PASSGUIDE.300-135.92.QAs

VCEplus.com

Number: 300-135
Passing Score: 800
Time Limit: 120 min
File Version: 25.9

300-135

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

- categorized in topics help a lot learning these exam dumps. I passed with 89% valid enough to share.

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, andRouterB, 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
!
```

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?

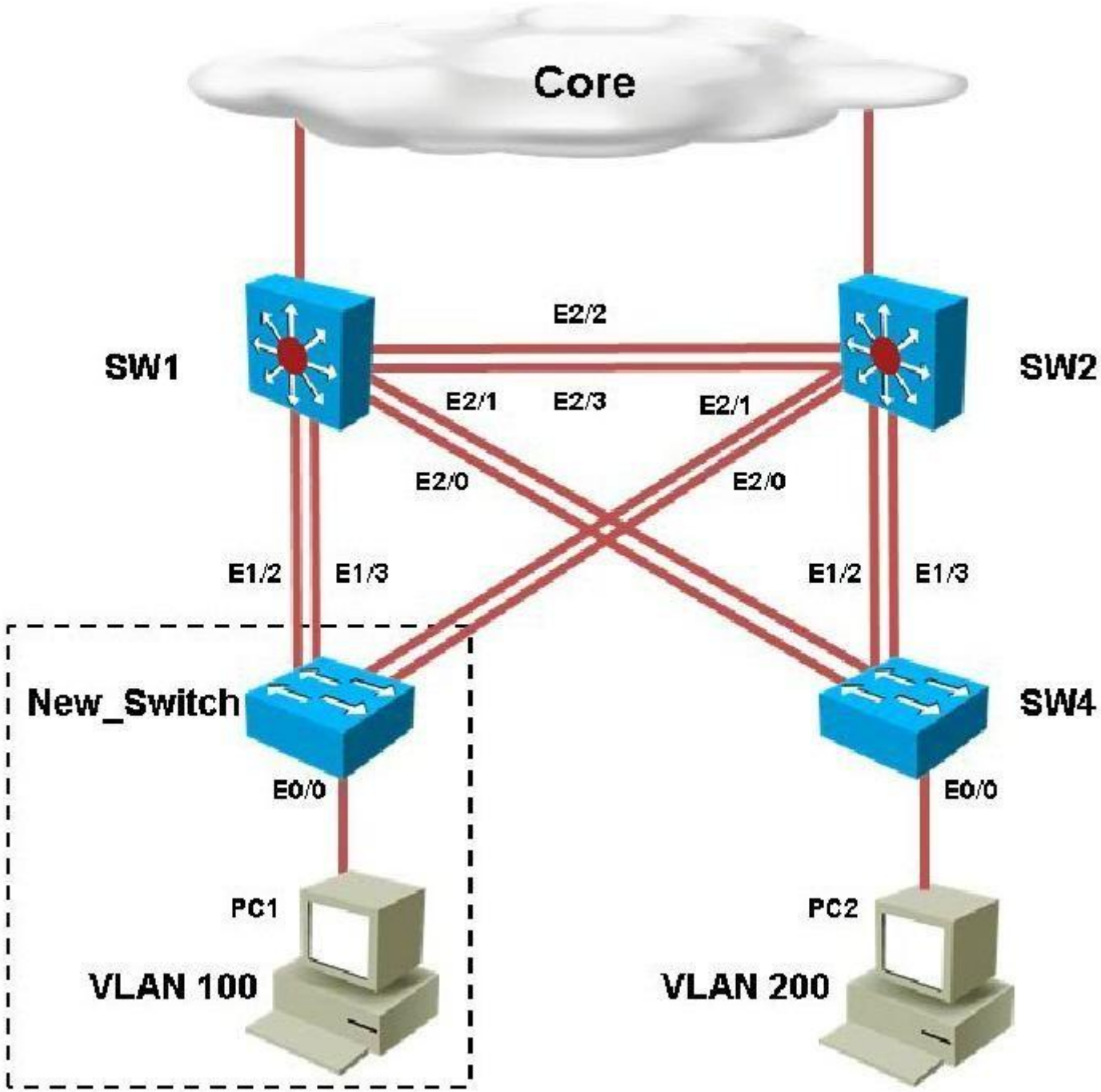
A. The GRE tunnel source and destination addresses are specified within the IPsec transform set.
B. An IPsec/GRE tunnel must use IPsec tunnel mode.
C. GRE encapsulation occurs before the IPsec encryption process.

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.


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

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

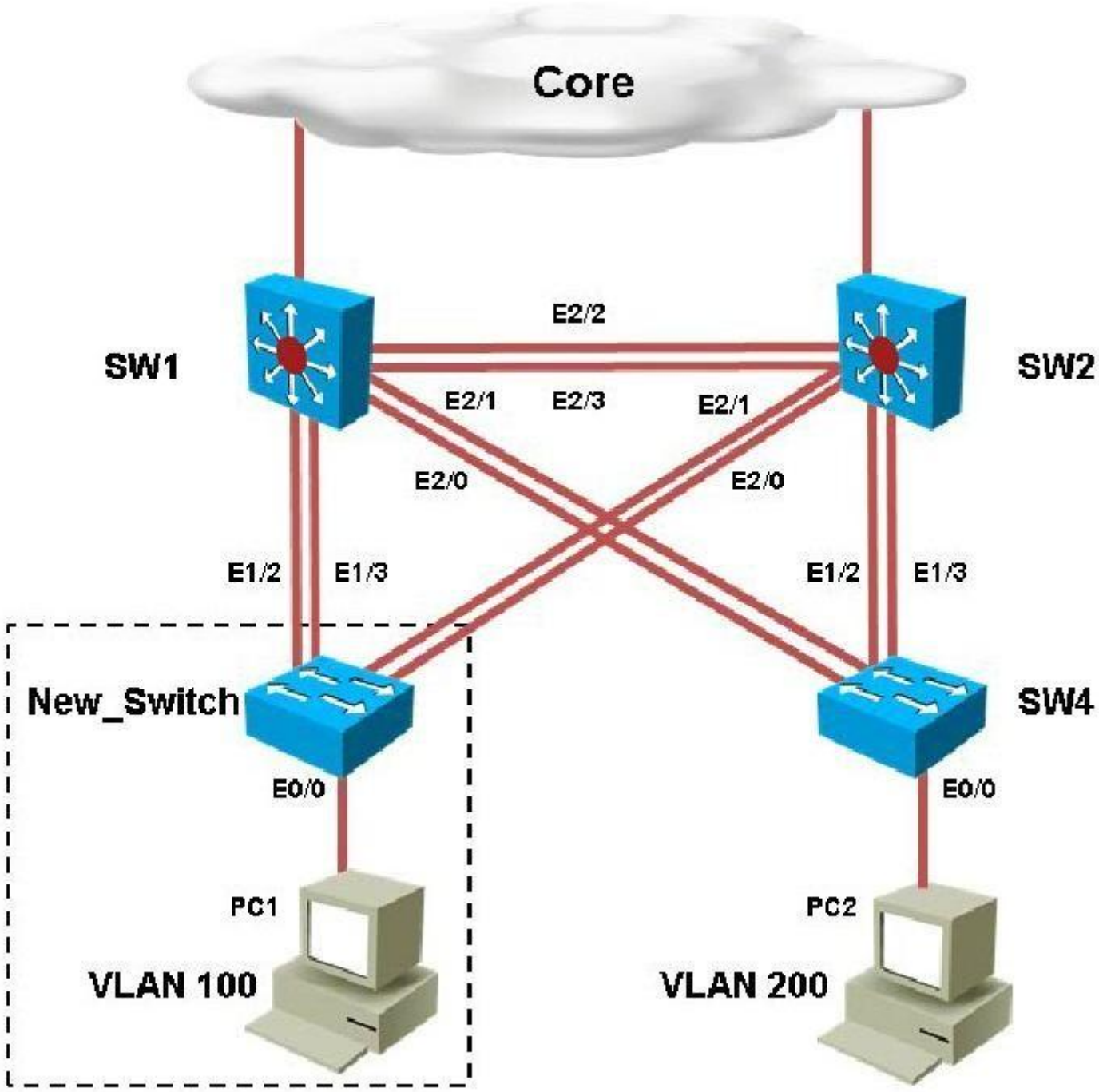
Explanation/Reference:
Explanation:

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.


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

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

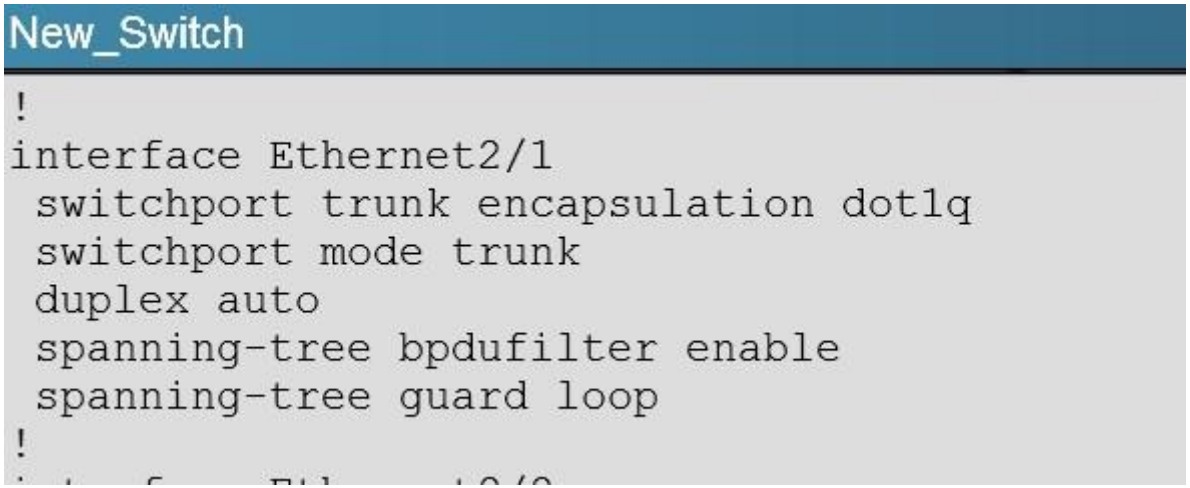
A. Loopguard configured on the New_Switch places the ports in loop inconsistent state
B. Rootguard configured on SW1 places the ports in root inconsistent state
C. Bpduguard configured on the New_Switch places the access ports in error-disable
D. Rootguard configured on SW2 places the ports in root inconsistent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

Correct Answer: A
Section: Troubleshooting VTP

Explanation

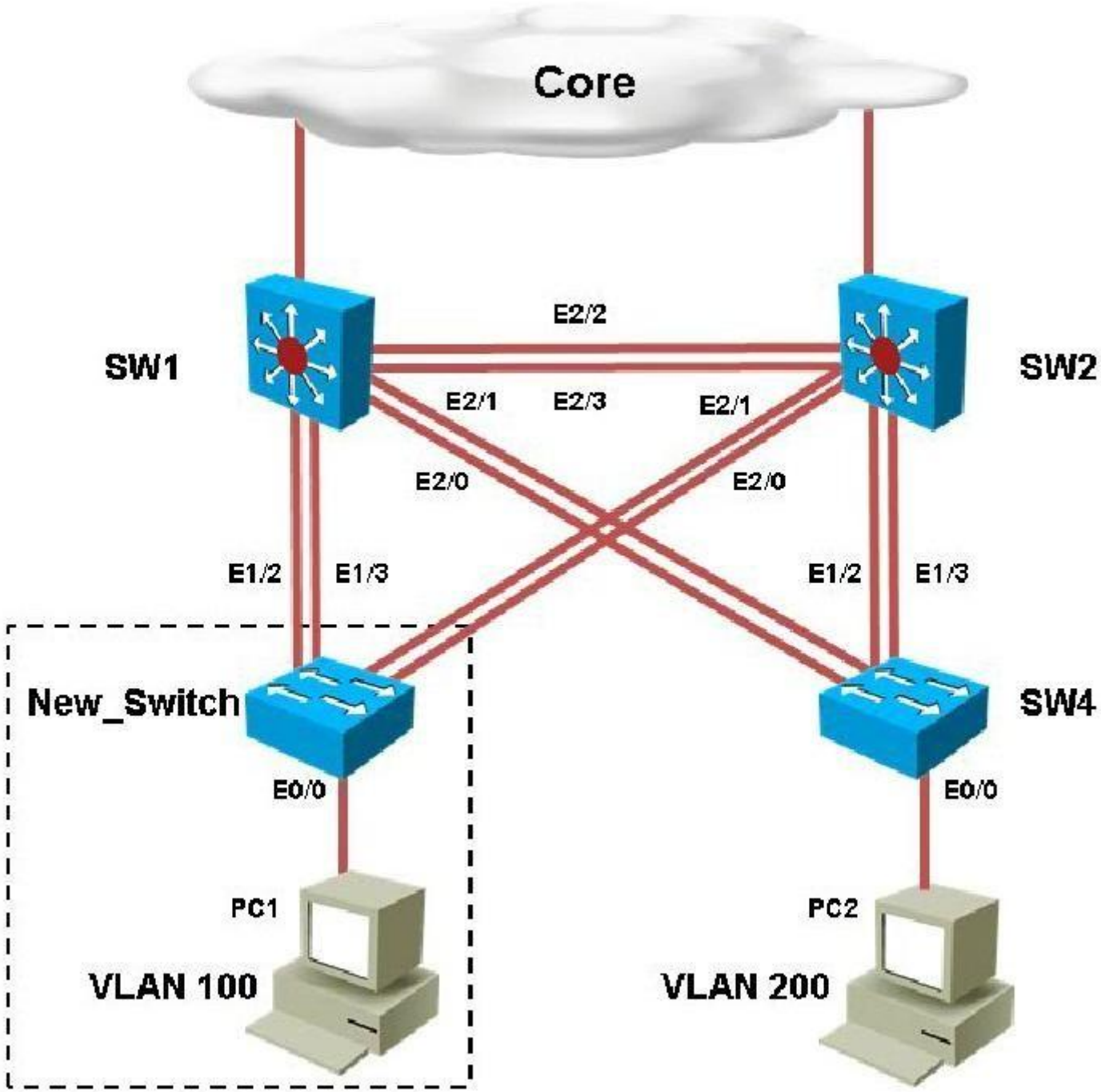
Explanation/Reference:
Explanation:

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



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.


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

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:

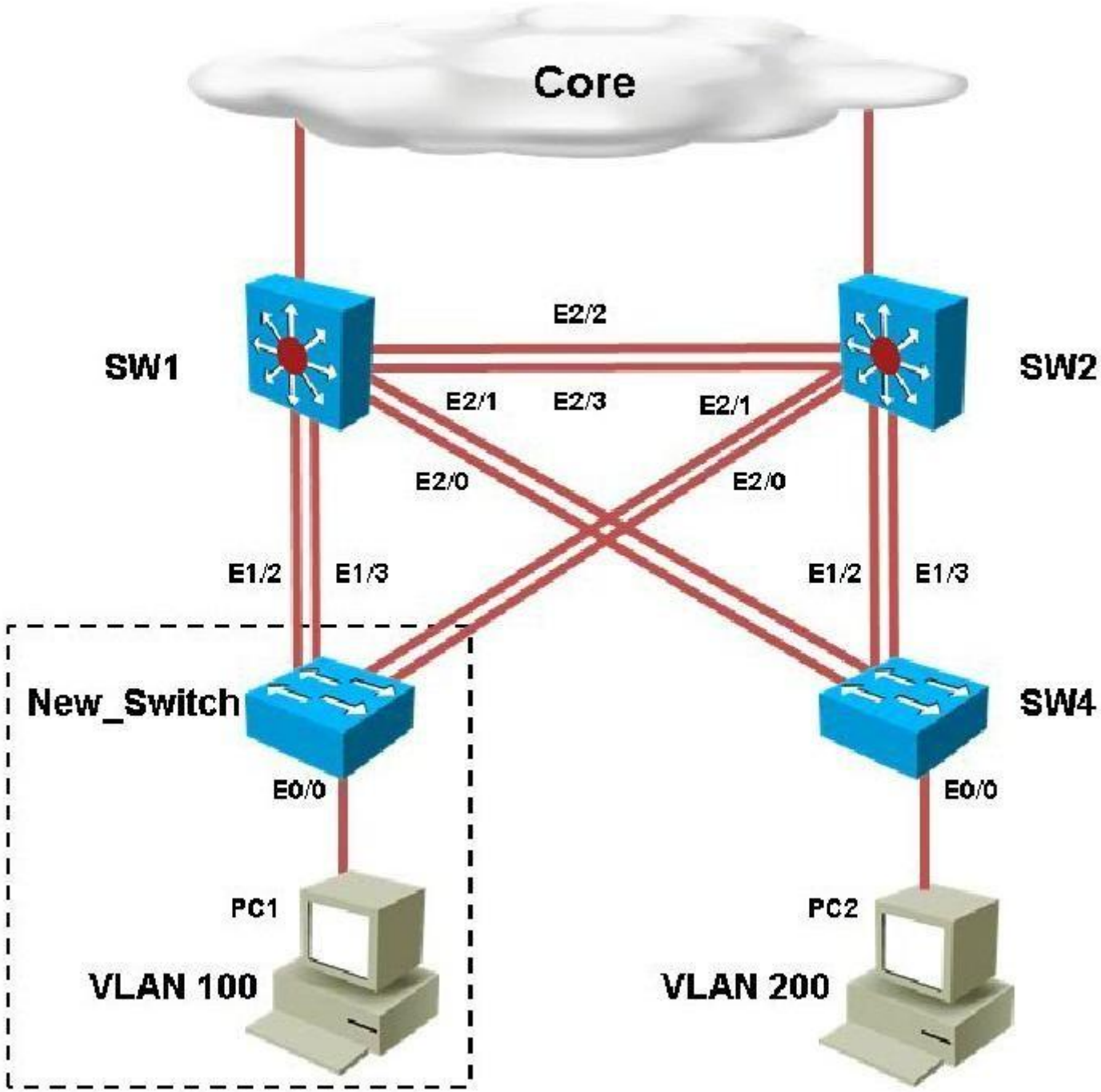
Here is the configuration found on the New_Switch:

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.


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

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: Mix Questions
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

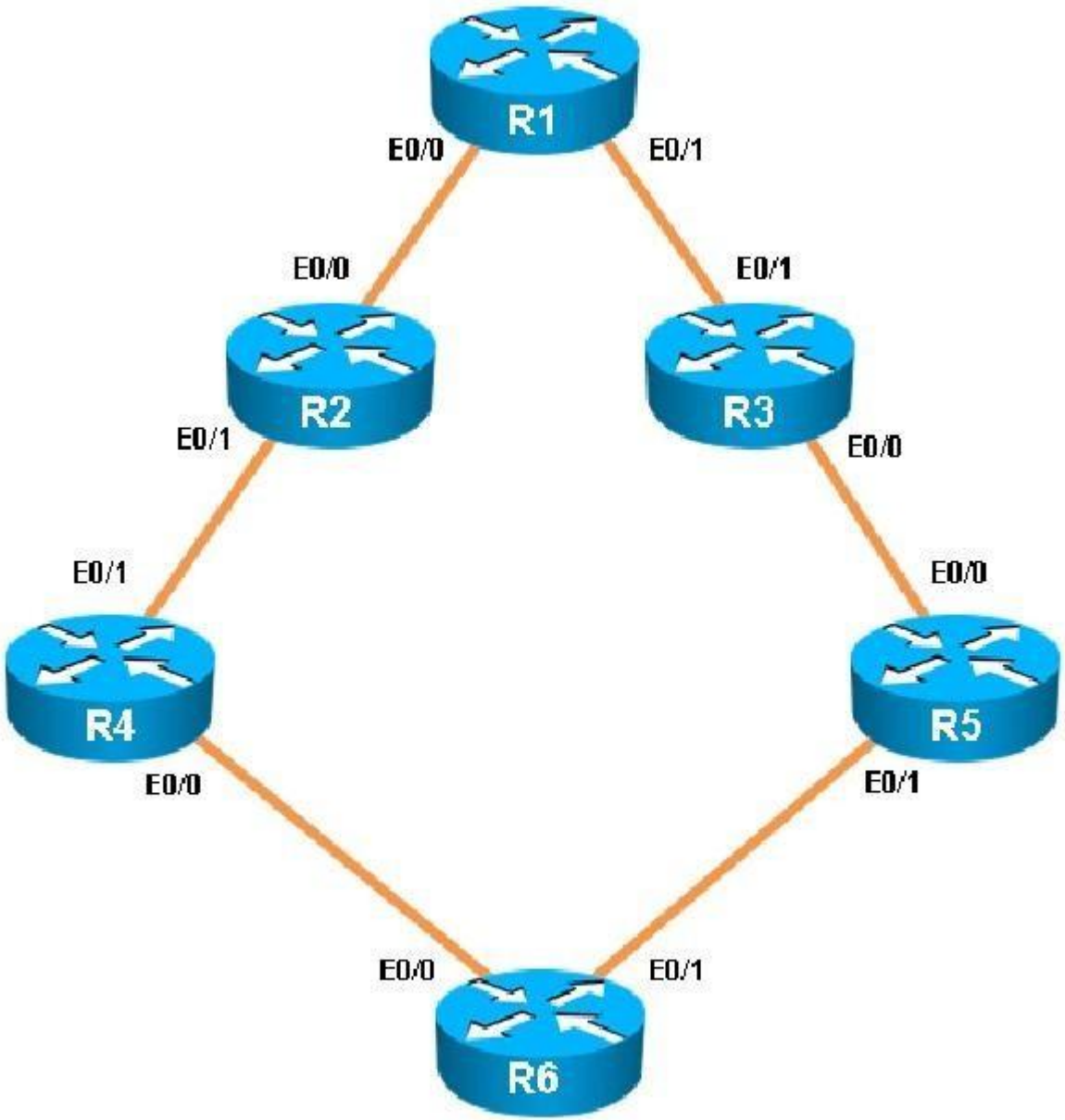
```
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 172.16.100.1 255.255.255.0
!
interface Vlan200
 ip address 172.16.200.1 255.255.255.0
!
interface Vlan300
 ip address 192.168.10.1 255.255.255.0
!
```

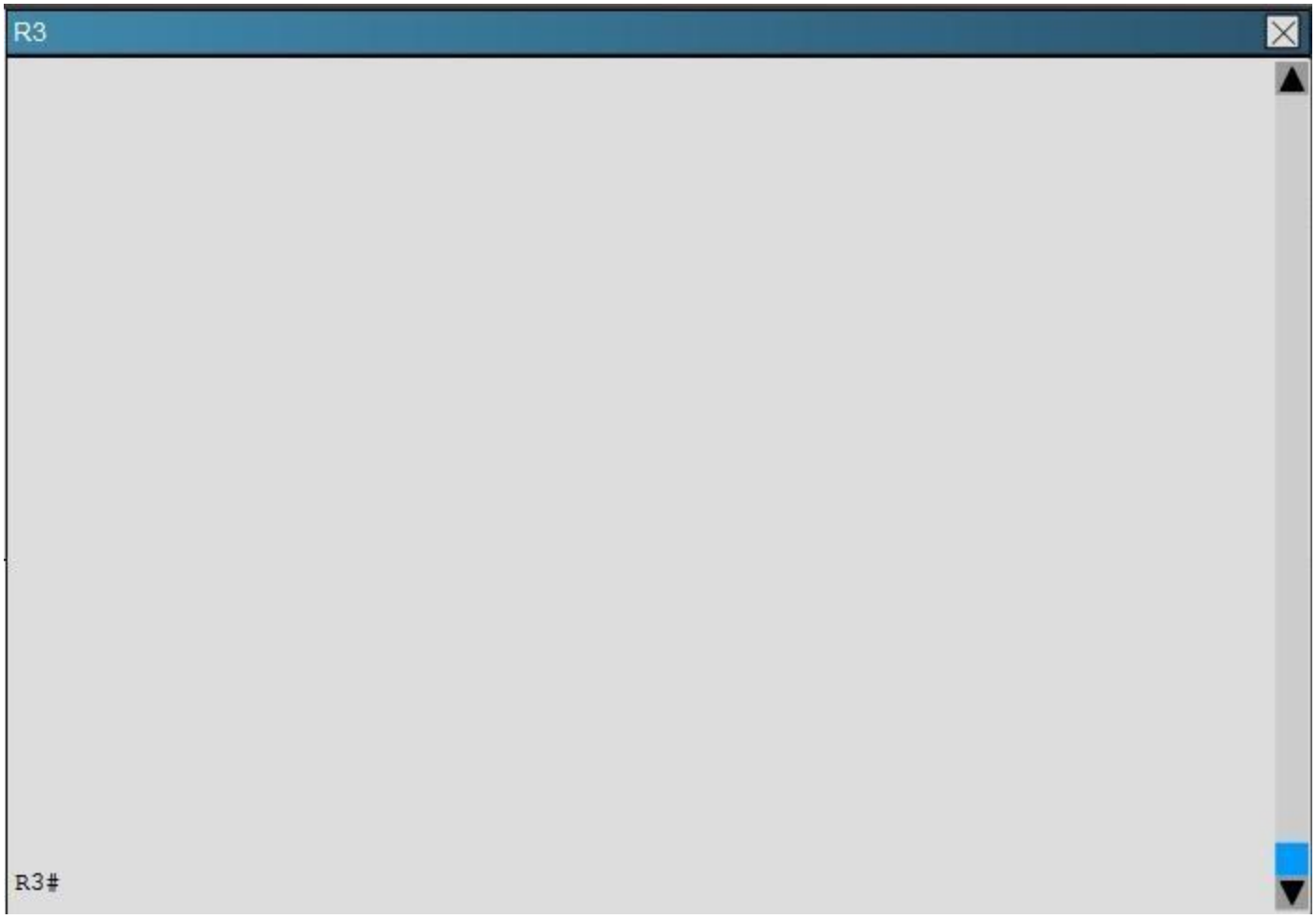
SW4

