Reference:

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

QUESTION 49

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

Correct Answer: J

Section: Ticket 10 : VLAN Access Map

Explanation

Explanation/Reference:

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

QUESTION 50

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.

Correct Answer: C

Section: Ticket 10 : VLAN Access Map

Explanation

Explanation/Reference:

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)

o

Client Should have IP 10.2.1.3

o

EIGRP 100 is running between switch DSW1 & DSW2

o

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

o

Network of OSPF is redistributed in EIGRP

o

BGP 65001 is configured on R1 with Webserver cloud AS 65002 o

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.

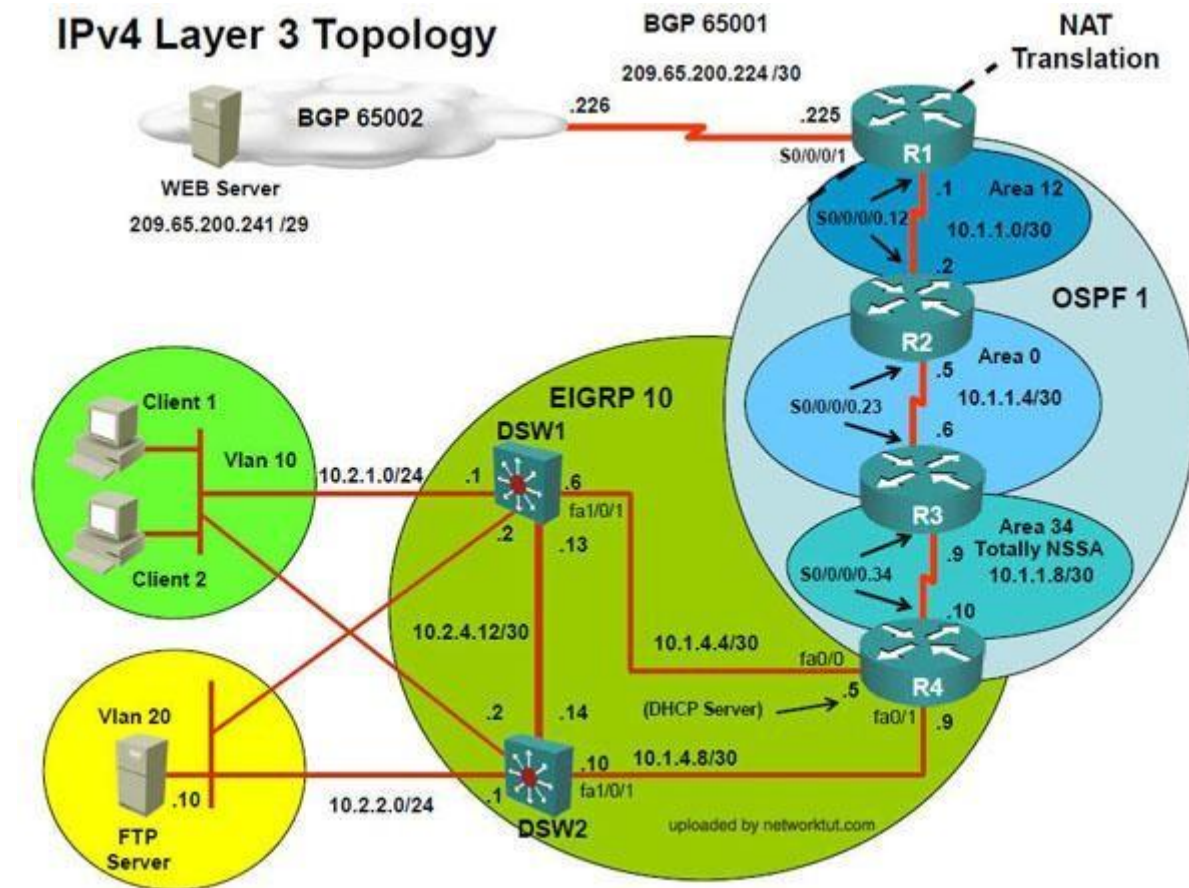
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations. Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