```
 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

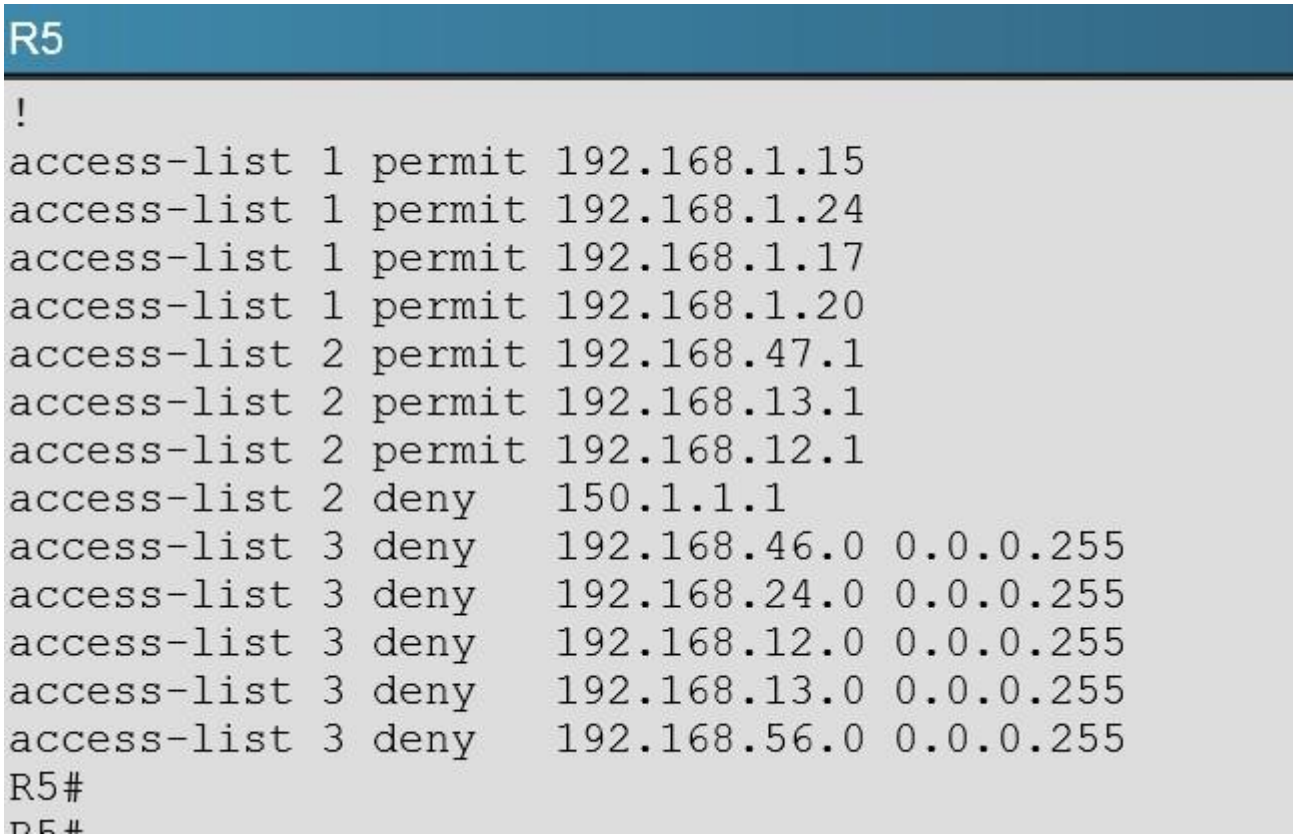
Correct Answer: B
Section: Troubleshooting EIGRP
Explanation

Explanation/Reference:
Explanation:

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

R5

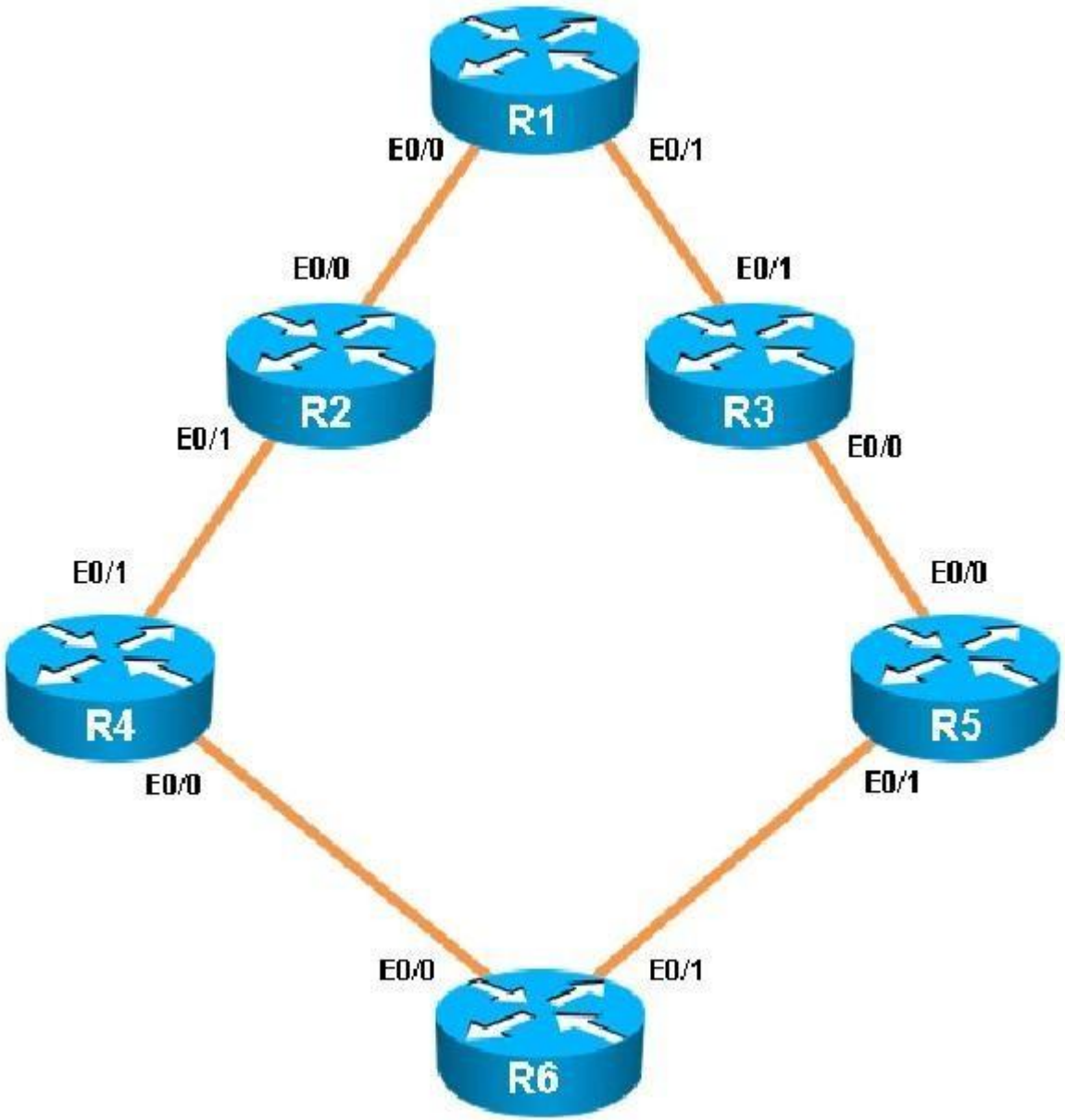
```
!
router eigrp 1
 distribute-list 3 in Ethernet0/0
 distribute-list 3 in Ethernet0/1
 network 192.168.35.0
 network 192.168.56.0
!
!
```

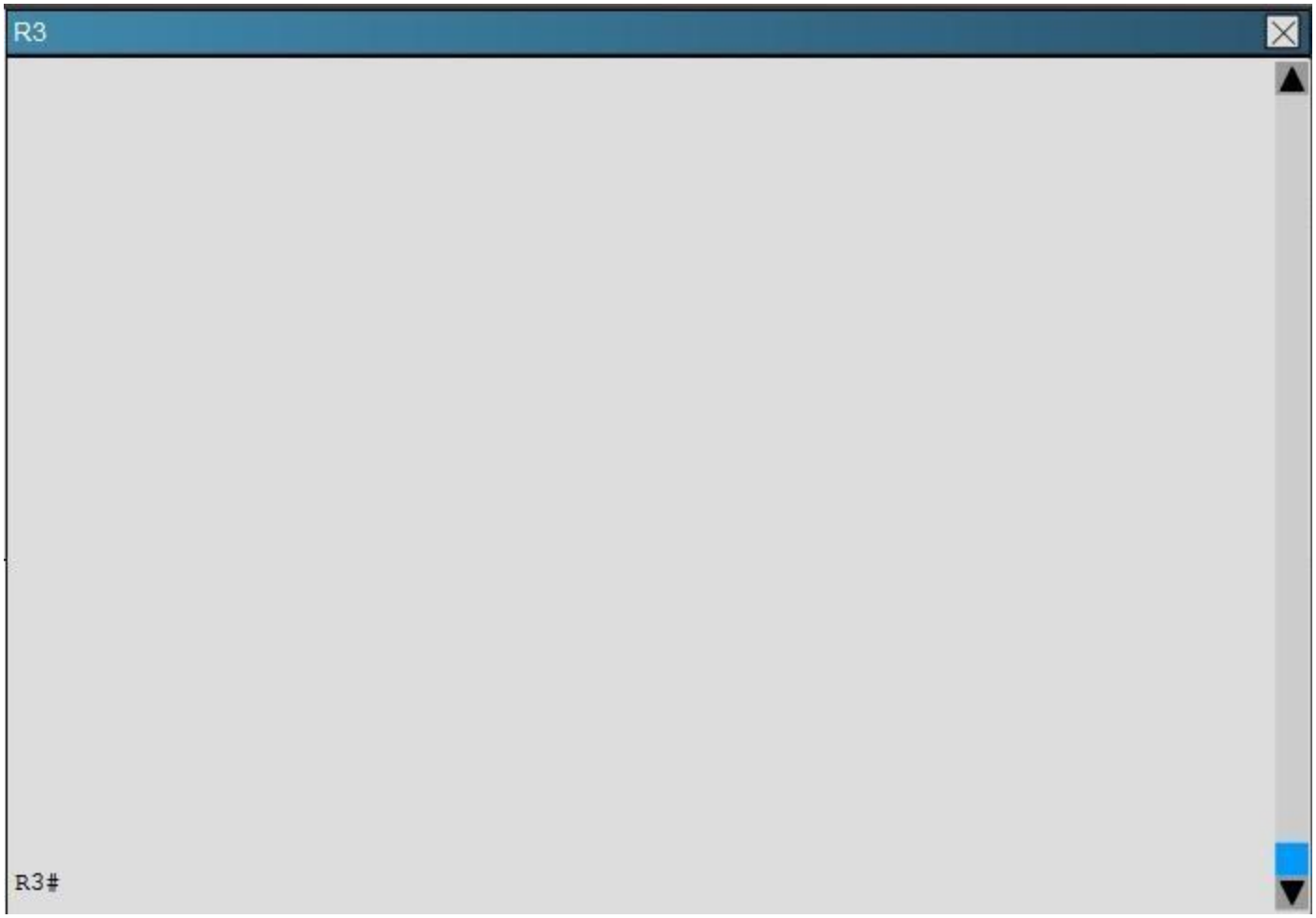


QUESTION 12
Scenario:

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.





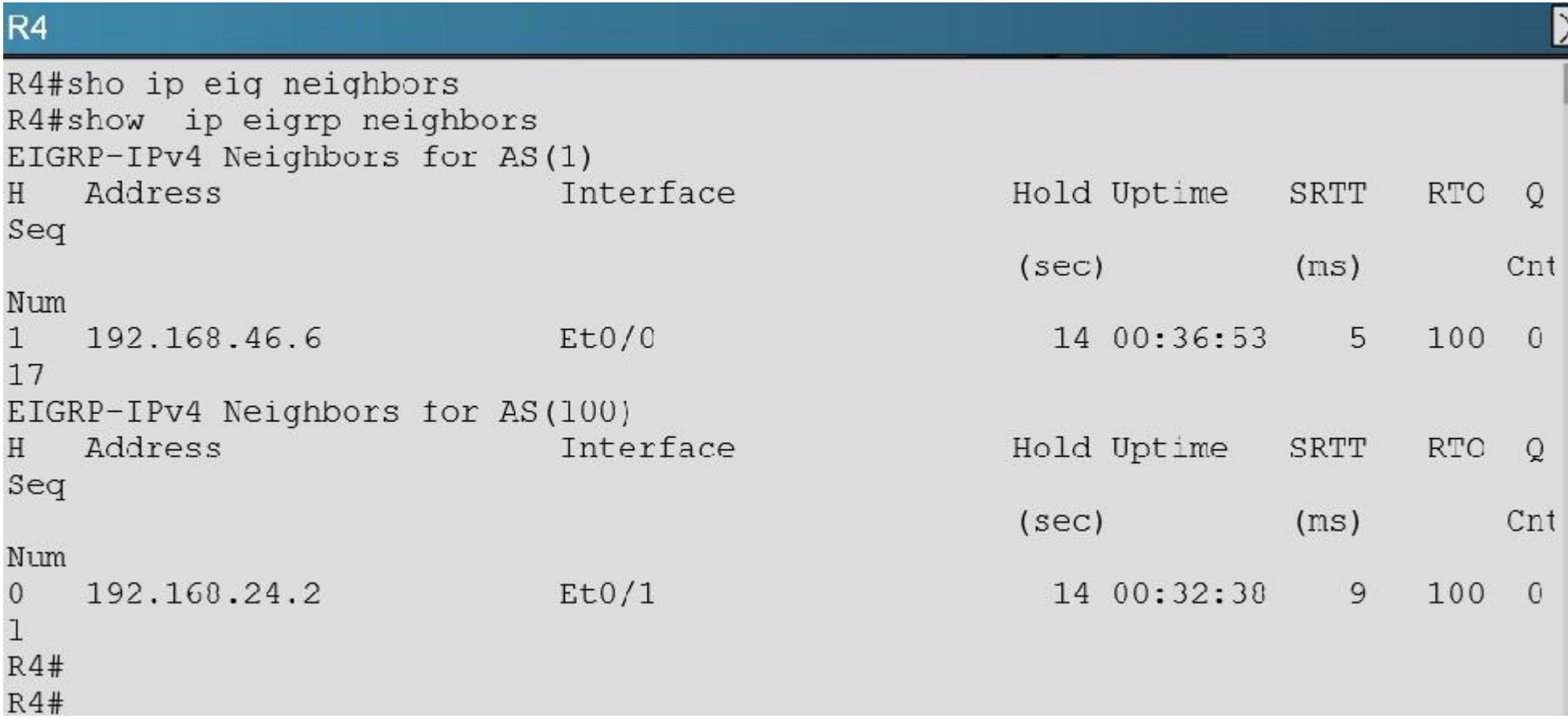
The network segment between R2 and R4 has become disconnected from the remainder of the network. How should this issue be resolved?

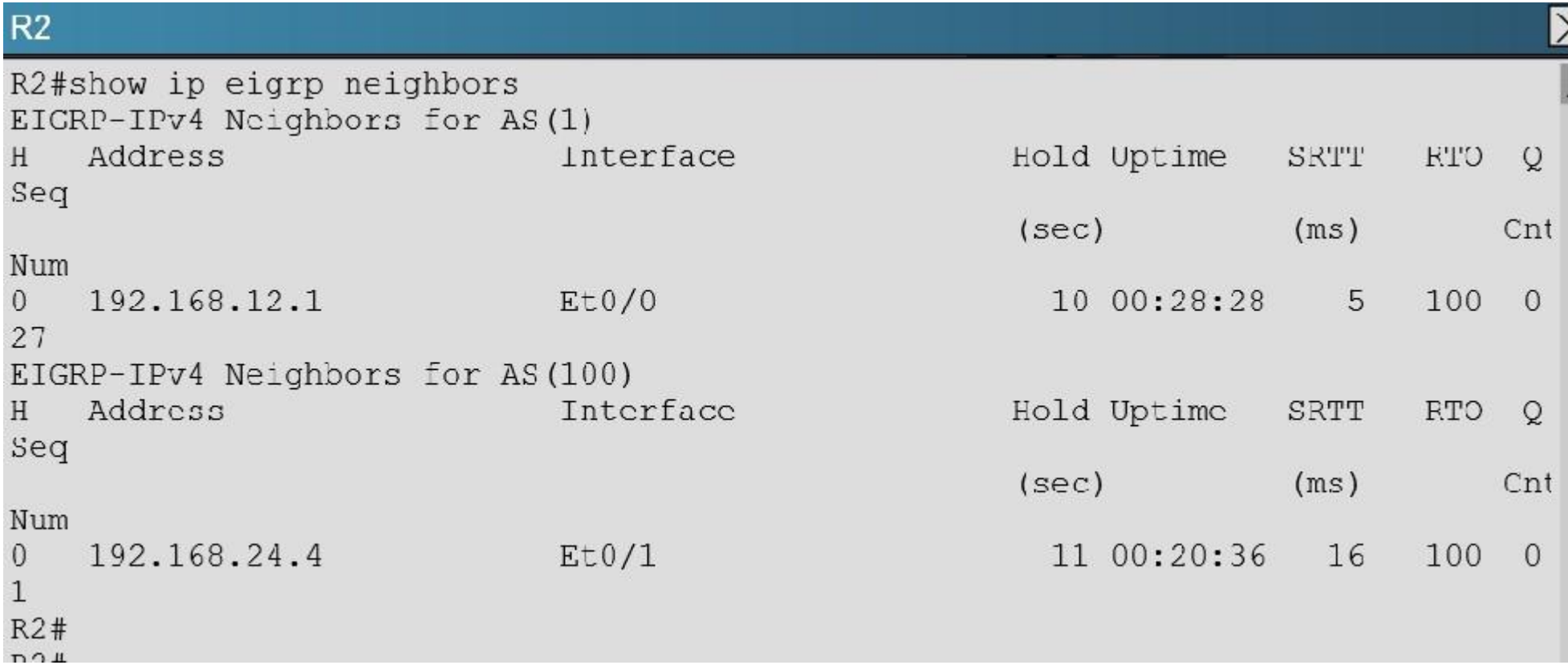
A. Change the autonomous system number in the remainder of the network to be consistent with R2 and R4.
B. Move the 192.168.24.0 network to the EIGRP 1 routing process in R2 and R4.
C. Enable the R2 and R4 router interfaces connected to the 192.168.24.0 network.
D. Remove the distribute-list command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

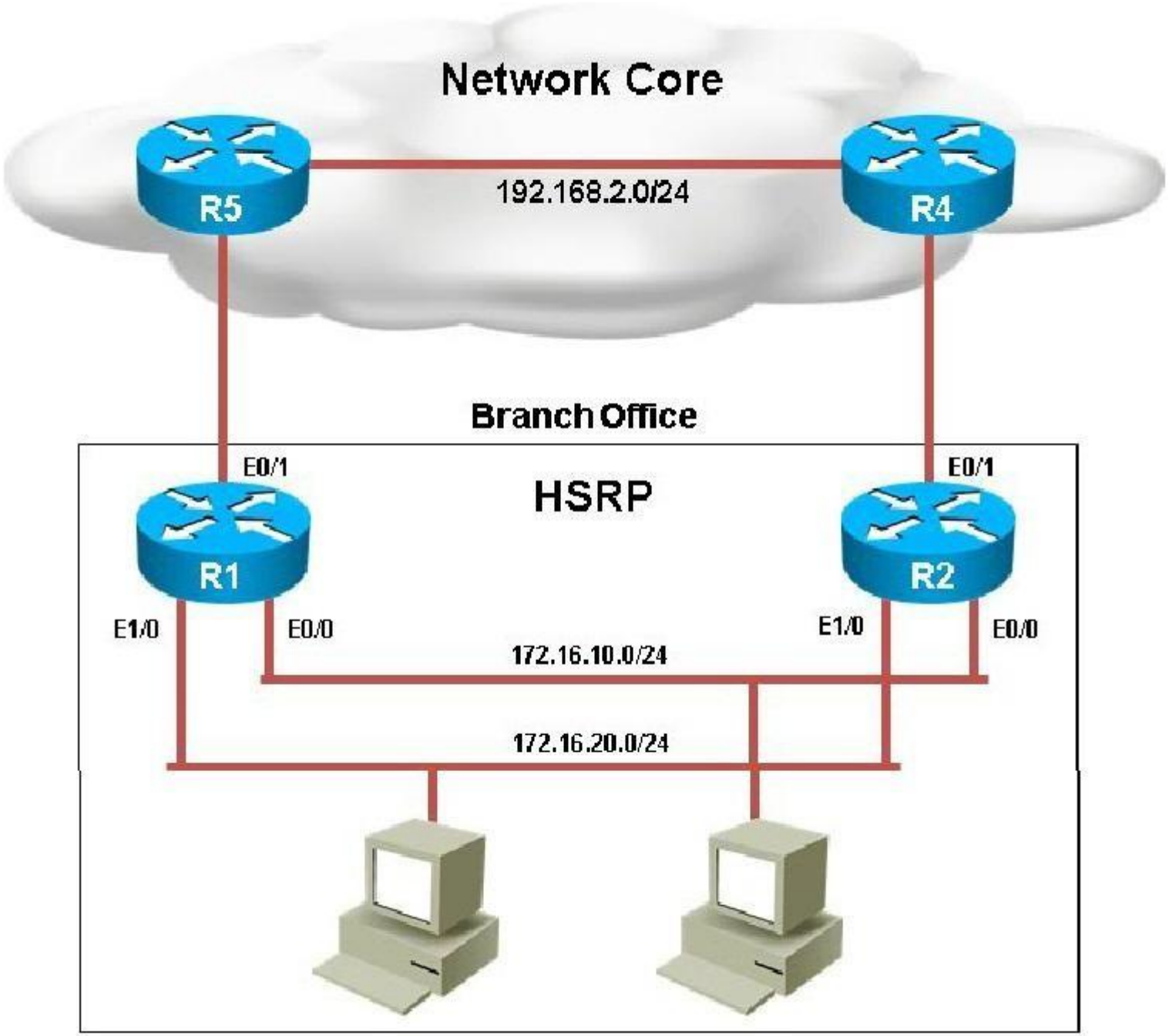
When issuing the "show ipeigrp neighbor" command (which is about the only command that it lets you do in this question) you will see that all other routers are configured for EIGRP AS 1. However, the 192.16824.0 network between R2 and R4 is incorrectly configured for EIGRP AS 100:





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.


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

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

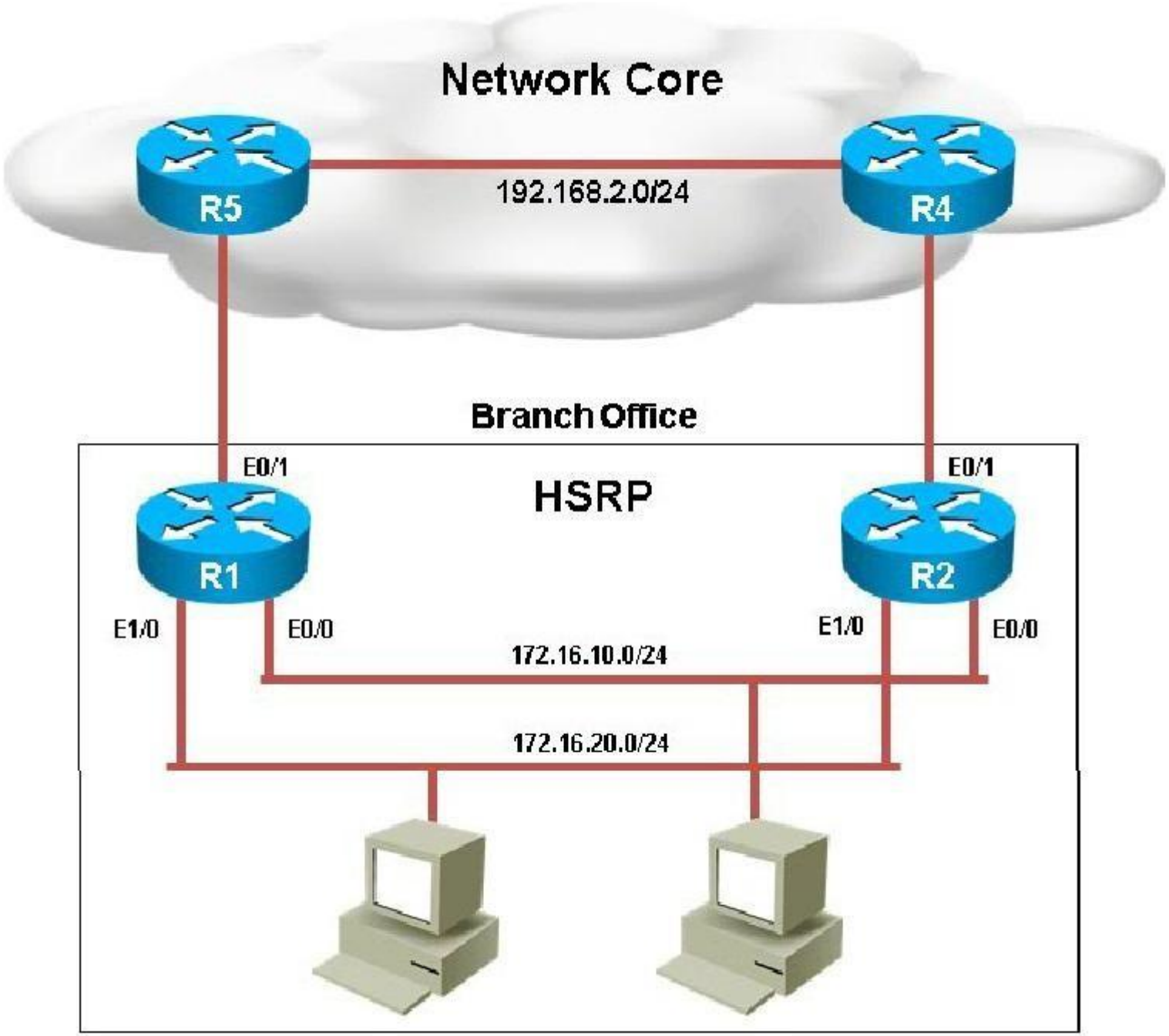
```
!
track 1 interface Ethernet0/0 line-protocol
!
!
!
!
interface Ethernet0/0
 description connection to 172.16.10.0/24 network
 ip address 172.16.10.2 255.255.255.0
 standby 1 ip 172.16.10.254
 standby 1 priority 130
 standby 1 preempt delay reload 180
 standby 1 mac-address 4000.0000.0010
 standby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


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

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

'Mar 26 11:17:42.719: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP 172.16.10.254
'Mar 26 11:17:42.918: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
R1#
'Mar 26 11:17:44.869: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP 172.16.20.254
'Mar 26 11:17:45.485: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP 172.16.10.254
'Mar 26 11:17:45.718: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
R1#
'Mar 26 11:17:47.439: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP 172.16.20.254
'Mar 26 11:17:48.252: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
'Mar 26 11:17:48.322: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP 172.16.10.254
R1#
'Mar 26 11:17:50.389: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP 172.16.20.254
'Mar 26 11:17:50.735: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
'Mar 26 11:17:50.921: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP 172.16.10.254
R1#
'Mar 26 11:17:53.089: HSRP: Et1/0 Grp2 Hello out 172.16.20.2 Active pri 100 vIP 172.16.20.254
'Mar 26 11:17:53.338: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active pri130vlP 172.16.10.254
'Mar 26 11:17:53.633: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254

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

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
!
```

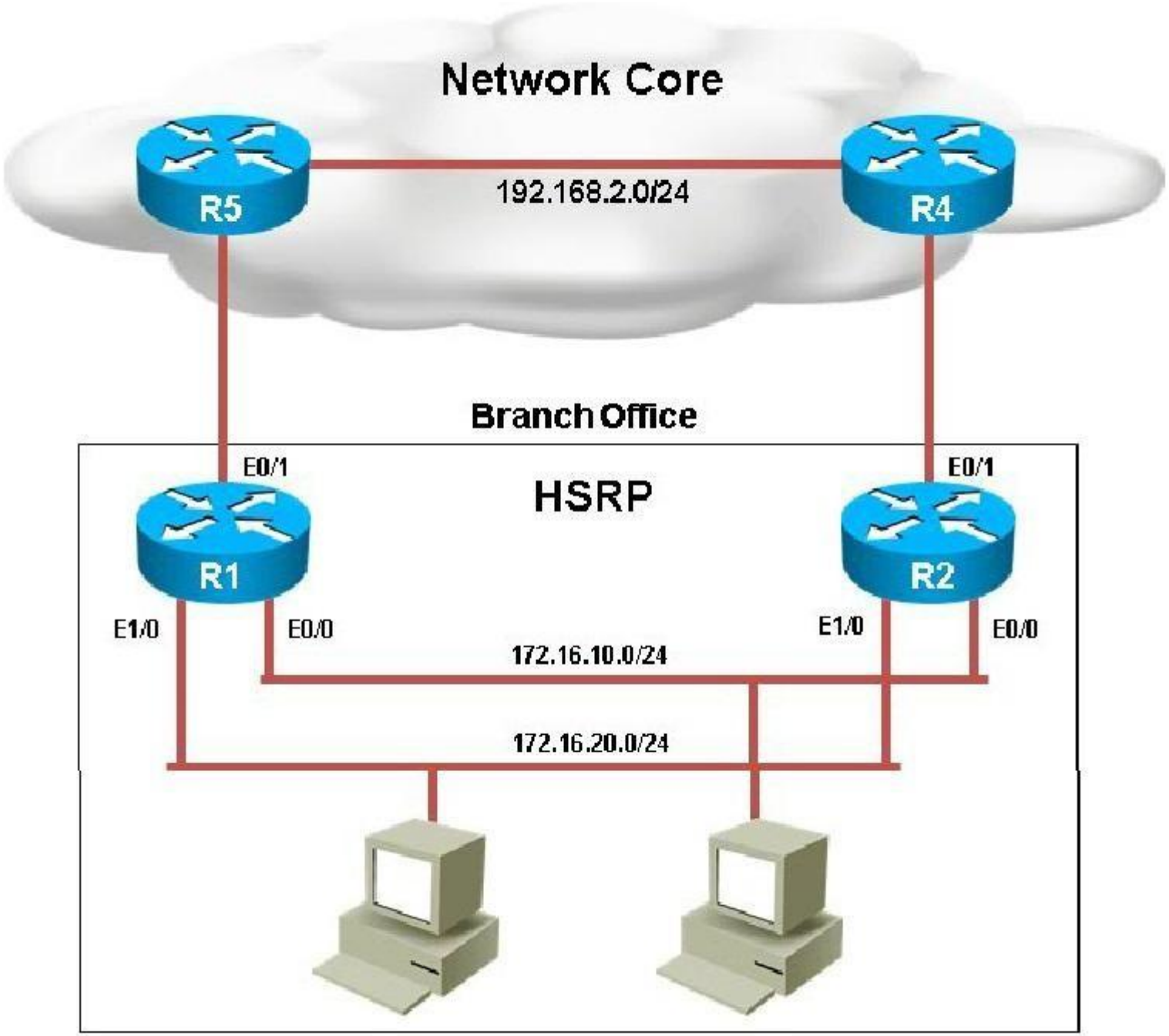
R1

```
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.


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

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.

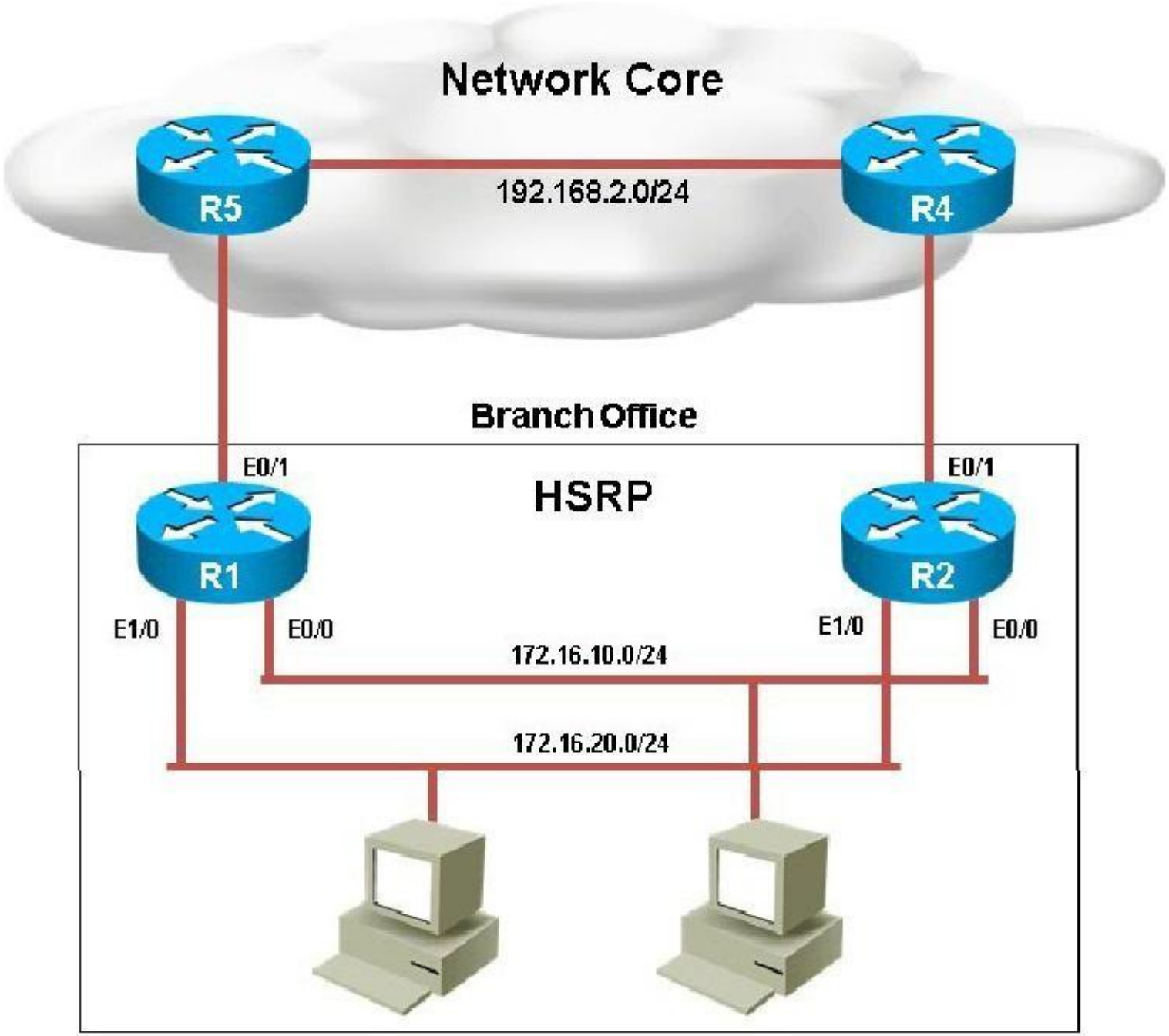
R4

```
!
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.

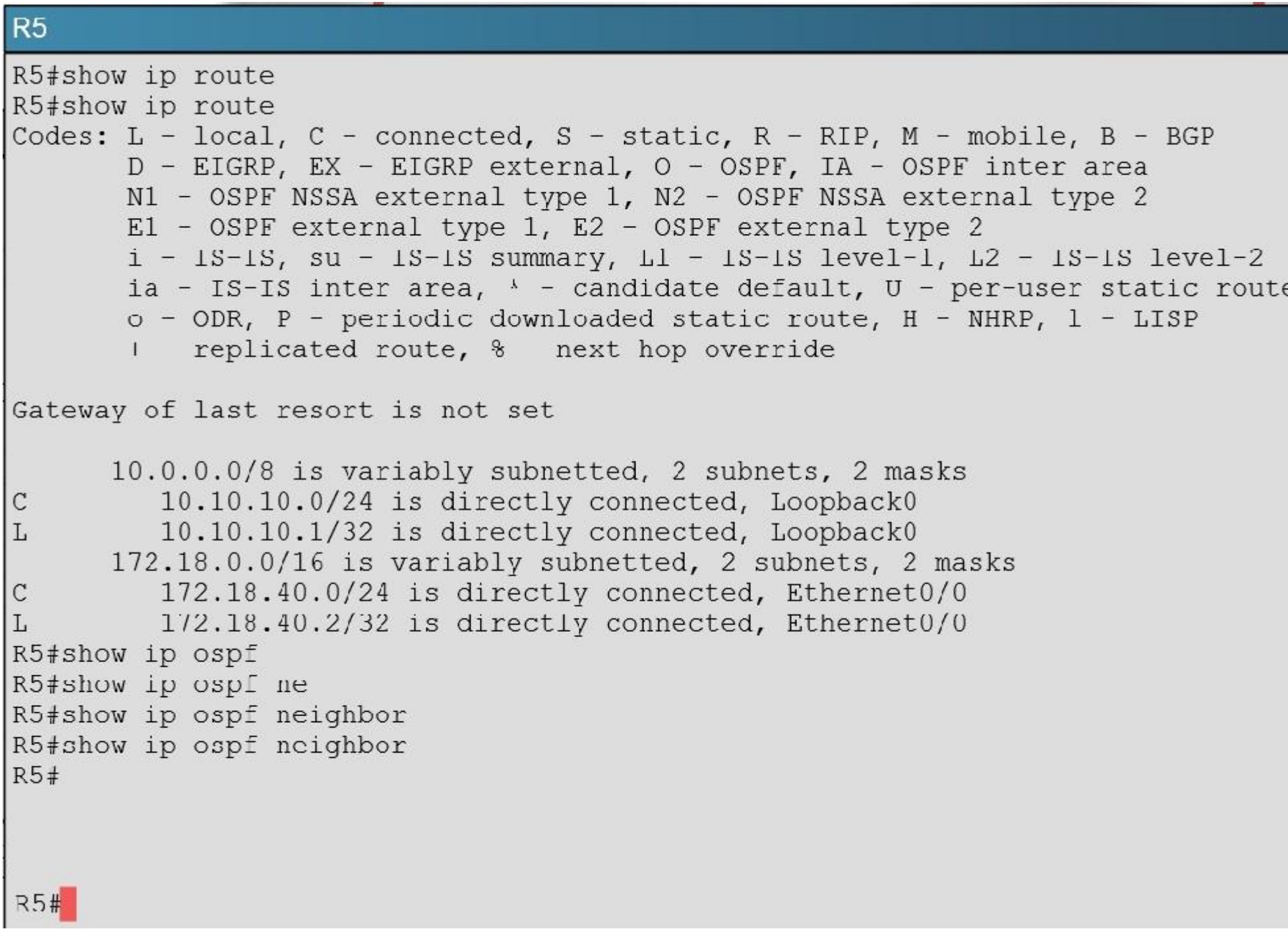

Network Core
R5
192.168.2.0/24
R4
Branch Office
E0/1
HSRP
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24

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

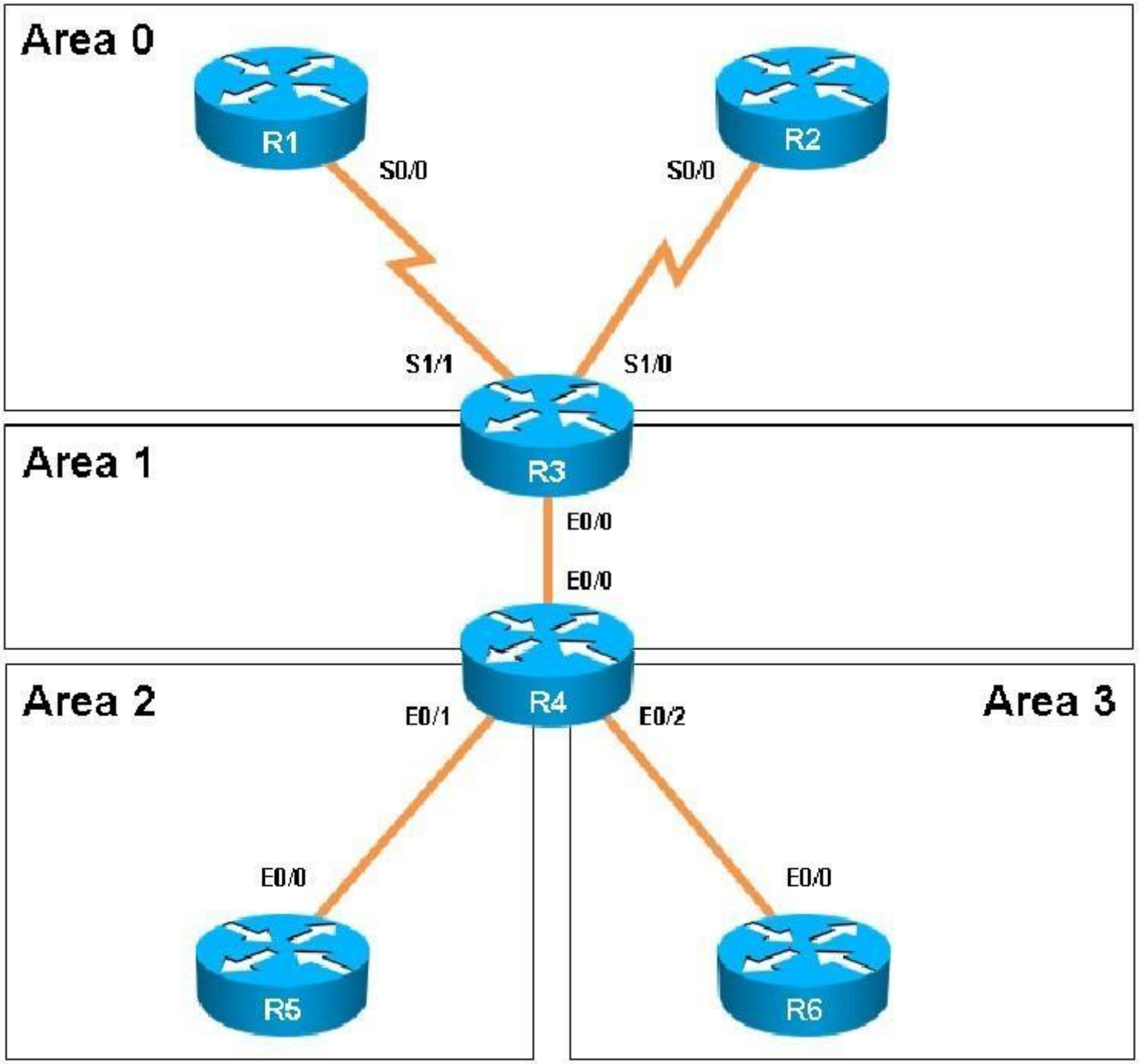
Explanation/Reference:
Explanation:
If we issue the "show ip route" and "show ipospf neighbor" commands on R5, we see that there are no learned OSPF routes and he has no OSPF neighbors.