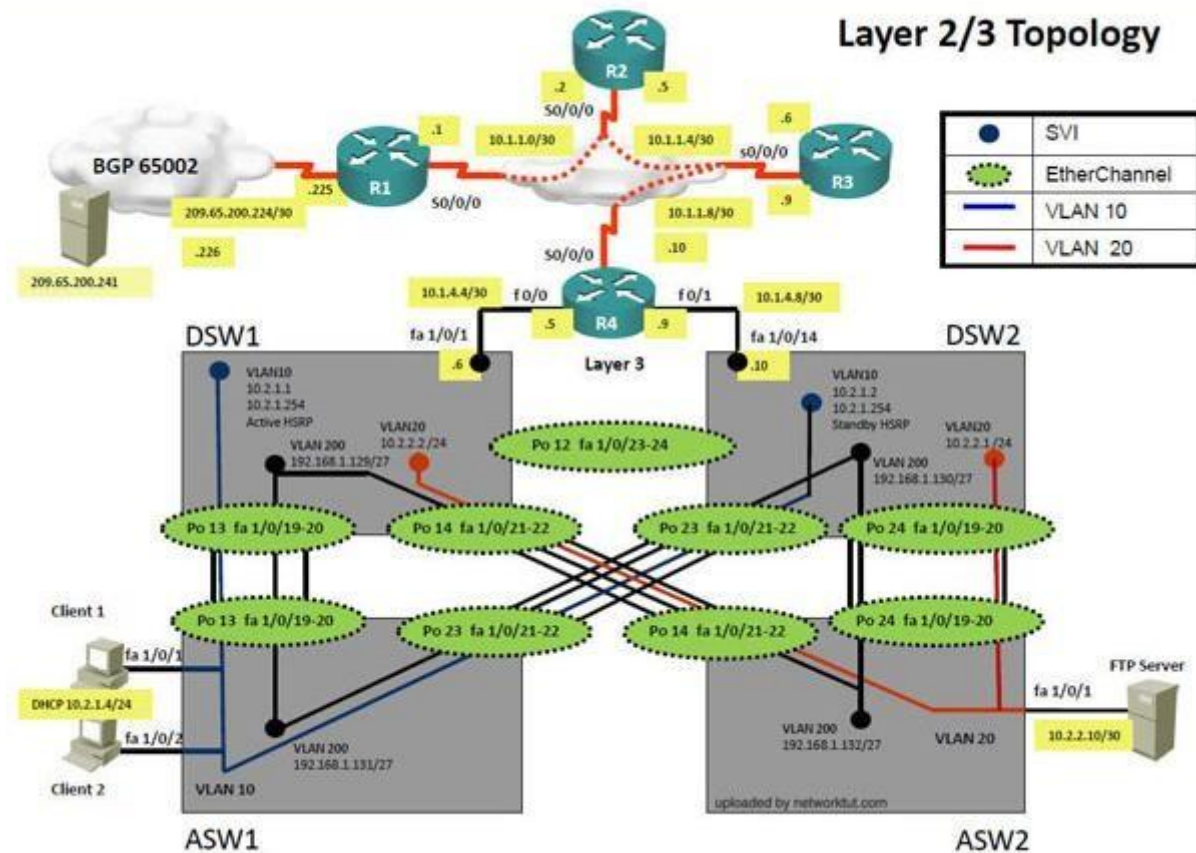
Each ticket has 3 sub questions that need to be answered & topology remains same.

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





Questions

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

Solution

Steps need to follow as below:-

1. 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

2. From Client PC we can ping 10.2.1.254....
3. But IP 10.2.1.3 is able to ping from R4, R3, R2, R1.
4. Since the problem is R1 (2026::111:1) is not able to ping loopback of DSW1 (2026::102:1).
5. 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
!
```

6. 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

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

QUESTION 51

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.

On which device is the fault condition located?

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

Correct Answer: B

Section: Ticket 11 : IPV6 OSPF

Explanation

Explanation/Reference:

Explanation:

R2 is missing the needed IPV6 OSPF for interface s0/0/0.23

QUESTION 52

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

Correct Answer: C

Section: Ticket 11 : IPV6 OSPF

Explanation

Explanation/Reference:

Explanation:

On R2, IPV6 OSPF routing, configuration is required to add ipv6ospf 6 area 0 under interface serial 0/0/0.23

QUESTION 53

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.

What is the solution to fault condition?

- A. Under the interface Serial 0/0/0.23 configuration enter the ipv6 ospf 6 area 0 command.
- B. Under the interface Serial0/0/0.12 configuration enter the ipv6 ospf 6 area 12 command.
- C. Under ipv6 router ospf 6 configuration enter the network 2026::1/122 area 0 command.
- D. Under ipv6 router ospf 6 configuration enter no passive-interface default command.

Correct Answer: A

Section: Ticket 11 : IPV6 OSPF

Explanation

Explanation/Reference:

Explanation:

On R2, IPV6 OSPF routing, configuration is required to add ipv6ospf 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)

- o
- Client Should have IP 10.2.1.3
- o
- EIGRP 100 is running between switch DSW1 & DSW2
- o
- OSPF (Process ID 1) is running between R1, R2, R3, R4
- o
- Network of OSPF is redistributed in EIGRP
- o
- BGP 65001 is configured on R1 with Webserver cloud AS 65002 o
- 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.

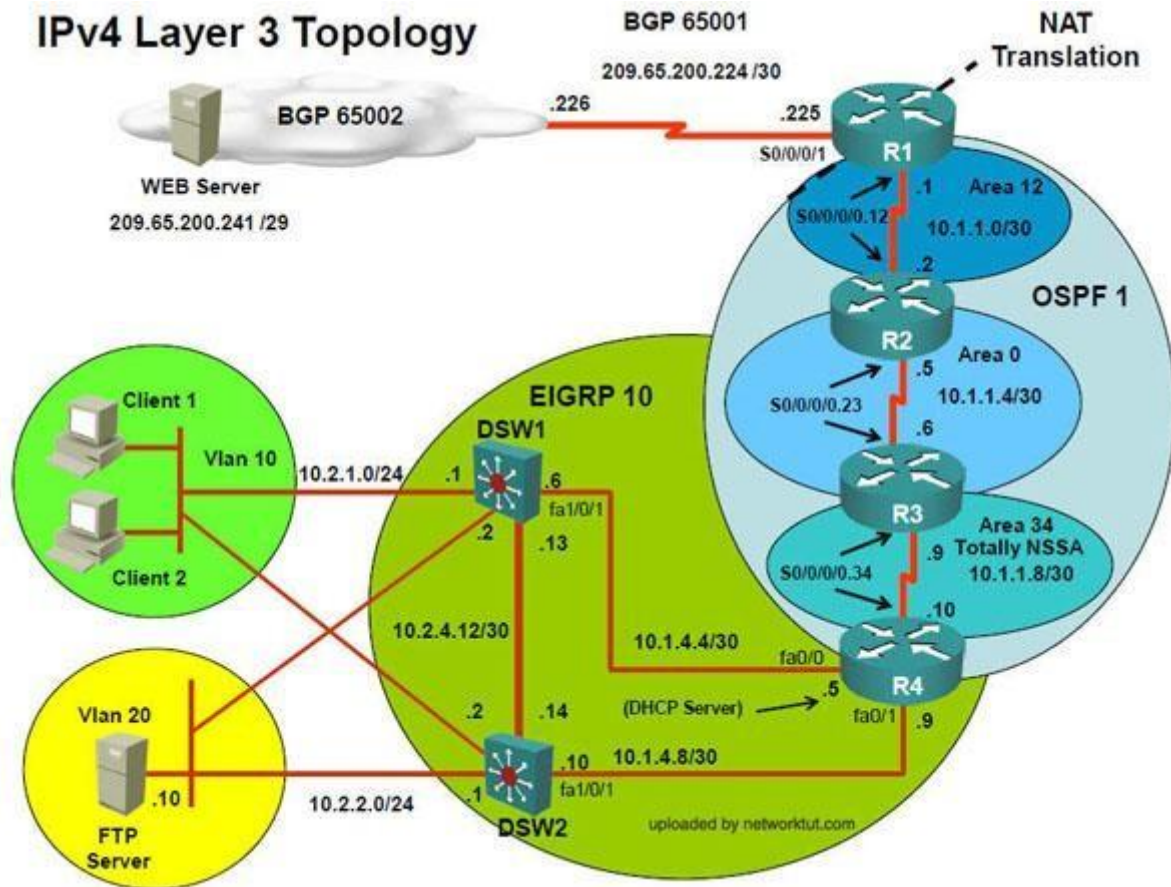
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

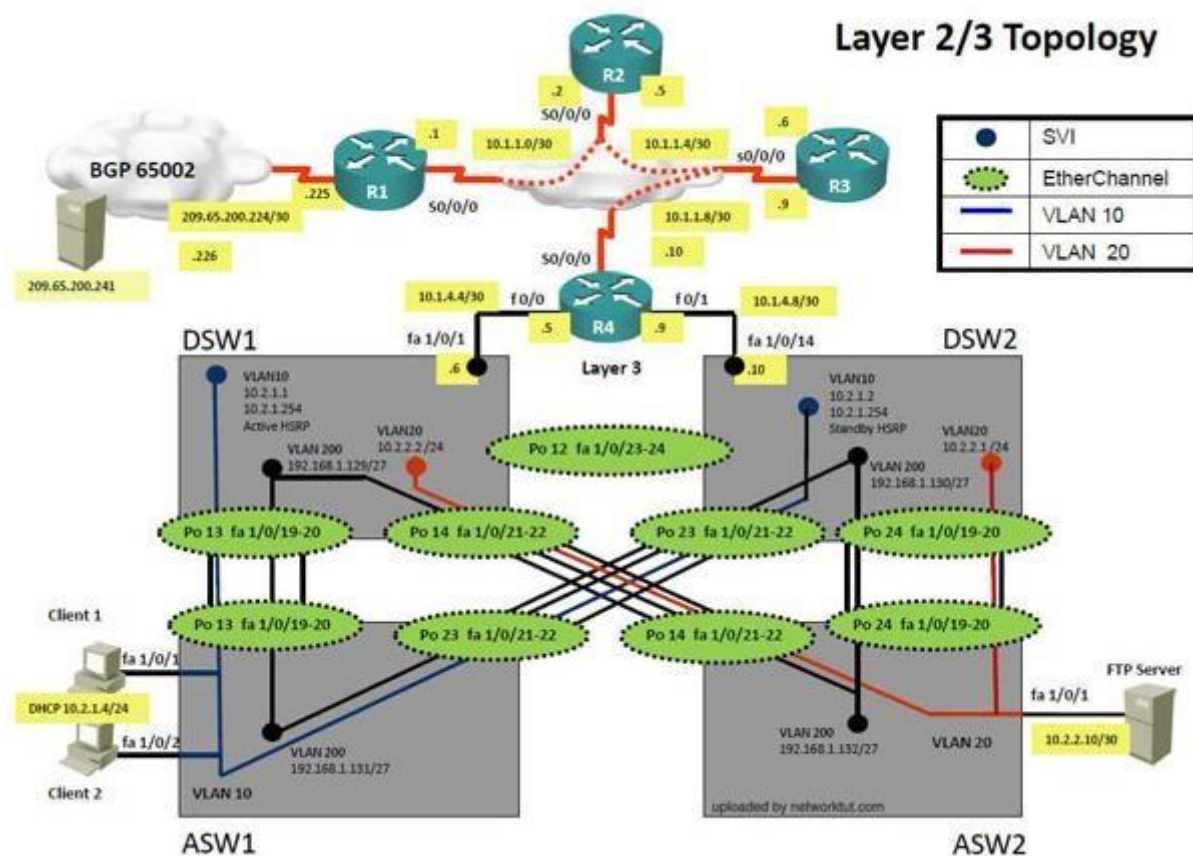
Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



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:-

1. Since the problem is raised that DSW1 will not become active router for HSRP group 10

2. we will check for the HSRP configuration...

DSW1