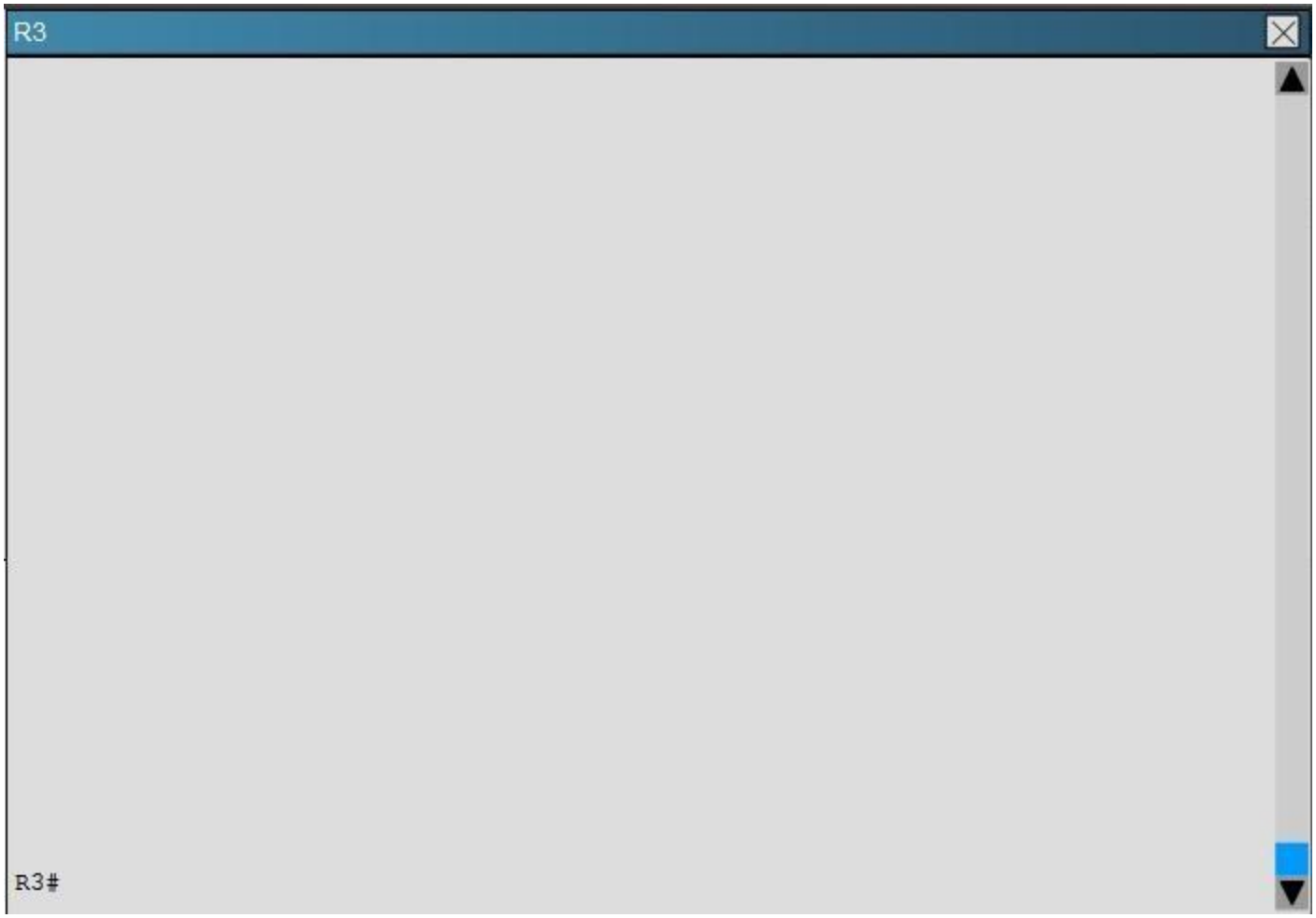

R5
R5#show ip route
R5#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, 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 neighbor
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.


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



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
!
```

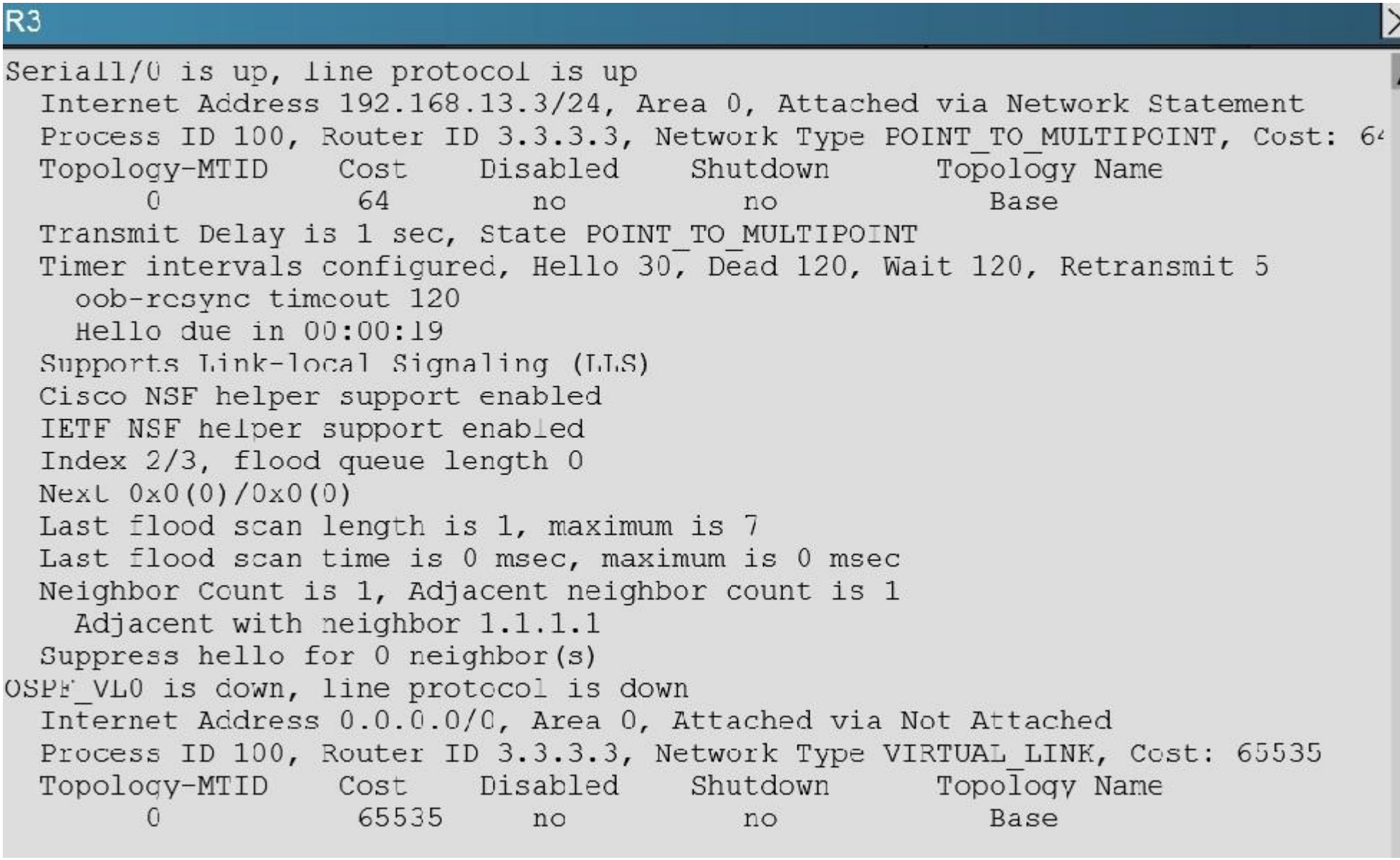
R3

```
!
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:

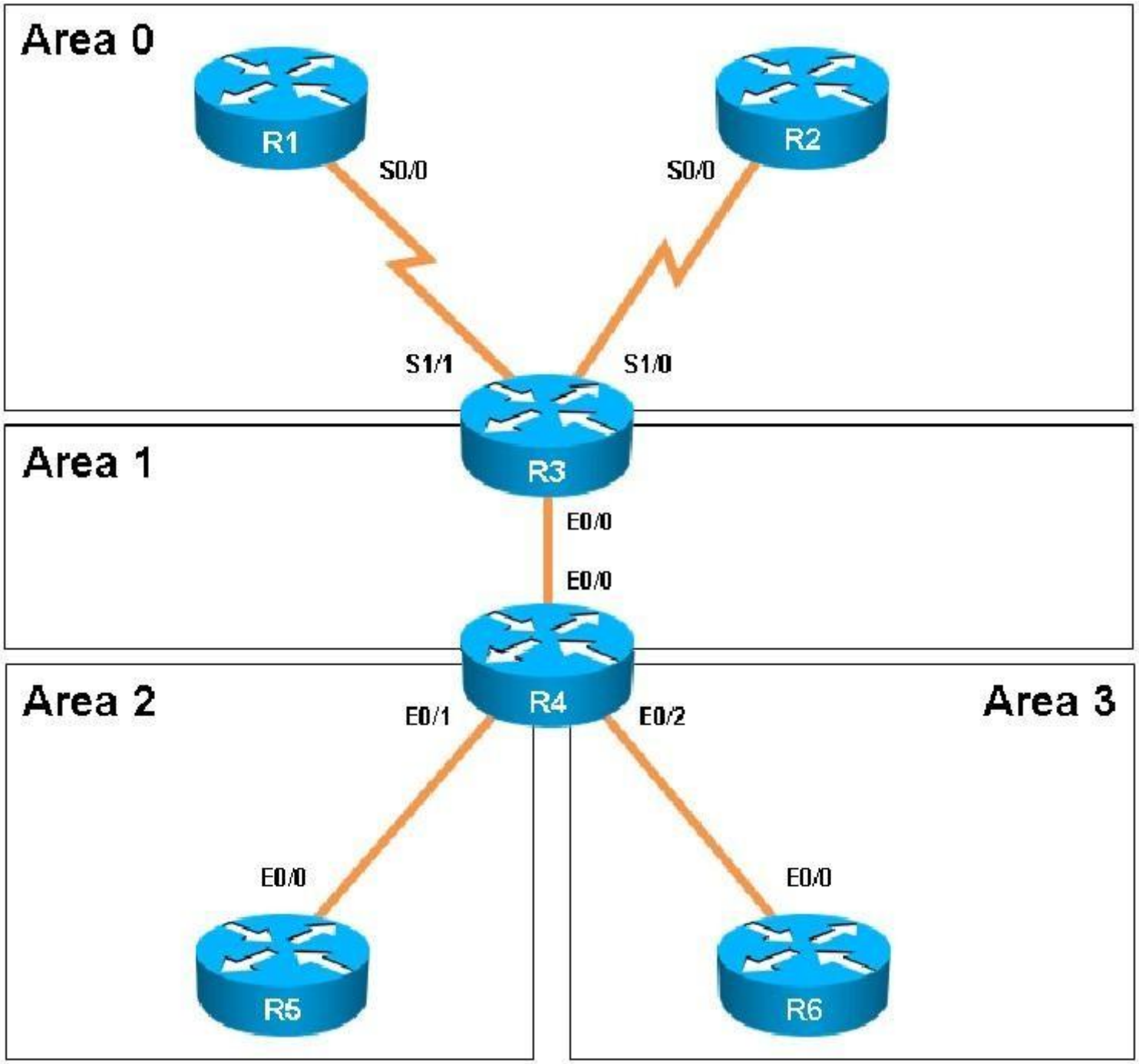
R1

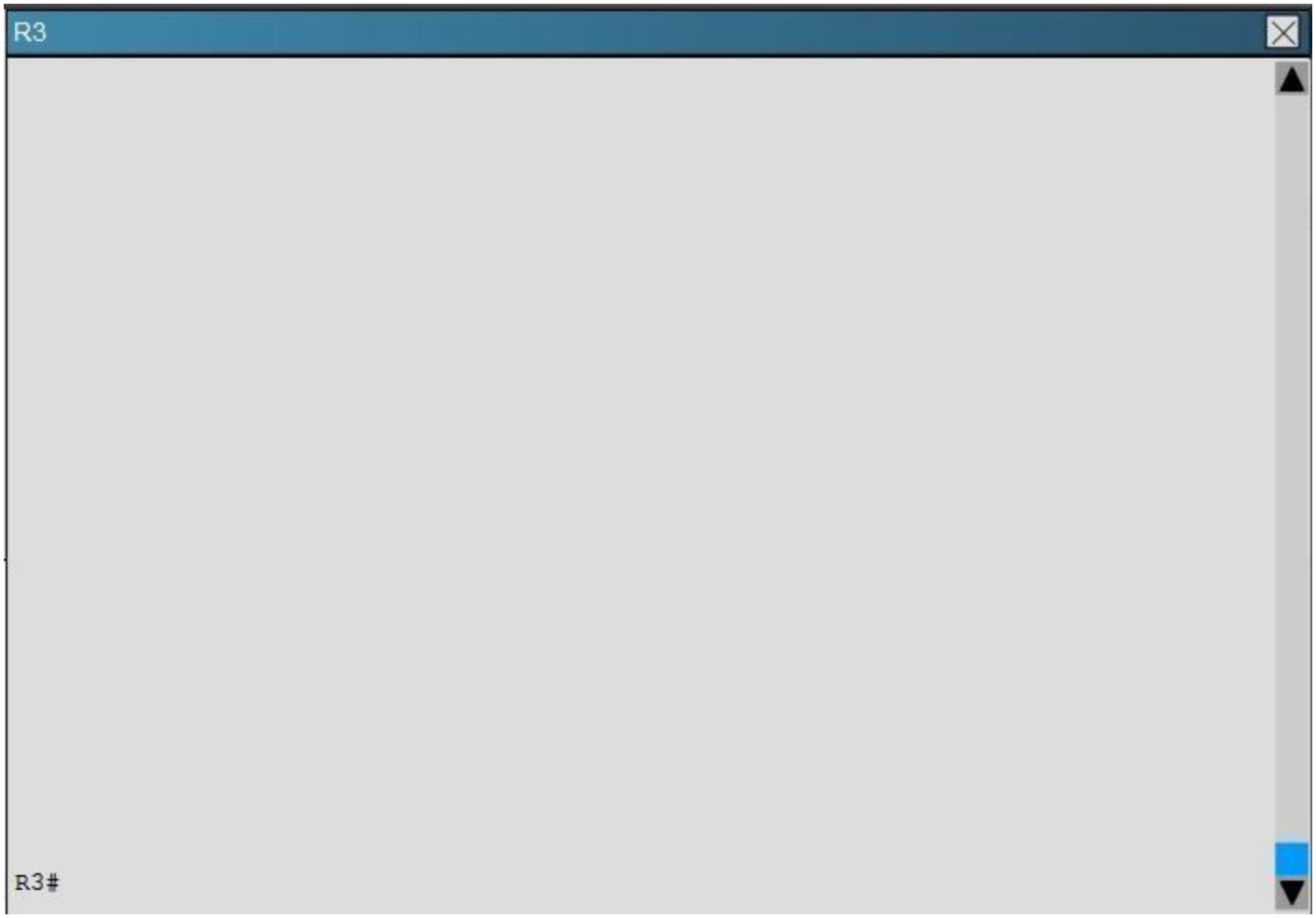
```
Serial0/0 is up, line protocol is up
  Internet Address 192.168.13.1/24, Area 0, Attached via Network Statement
  Process ID 100, Router ID 1.1.1.1, Network Type NON_BROADCAST, Cost: 1943
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1943      no          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#
```



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.


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



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

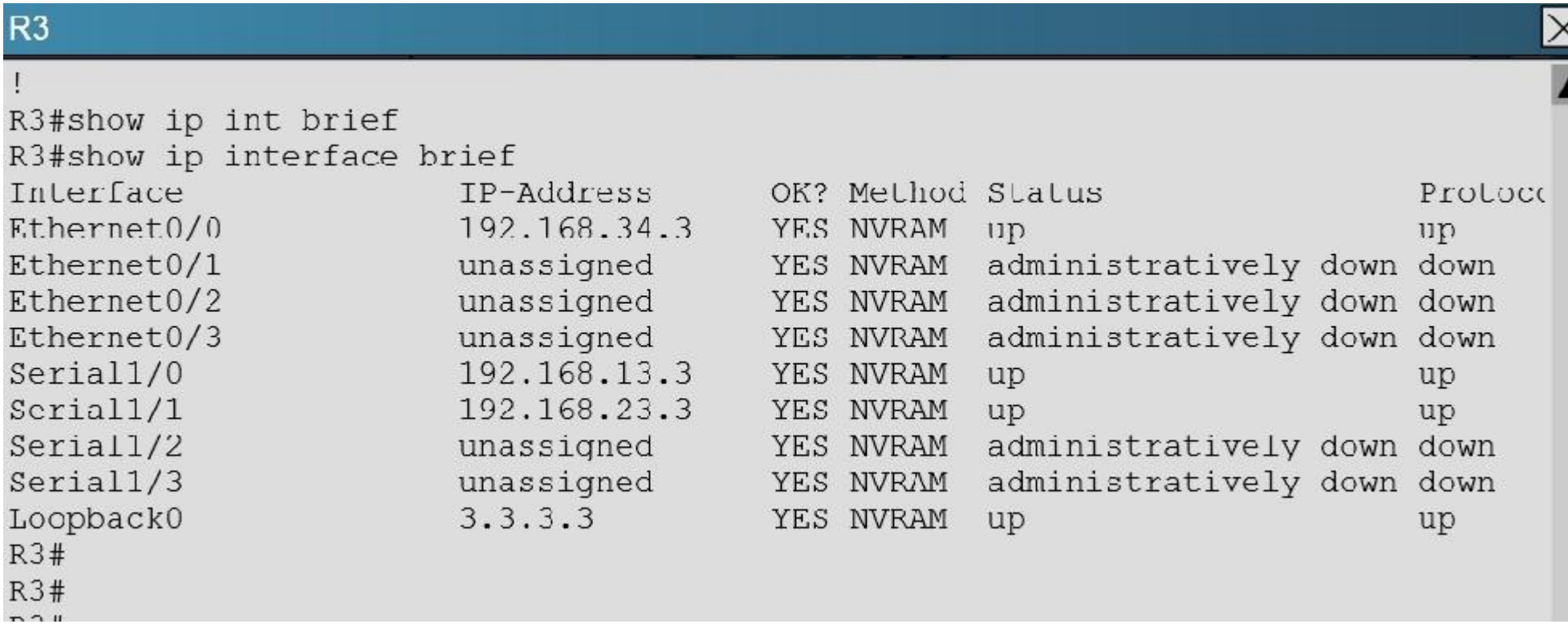
A. Configure R4 with a virtual link to 192.168.13.2
B. Change the R3 and R4 hello-interval and retransmit-interface timers to zero so the link won't go down.
C. Add an OSPF network statement for 4.4.4.4 0.0.0.0 area 1 in R3
D. Add an OSPF network statement for 192.168.34.3 0.0.0.255 area 2 in R3
E. Add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



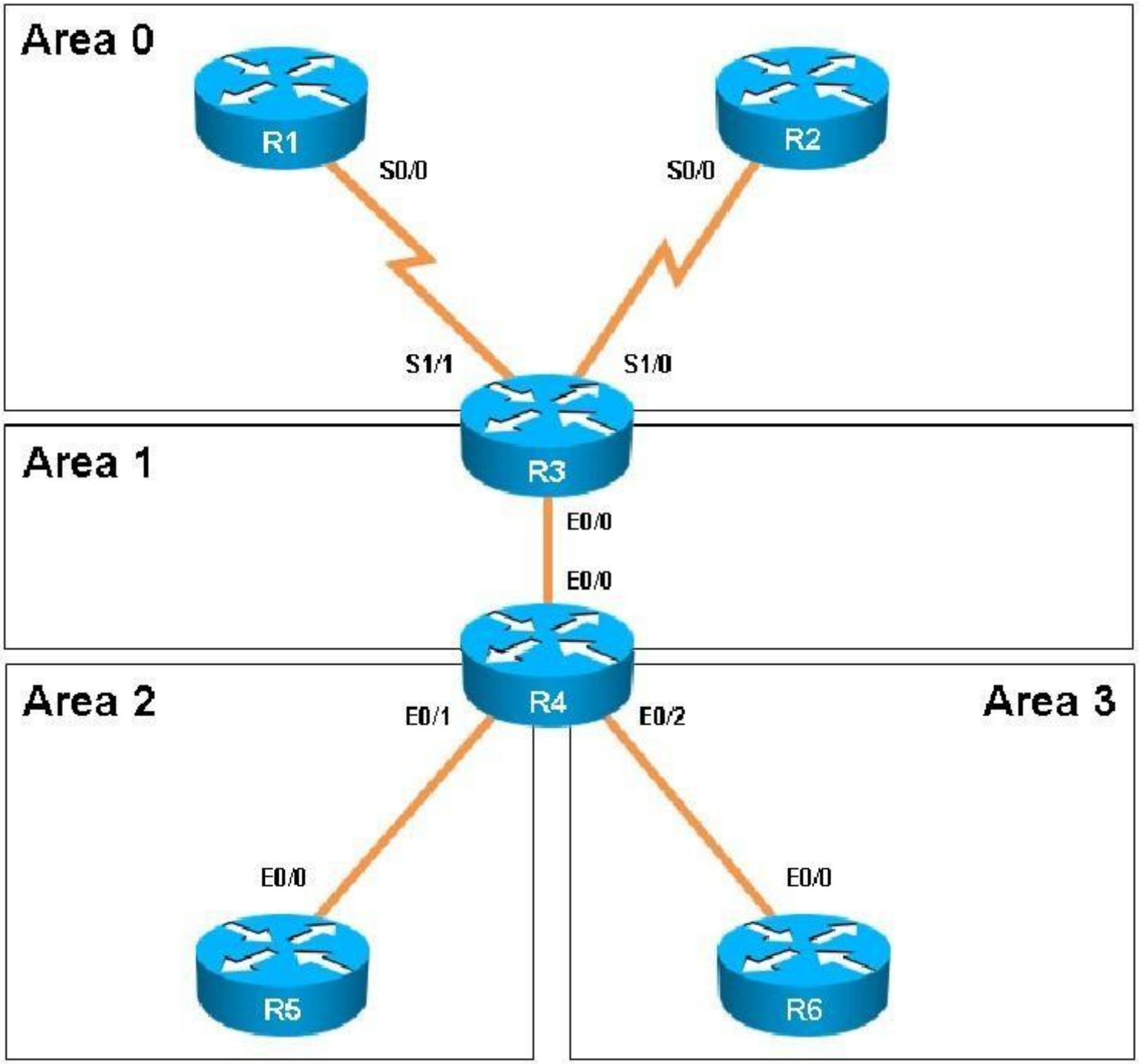
R3

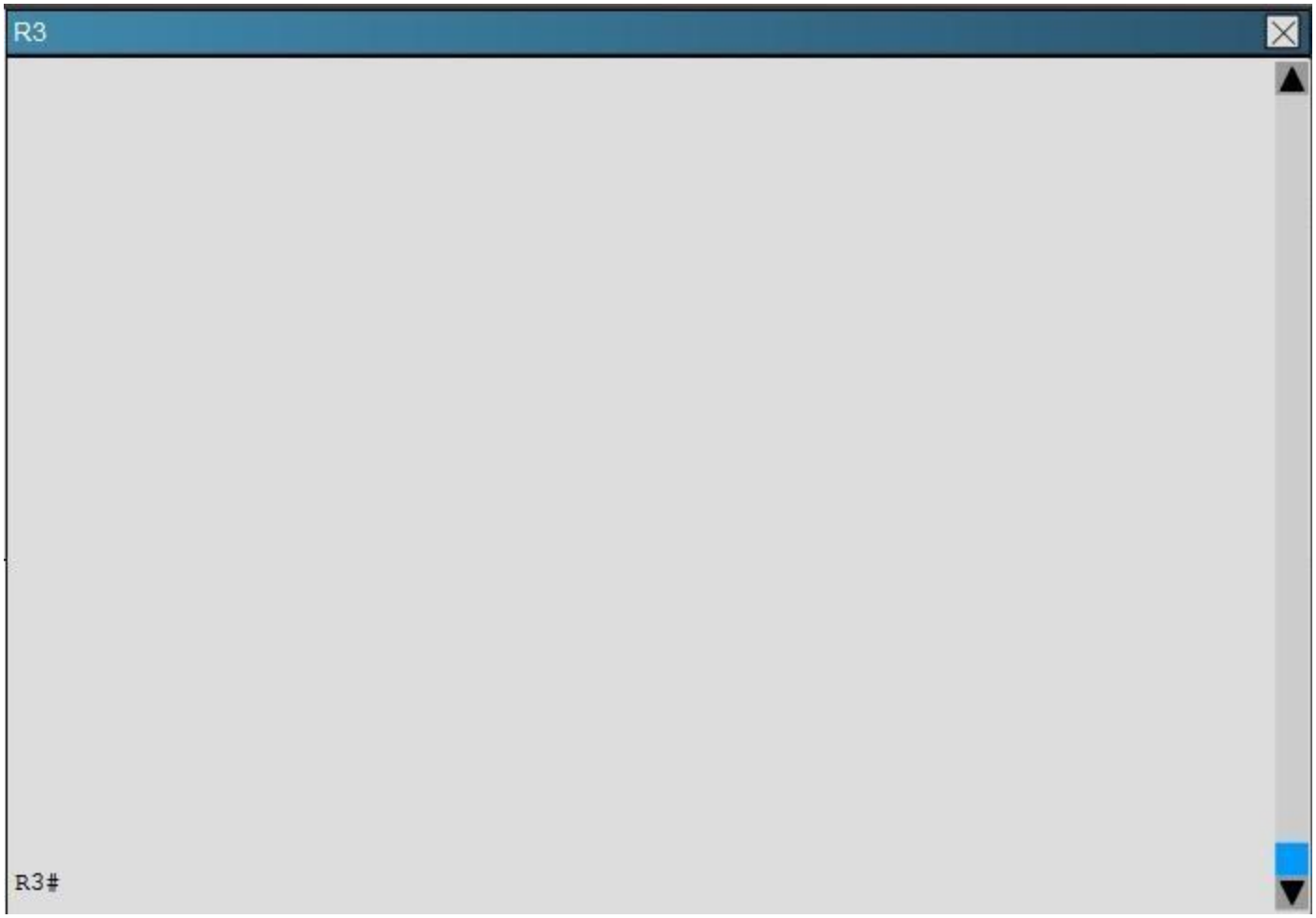
```
!
router ospf 100
 router-id 3.3.3.3
 area 1 virtual-link 4.4.4.4
 network 3.3.3.3 0.0.0.0 area 1
 network 192.168.13.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
 neighbor 192.168.13.1
!
!
```

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.


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



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
```

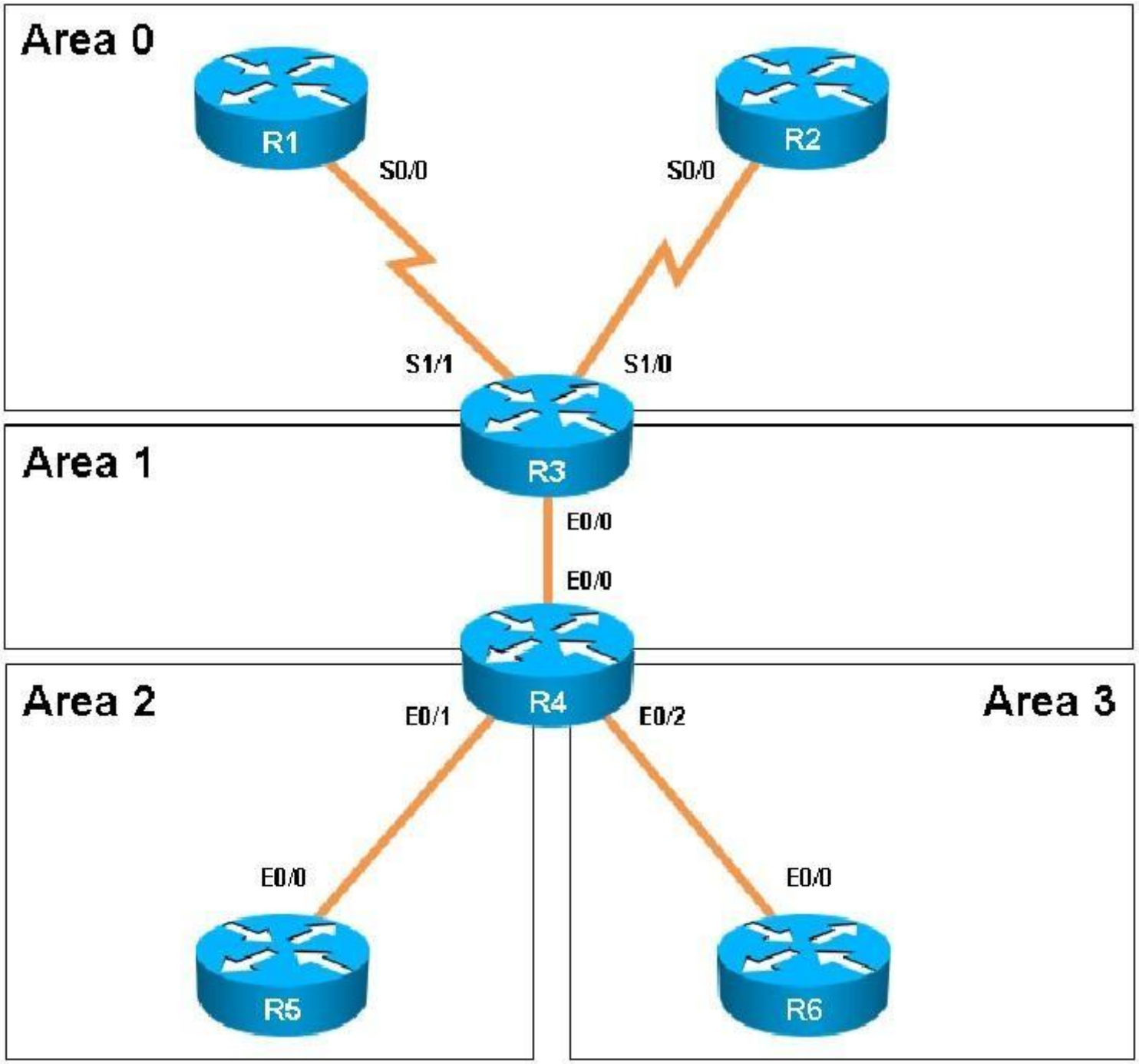
However, this has not been done on the link to R5 on R4:

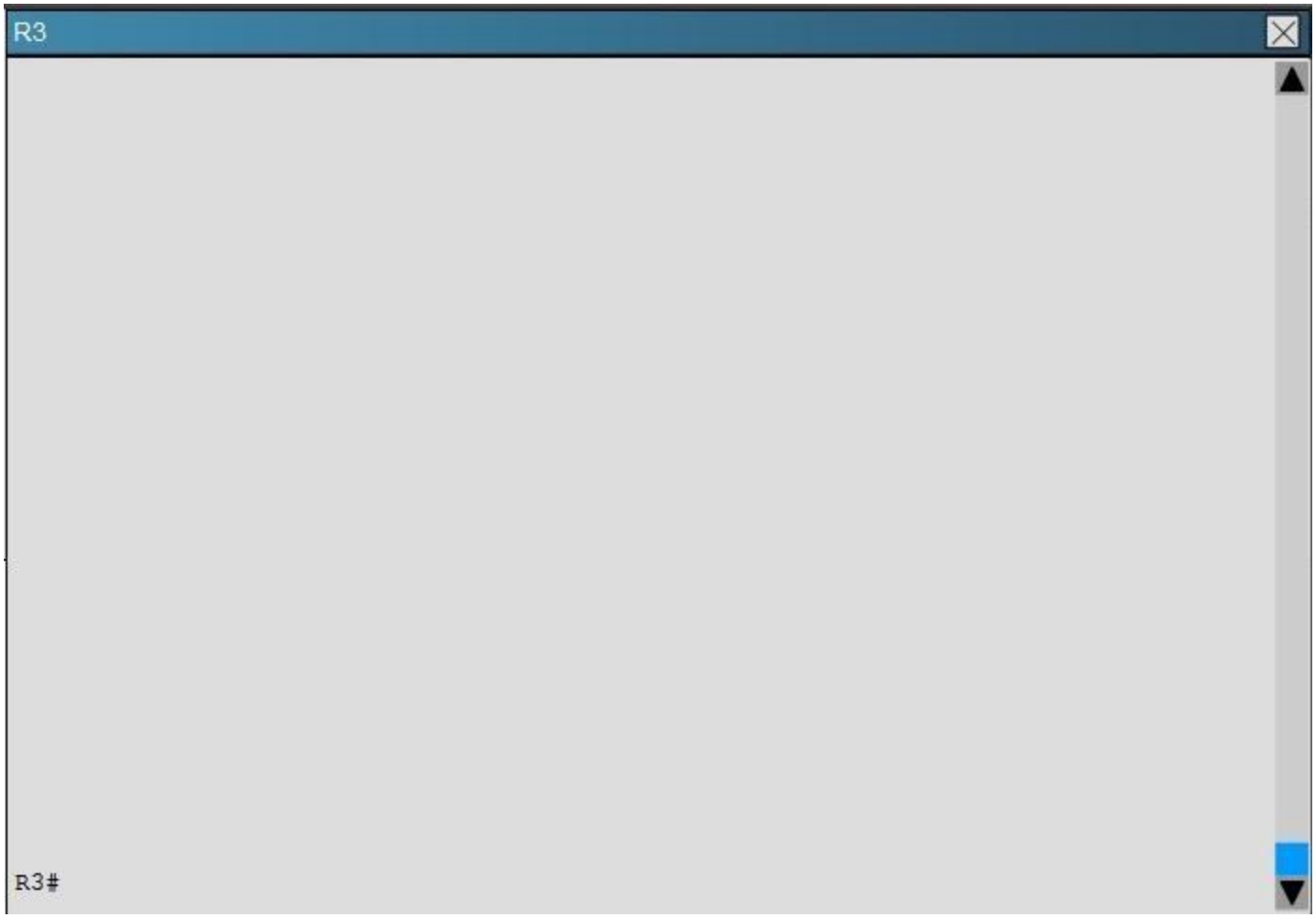
R4

```
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.


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



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.

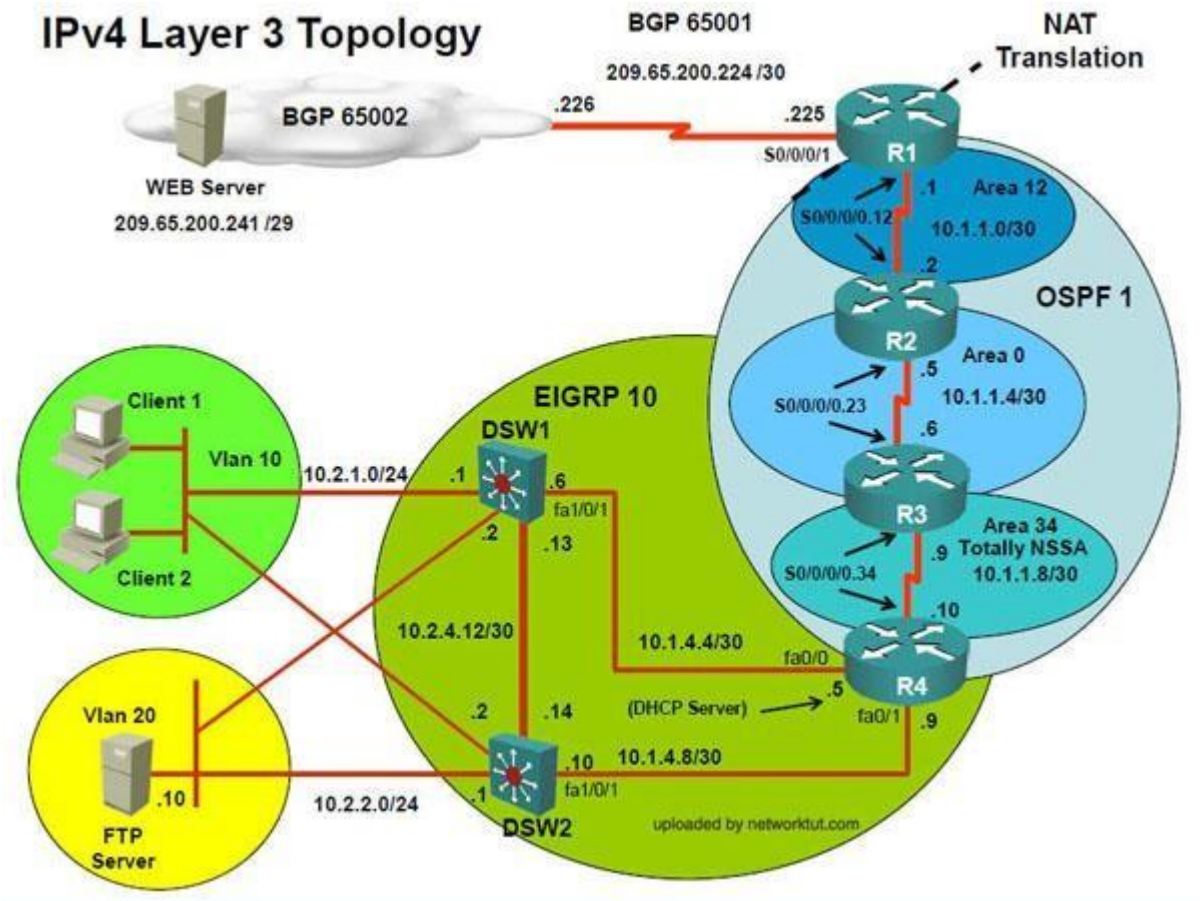
Question-1 Fault is found on which device,

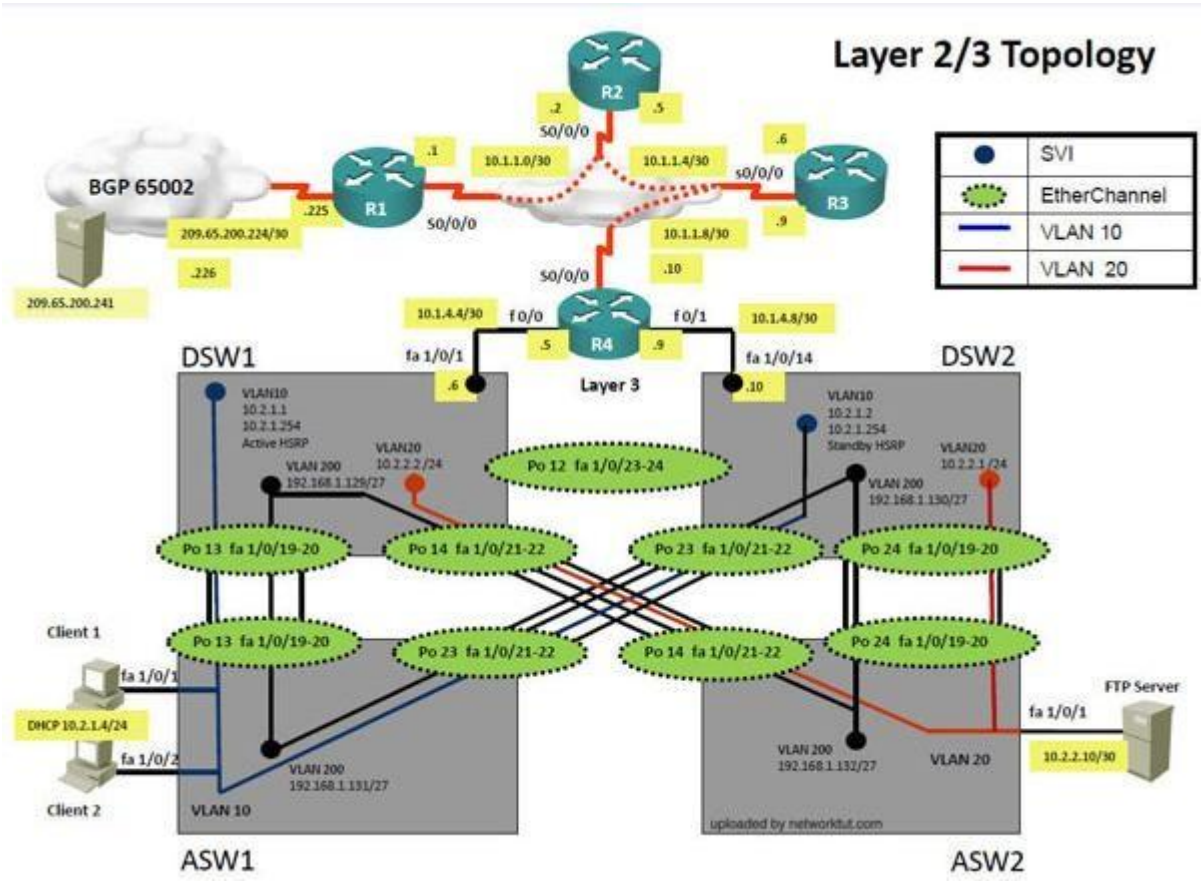
Question-2 Fault condition is related to,

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

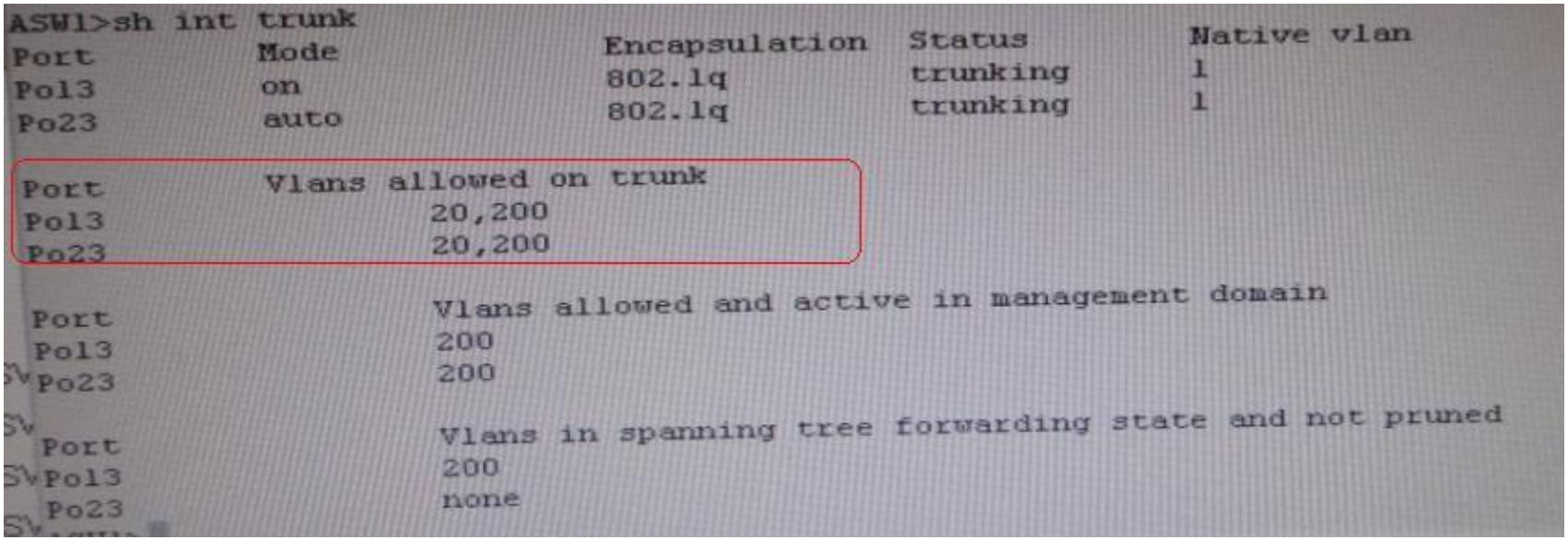
==========

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



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
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.