```
track 1 ip route 10.2.21.128 255.255.255.224 metric threshold
threshold metric up 1 down 2
track 10 ip route 10.1.21.128 255.255.255.224 metric threshold
threshold metric up 61 down 62
no ip subnet-zero
ip routing
ip domain-lookup
```

```
interface Vlan10
ip address 10.2.1.1 255.255.255.0
ip helper-address 10.1.21.129
standby 10 ip 10.2.1.254
standby 10 priority 200
standby 10 preempt
standby 10 track 1 decrement 60
```

DSW2

```
interface Vlan10
ip address 10.2.1.2 255.255.255.0
ip helper-address 10.1.21.129
standby 10 ip 10.2.1.254
standby 10 priority 150
standby 10 preempt
```

3. From snapshot we see that the track command given needs to be changed under active VLAN10 router

4. Change Required: On DSW1, related to HSRP, under vlan 10 change the given track 1 command to instead use the track 10 command.

QUESTION 54

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

Correct Answer: E

Section: Ticket 12 : HSRP Issue

Explanation

Explanation/Reference:

Explanation:

DSW references the wrong track ID number.

QUESTION 55

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 Vlan

Correct Answer: B

Section: Ticket 12 : HSRP Issue

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 56

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

Use the supported commands to isolated the cause of this fault and answer the following questions.

What is the solution to the fault condition?

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

Correct Answer: D

Section: Ticket 12 : HSRP Issue

Explanation

Explanation/Reference:

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)

- o Client Should have IP 10.2.1.3
- o EIGRP 100 is running between switch DSW1 & DSW2
- o OSPF (Process ID 1) is running between R1, R2, R3, R4
- o Network of OSPF is redistributed in EIGRP
- o BGP 65001 is configured on R1 with Webserver cloud AS 65002 o