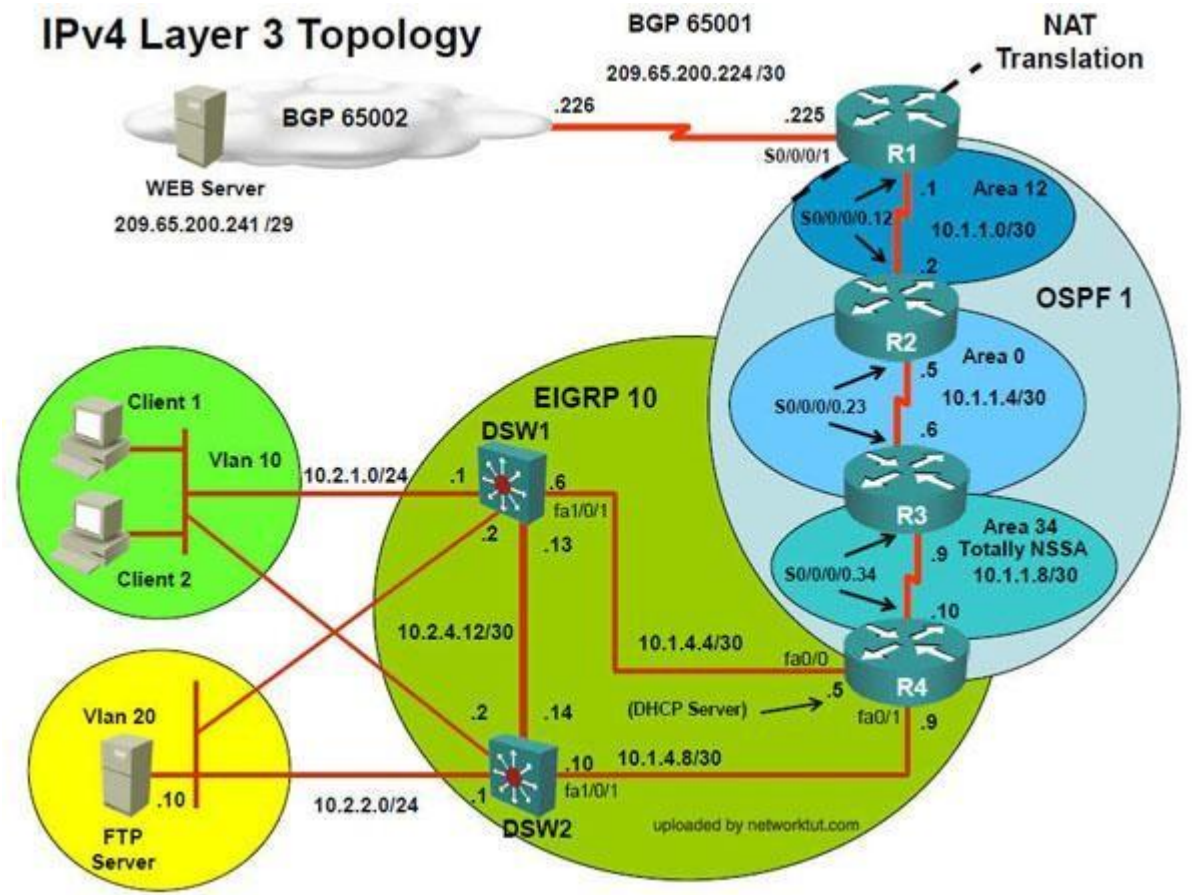
Question-1 Fault is found on which device,

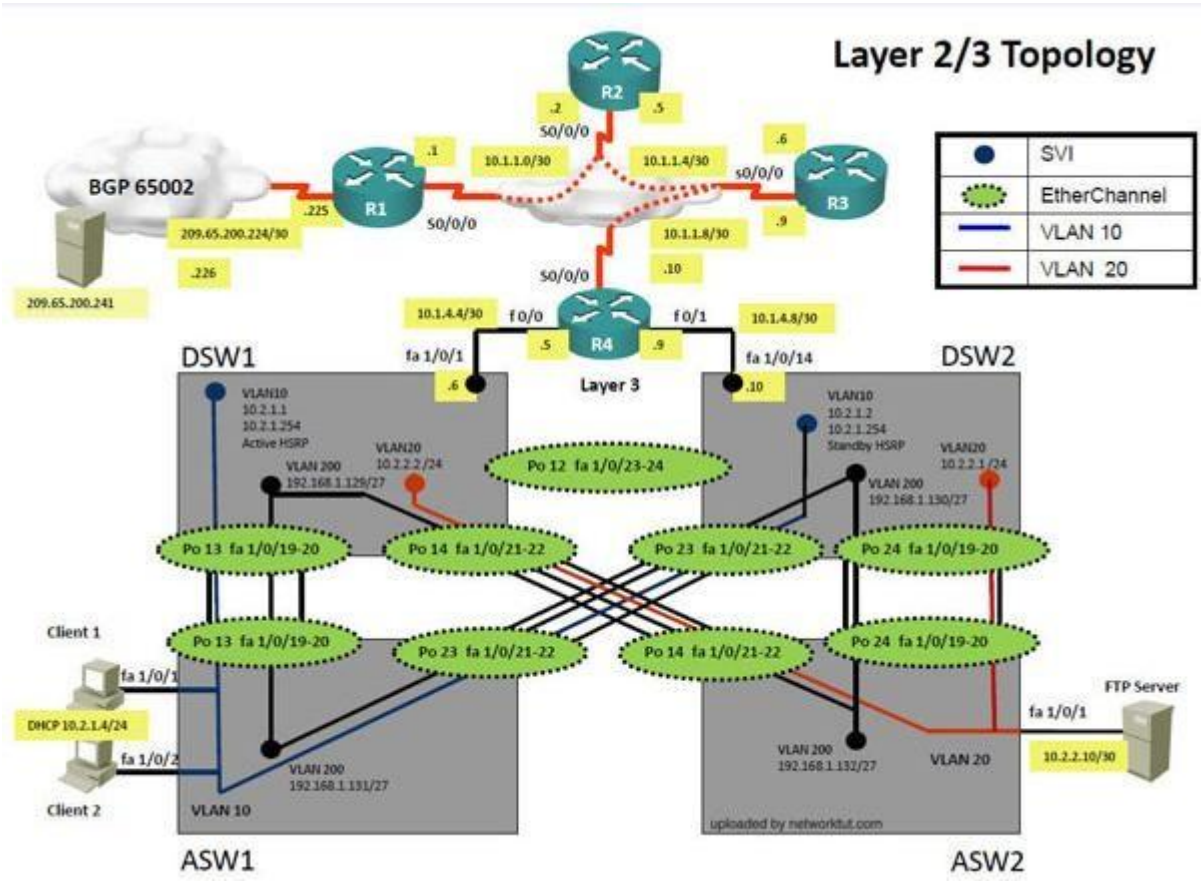
Question-2 Fault condition is related to,

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

==========

==========


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



Client is unable to ping IP 209.65.200.241

Solution

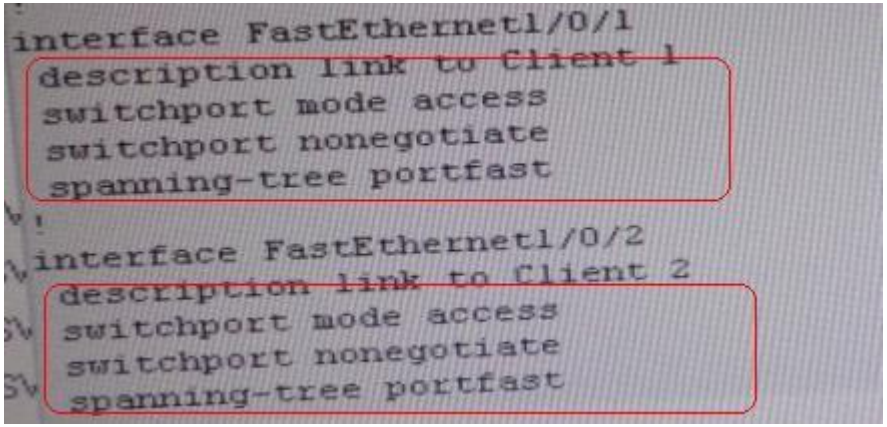
Steps need to follow as below:-

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

==========



==========

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 conditionwill 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.

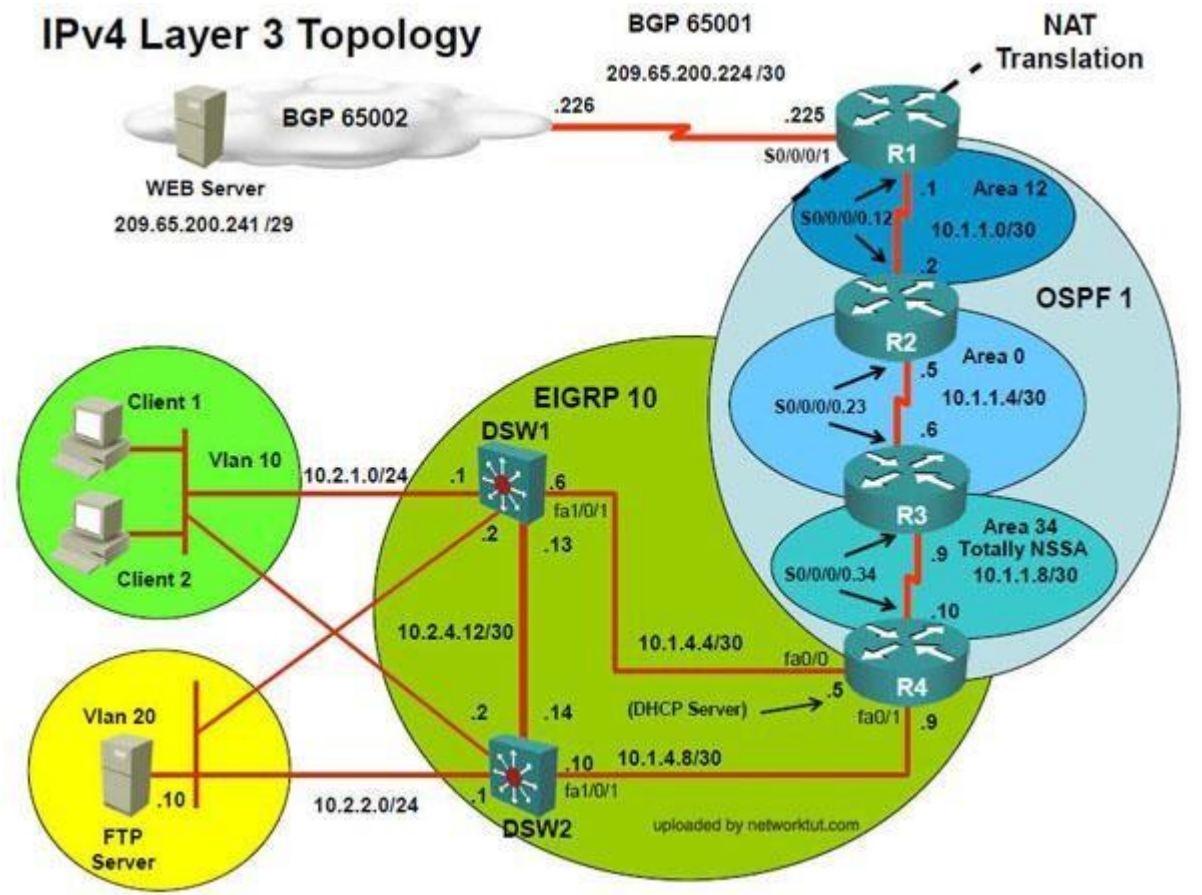
Question-1 Fault is found on which device,

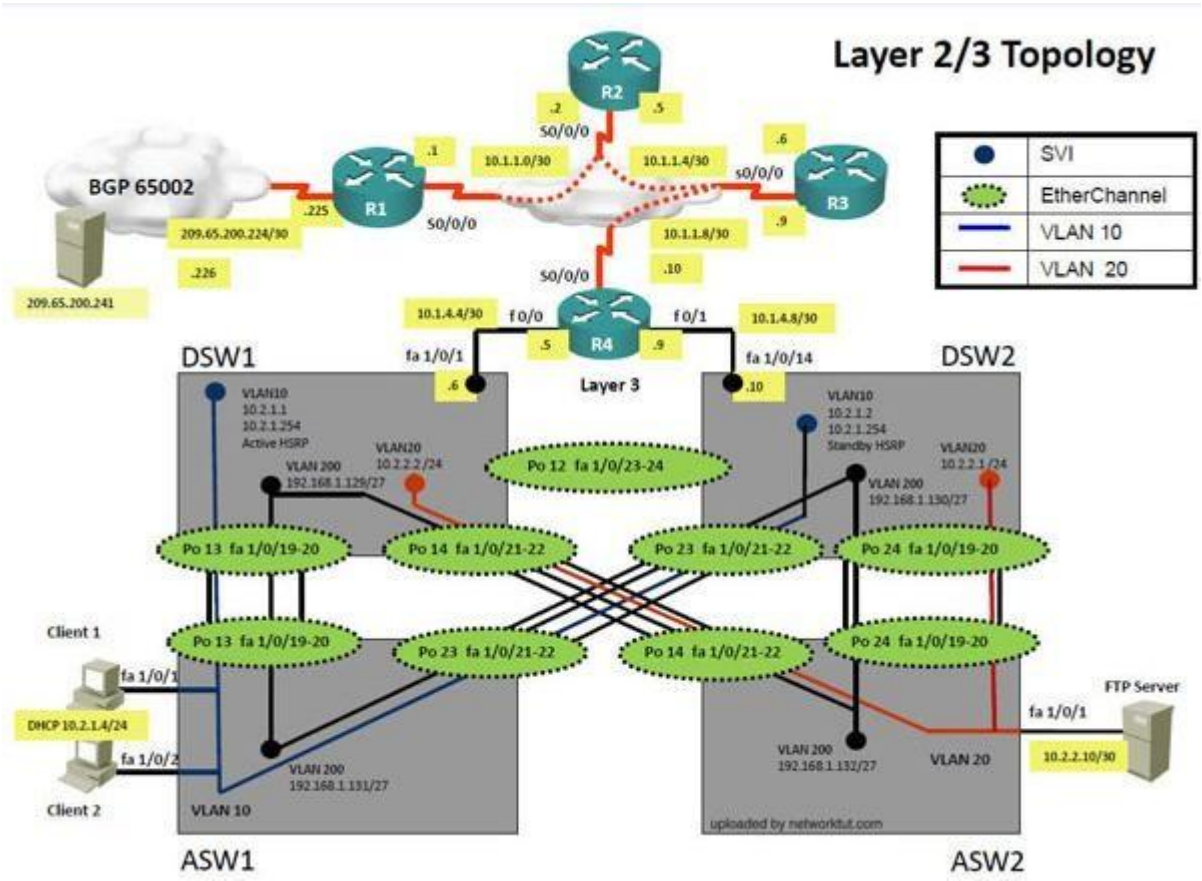
Question-2 Fault condition is related to,

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

==========

==========


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



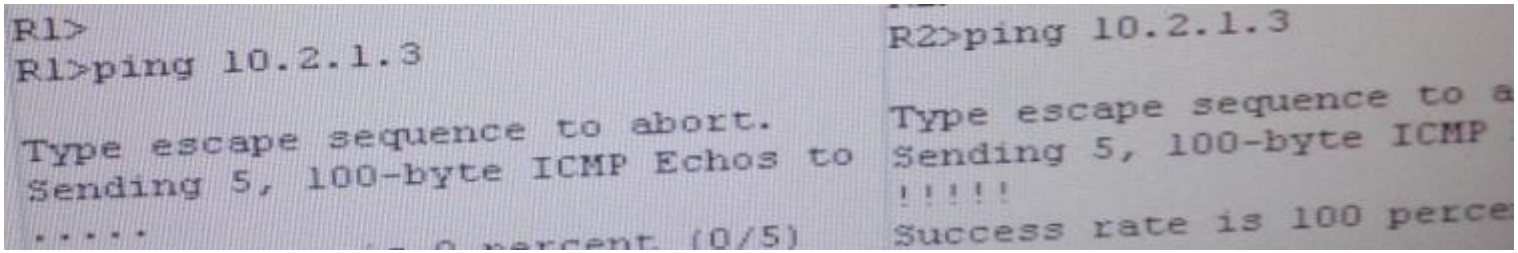
Client is unable to ping IP 209.65.200.241

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

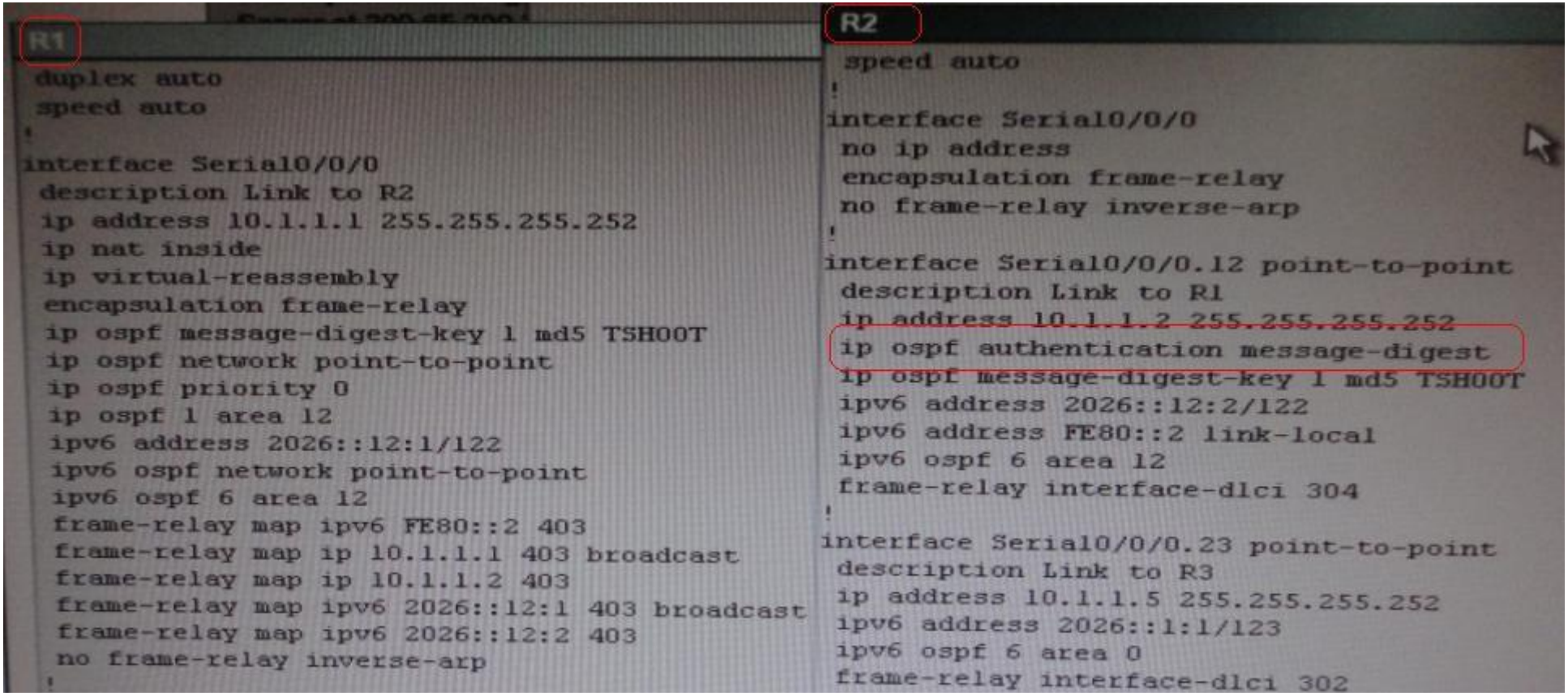
2. IP 10.2.1.3 will be able to ping from R4 , R3, R2 but not from R1



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



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.

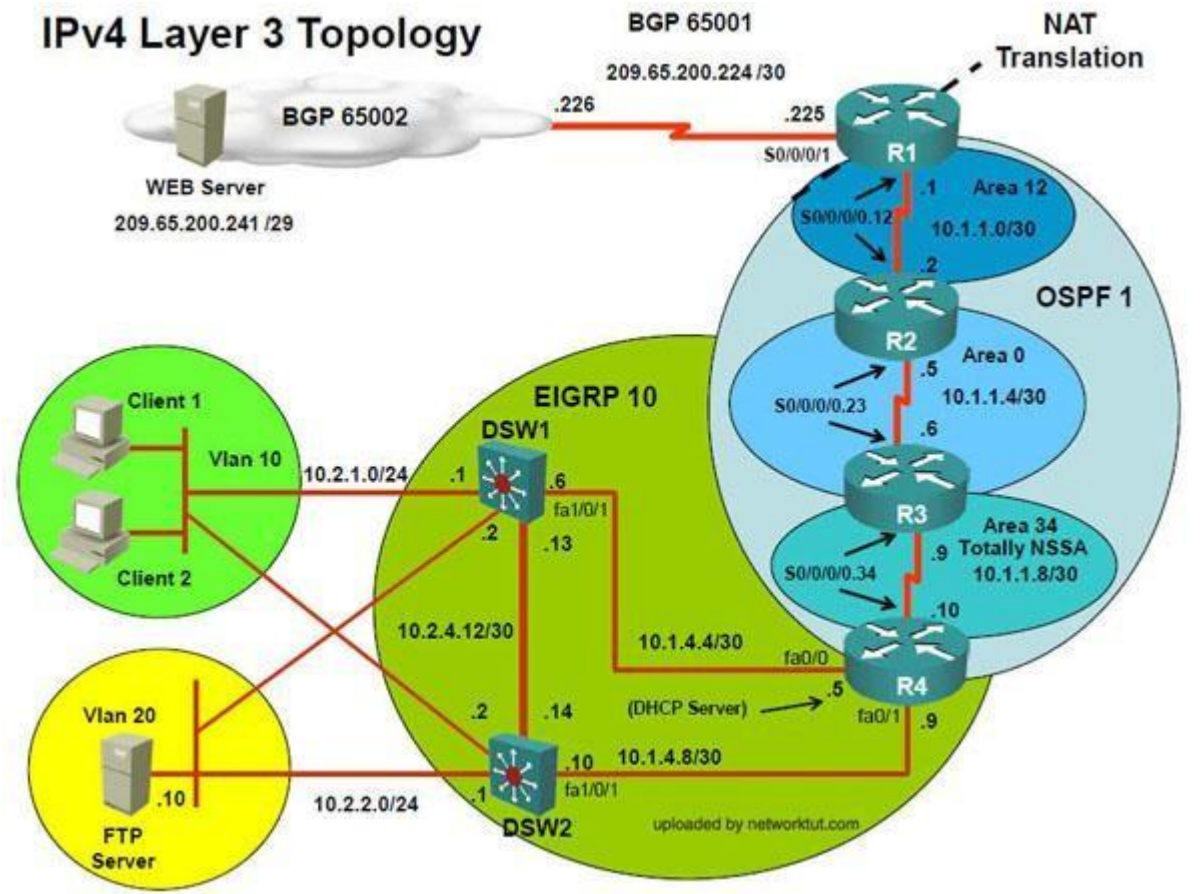
Question-1 Fault is found on which device,

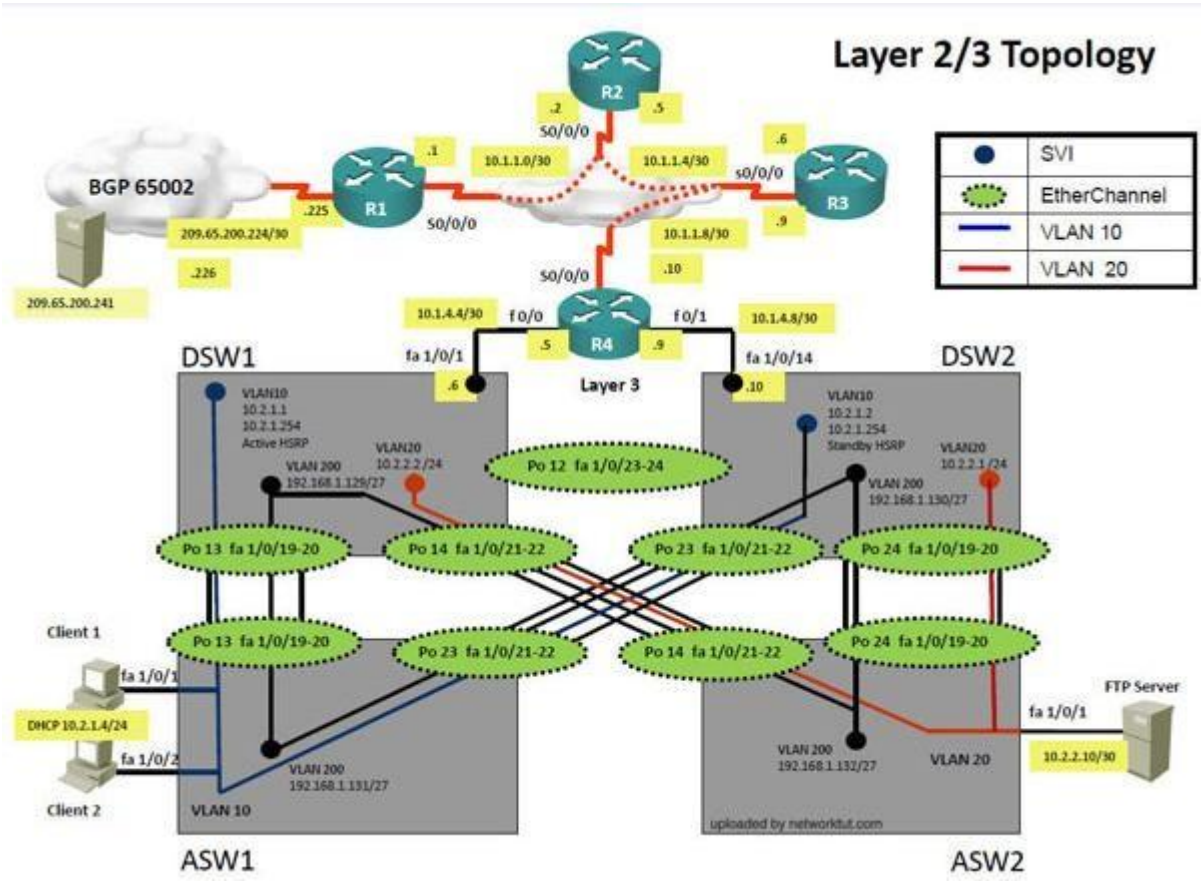
Question-2 Fault condition is related to,

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

==========

==========


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



Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

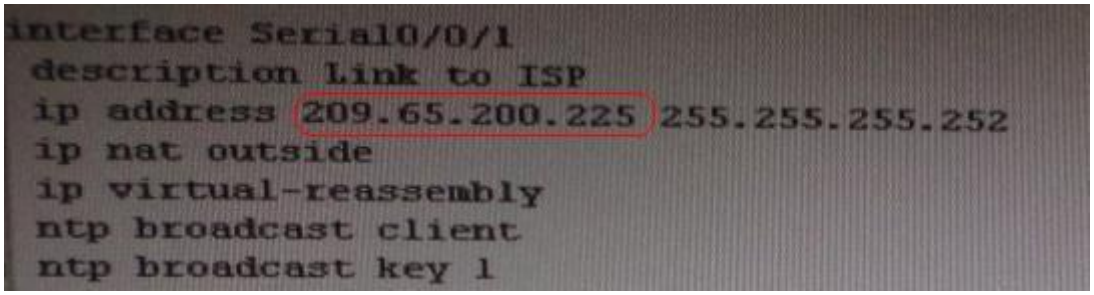
1) When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
ipconfig ----- Client will be receiving IP address 10.2.1.3

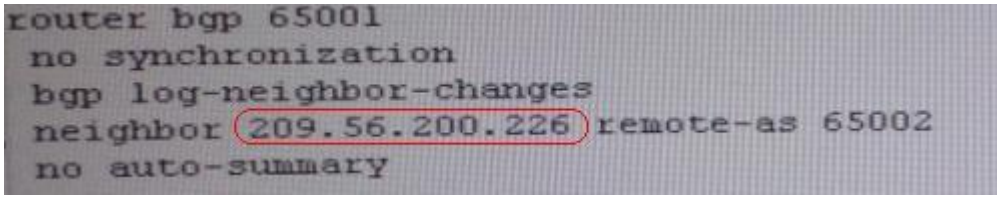
2) IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1

3) Look for BGP Neighbourship
Shipbgp 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





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

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. Redistrution is enabled where necessary.

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

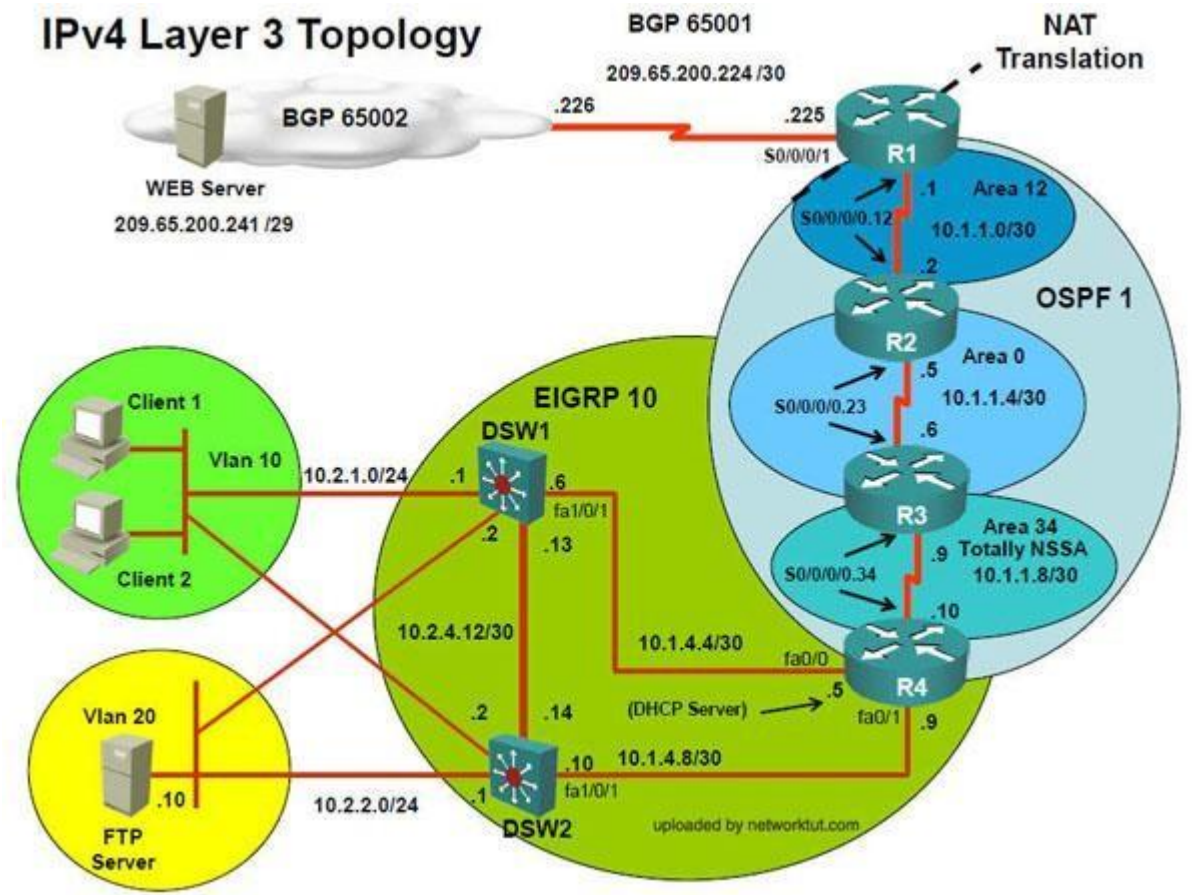
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.
Each ticket has 3 sub questions that need to be answered & topology remains same.

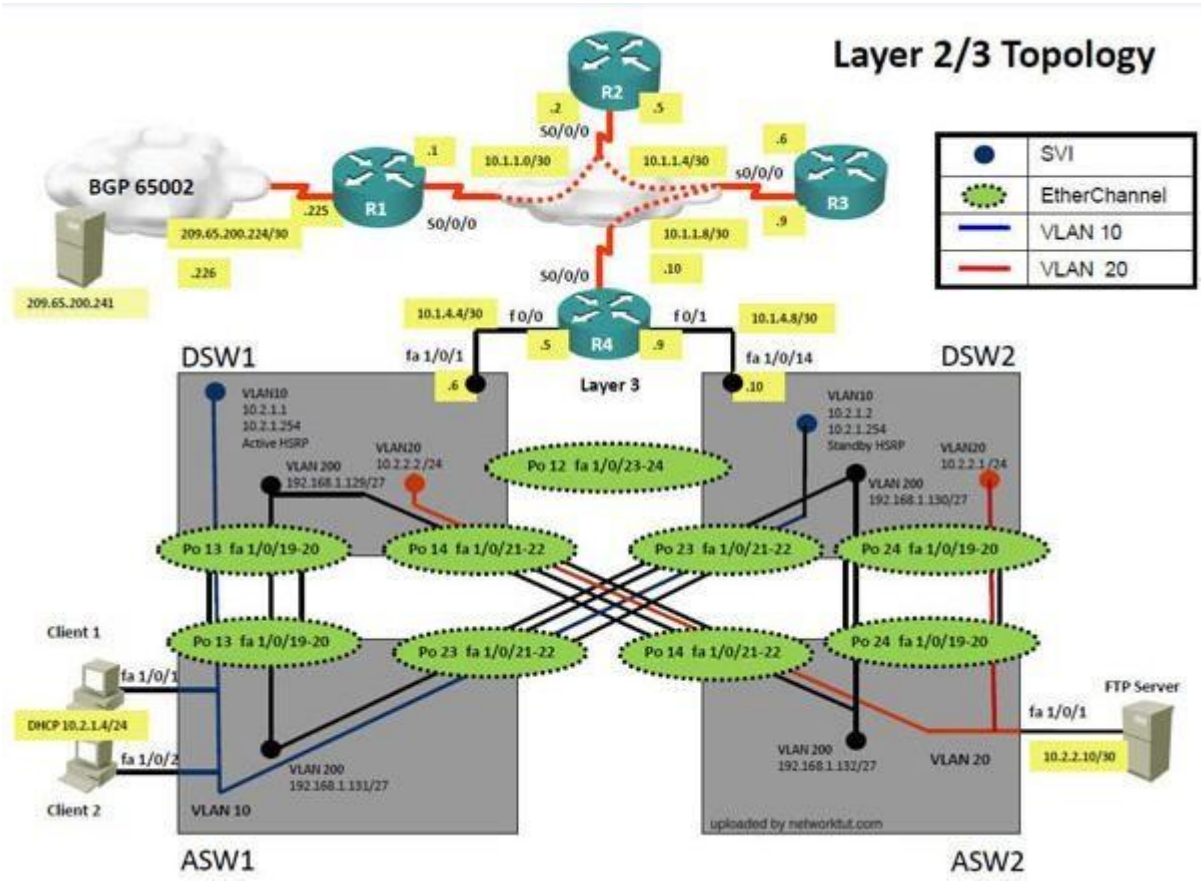
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

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

==========


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



Client is unable to ping IP 209.65.200.241

Solution

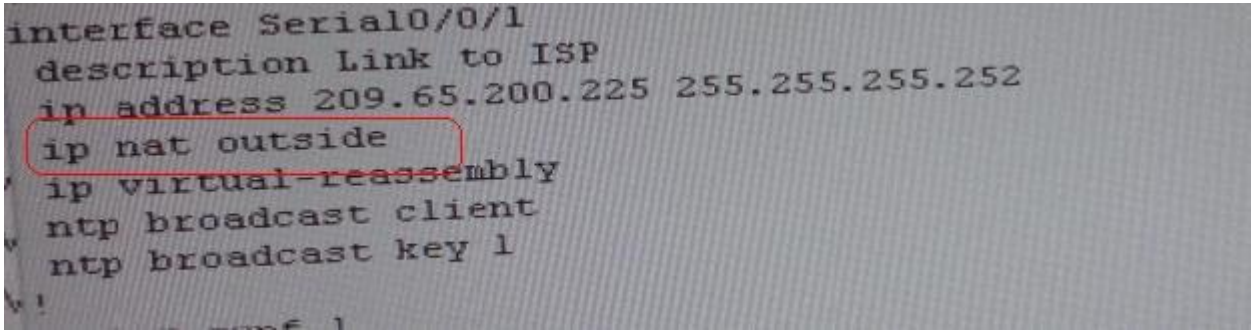
Steps need to follow as below:-

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

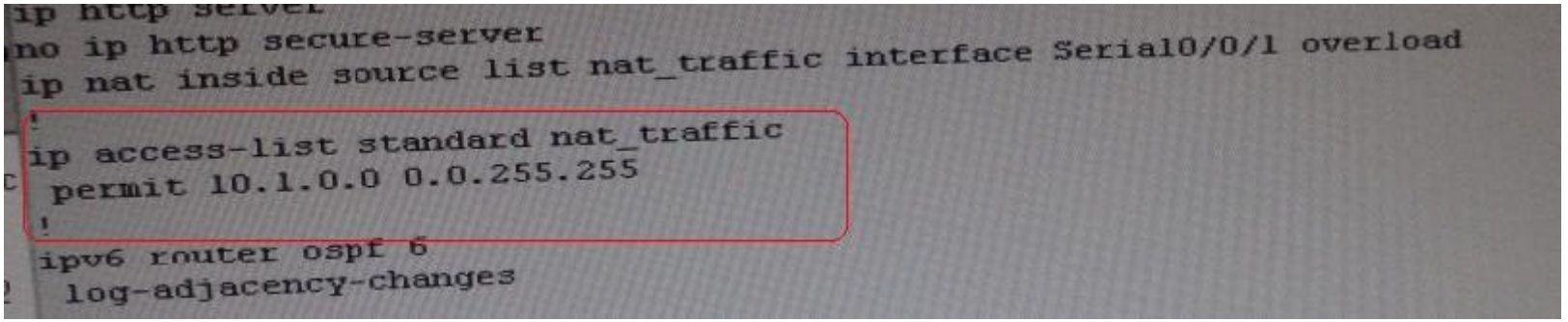
2) IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1

3) Look for BGP Neighbourship
Shipbgp 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..



!



!

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_trafic configuration enter the permit 10.2.0.0 0.0.255.255 command.
D. Under the ip access-list standard nat_trafic configuration enter the permit 209.65.200.0 0.0.0.255 command.

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.

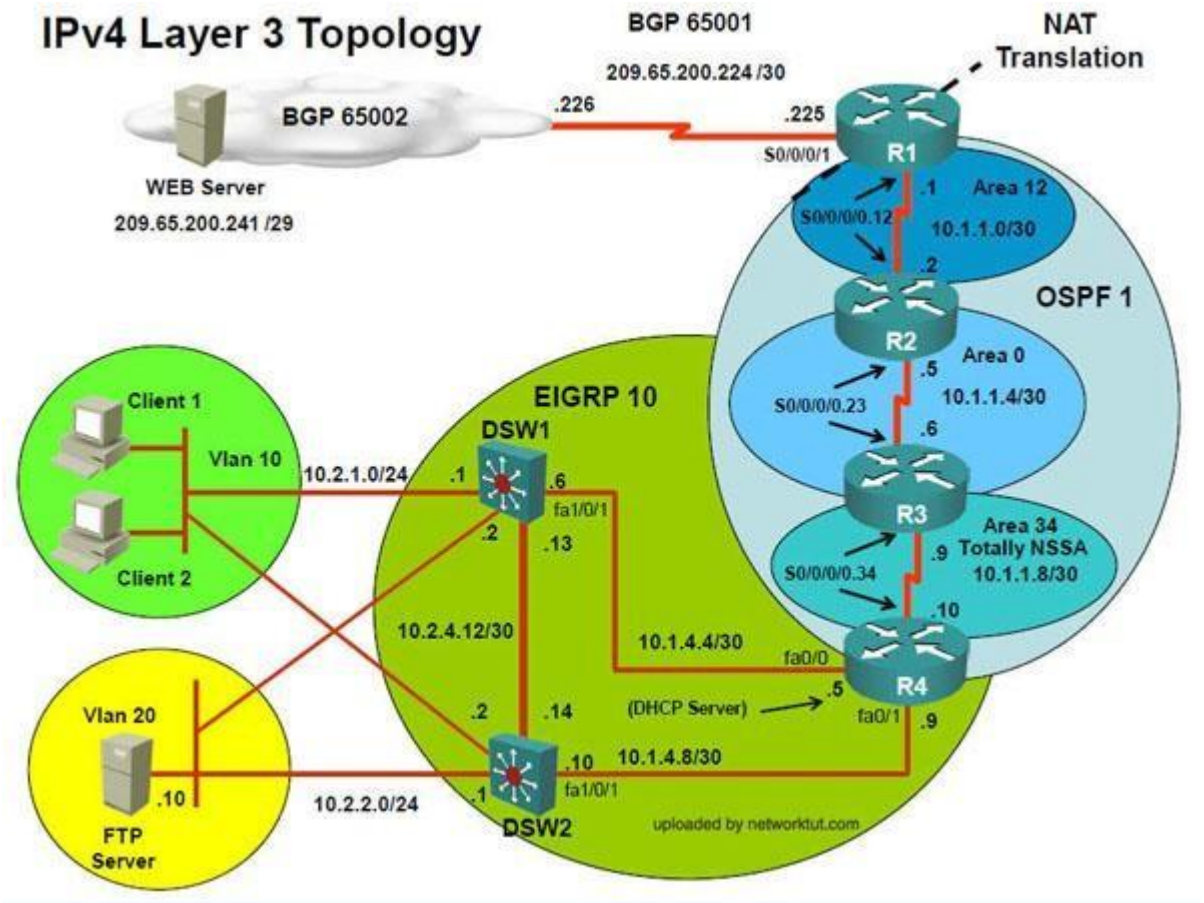
Each ticket has 3 sub questions that need to be answered & topology remains same.

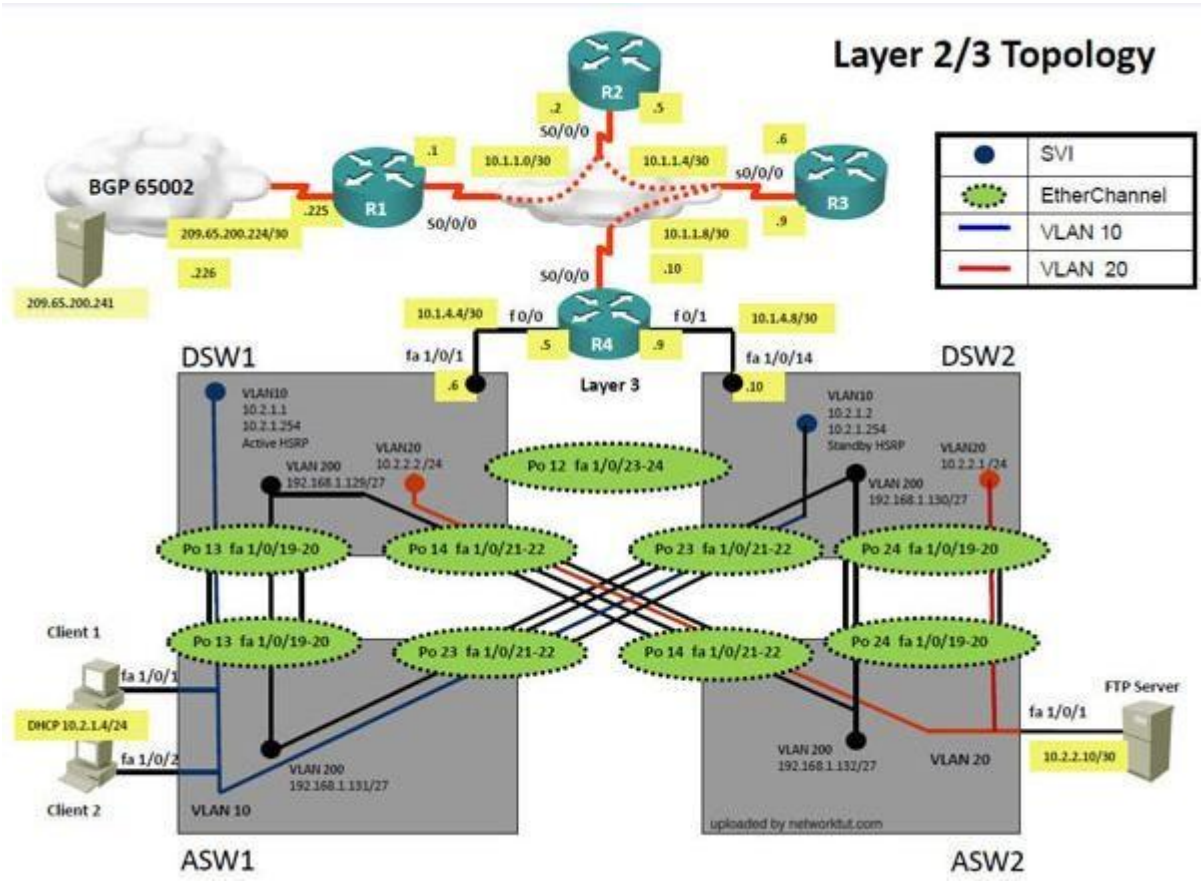
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

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

==========





Client is unable to ping IP 209.65.200.241...