- o 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.

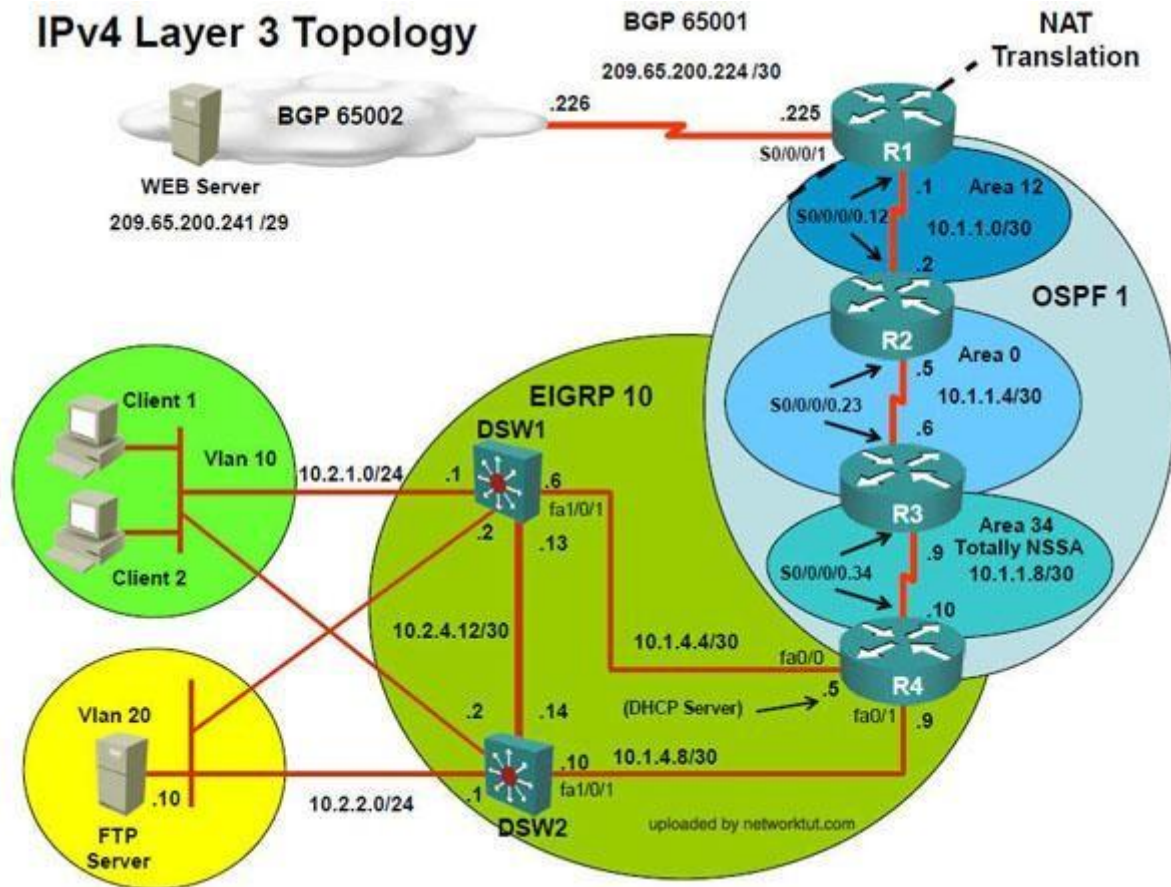
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

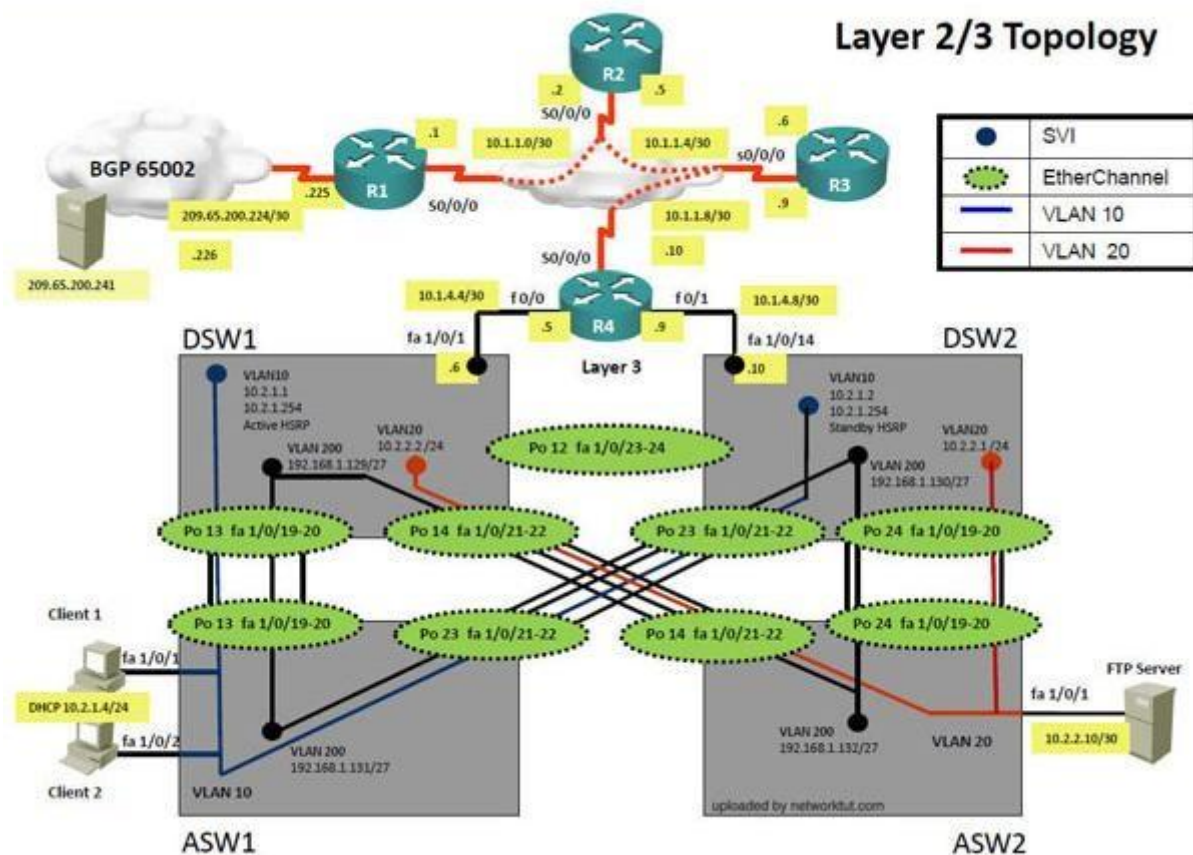
Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



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:-

1. 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
2. From ASW1 we can ping 10.2.1.254....

3. 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

QUESTION 57

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

Correct Answer: D

Section: Ticket 13 : DHCP Issue

Explanation

Explanation/Reference:

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

QUESTION 58

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.

Correct Answer: B

Section: Ticket 13 : DHCP Issue

Explanation

Explanation/Reference:

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

QUESTION 59

The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to isolate the cause of this fault and answer the following question.

What is the solution to the fault condition?

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

Correct Answer: D

Section: Ticket 13 : DHCP Issue

Explanation

Explanation/Reference:

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

QUESTION 60

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

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

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.

Improved

QUESTION 61

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

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

Cisco routers, switches, PIX and ASA firewalls prioritize log messages into 8 levels (0-7), as shown below:

Level	Level Name	Description
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.

Explanation Added.

QUESTION 62

You have the followings commands on your Cisco Router:

```
ip ftp username admin
```

```
ip ftp password backup
```

You have been asked to switch from FTP to HTTP. Which two commands will you use to replace the existing commands?

A. ip http username admin

B. ip http client username admin

C. ip http password backup

D. ip http client password backup

Correct Answer: BD

Section: Mix Questions

Explanation

Explanation/Reference:

Configuring the HTTP Client

Perform this task to enable the HTTP client and configure optional client characteristics.

The standard HTTP 1.1 client and the secure HTTP client are always enabled. No commands exist to disable the HTTP client. For information about configuring optional characteristics for the HTTPS client, see the HTTPS-HTTP Server and Client with SSL 3.0, Release 12.2(15)T, feature module.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip http client cache {ager interval minutes | memory {file file-size-limit | pool pool-size-limit}}
4. ip http client connection {forceclose | idle timeout seconds | retry count | timeout seconds}
5. ip http client password password
6. ip http client proxy-server proxy-name proxy-port port-number
7. ip http client response timeout seconds
8. ip http client source-interface type number
9. ip http client username username

References:

QUESTION 63

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

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

Correct Answer: BD

Section: Mix Questions

Explanation

Explanation/Reference:

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.

References:

QUESTION 64

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

- A. Physical
- B. Session

- C. Application
- D. Data-Link

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

CDP is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices. In this case, the line protocol is up which means that the physical layer is operational (layer 1) but the data link layer is not. References:

QUESTION 65

Refer to the shown below.

```
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
```

What statement is correct regarding the output shown in the graphic?

- A. These two log messages will not have a severity level. They are not errors but are just informational messages.
- B. The first log message is categorized as a warning message.
- C. These messages regarding interface status are normal output and will always be displayed when you exit config mode.
- D. The first log message is an error message with a severity level of 3.

Correct Answer: D

Section: Mix Questions

Explanation

Explanation/Reference:

Answer Corrected