Solution

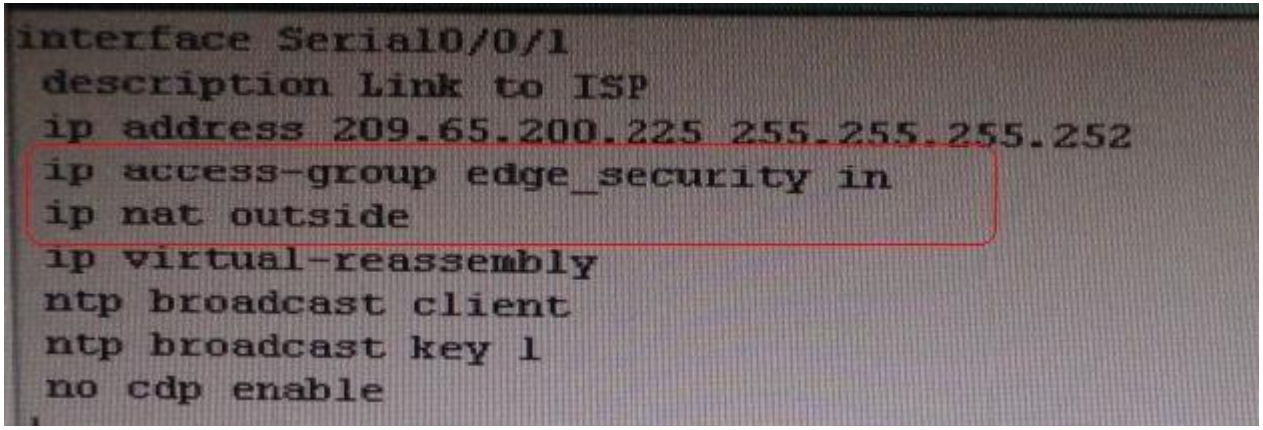
Steps need to follow as below:-

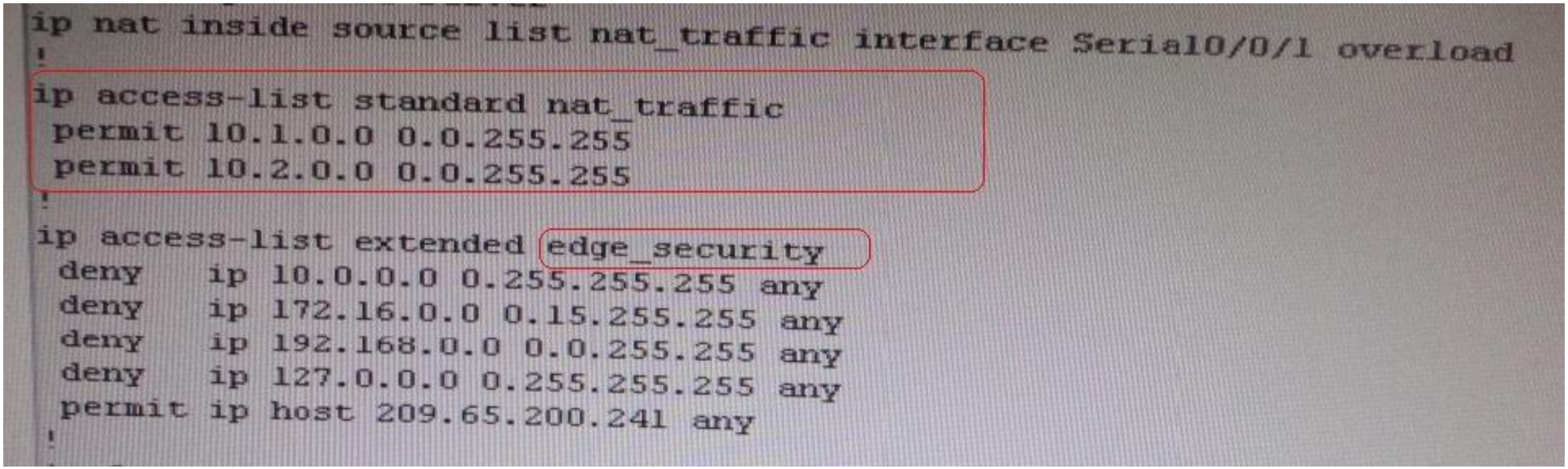
1) When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
2) Ipconfig ----- Client will be receiving IP address 10.2.1.3

3) IP 10.2.1.3 will be able to ping from R4 , R3, R2, R1

4) Look for BGP Neighbourship
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)





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 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
HSRP is running between DSW1 & DSW2 Switches

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

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

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

DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.

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

ASW1 and ASW2 are layer 2 switches.

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

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

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

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

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

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

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

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

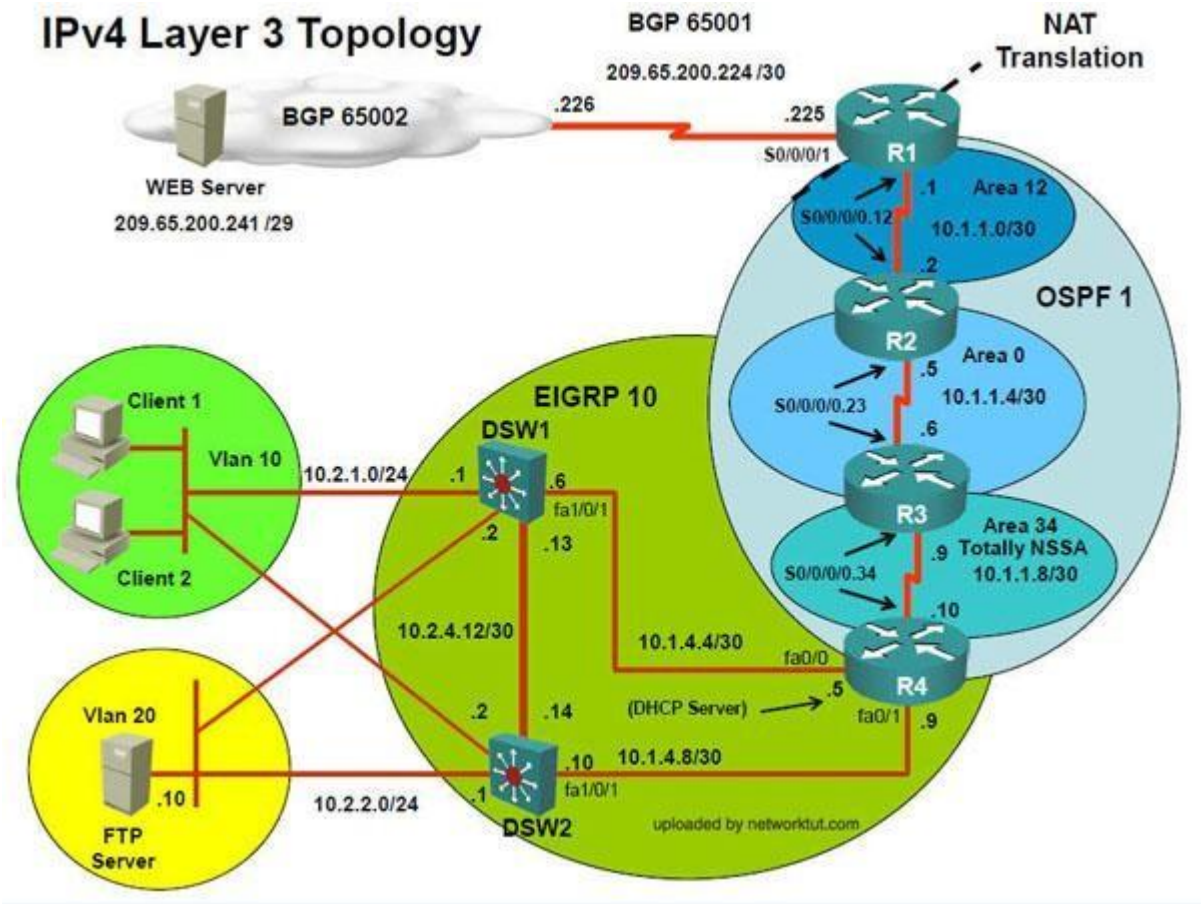
Each ticket has 3 sub questions that need to be answered & topology remains same.

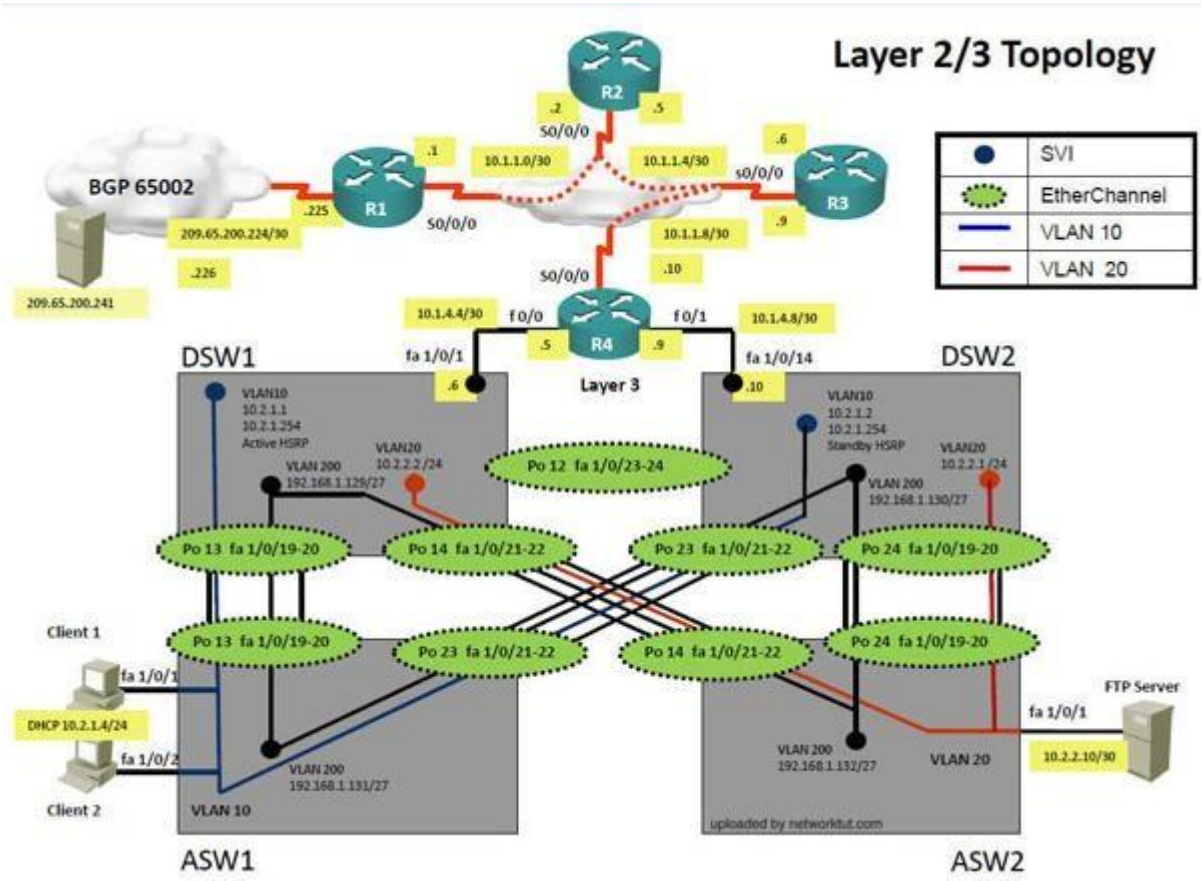
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

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

==========





Client is unable to ping IP 209.65.200.241

Solution

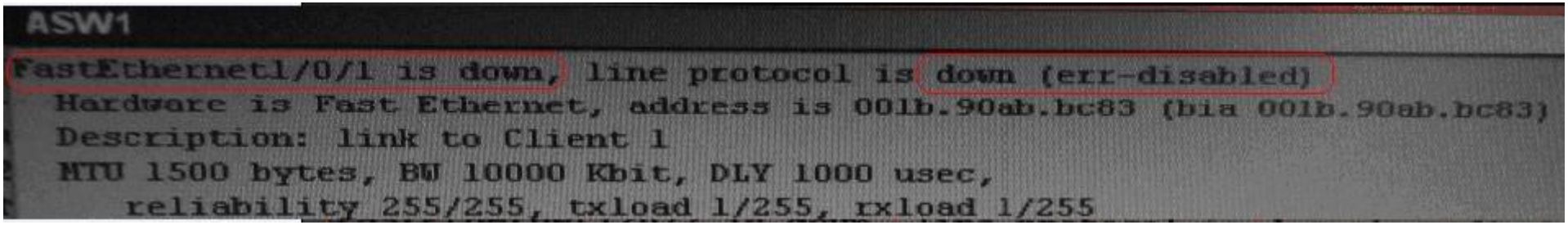
Steps need to follow as below:-

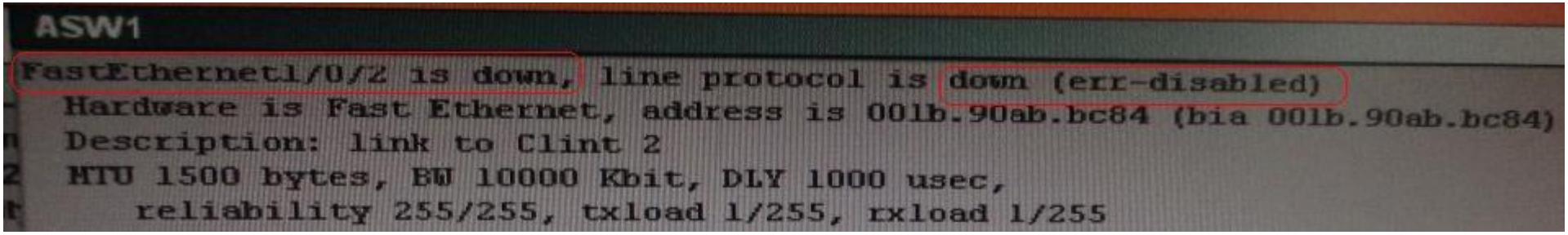
1) When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig----- Client will be getting 169.X.X.X

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





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 Vlans
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 1/01 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. Redistrution is enabled where necessary.

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

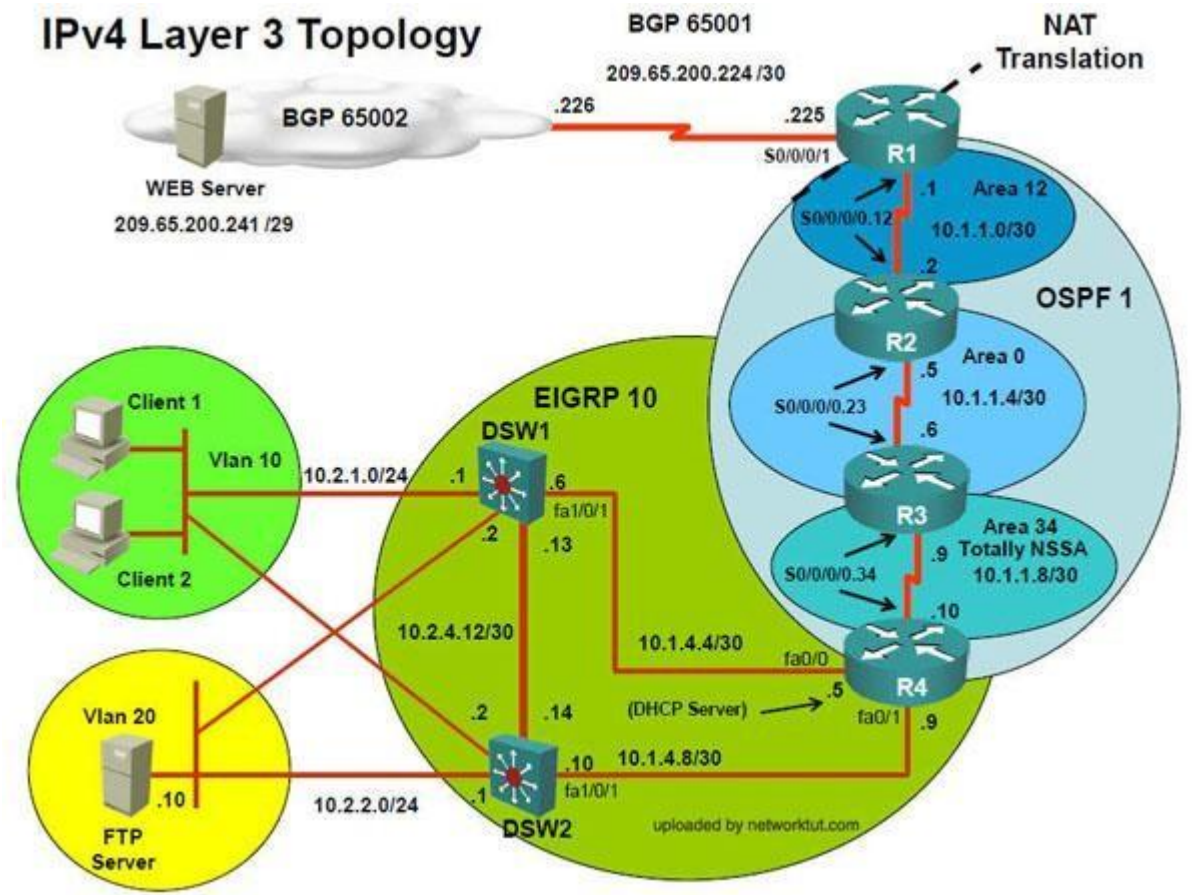
Each ticket has 3 sub questions that need to be answered & topology remains same.

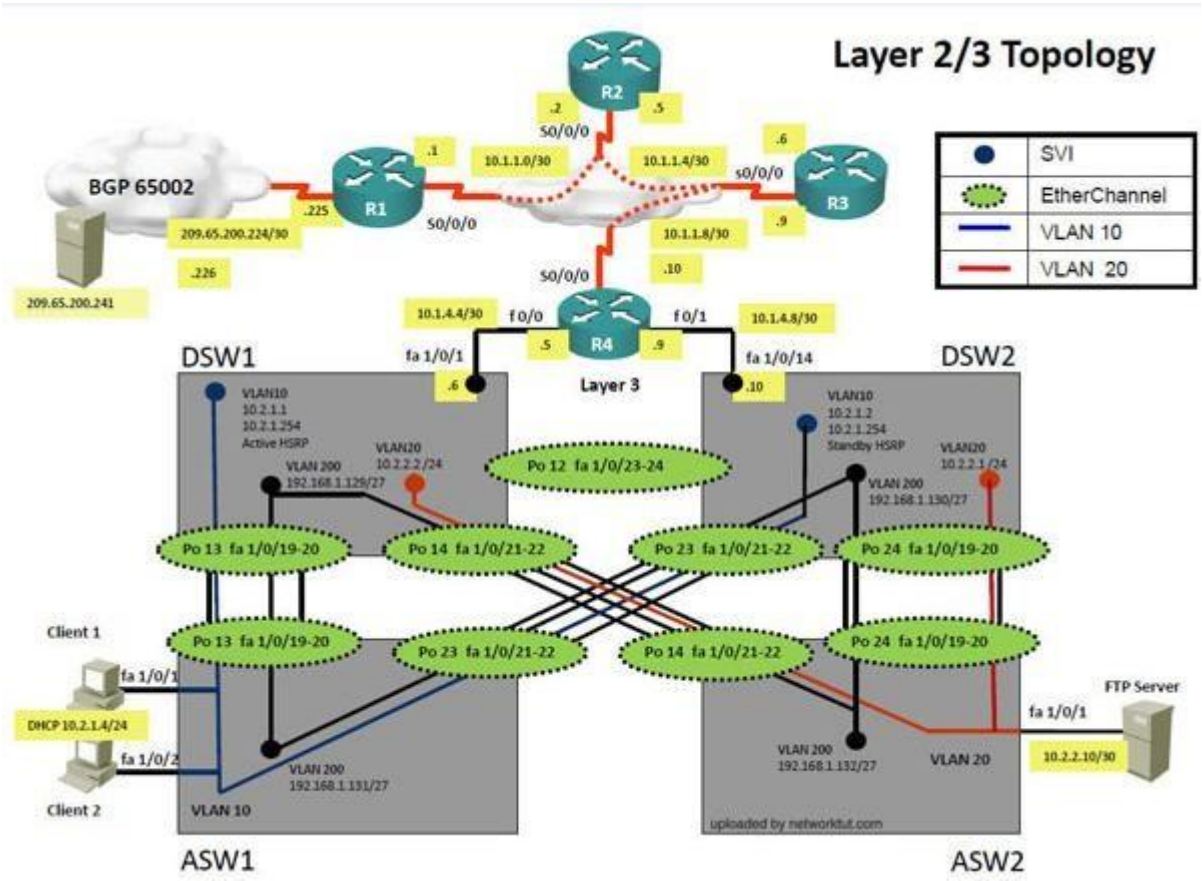
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

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

==========


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



Client is unable to ping IP 209.65.200.241

Solution

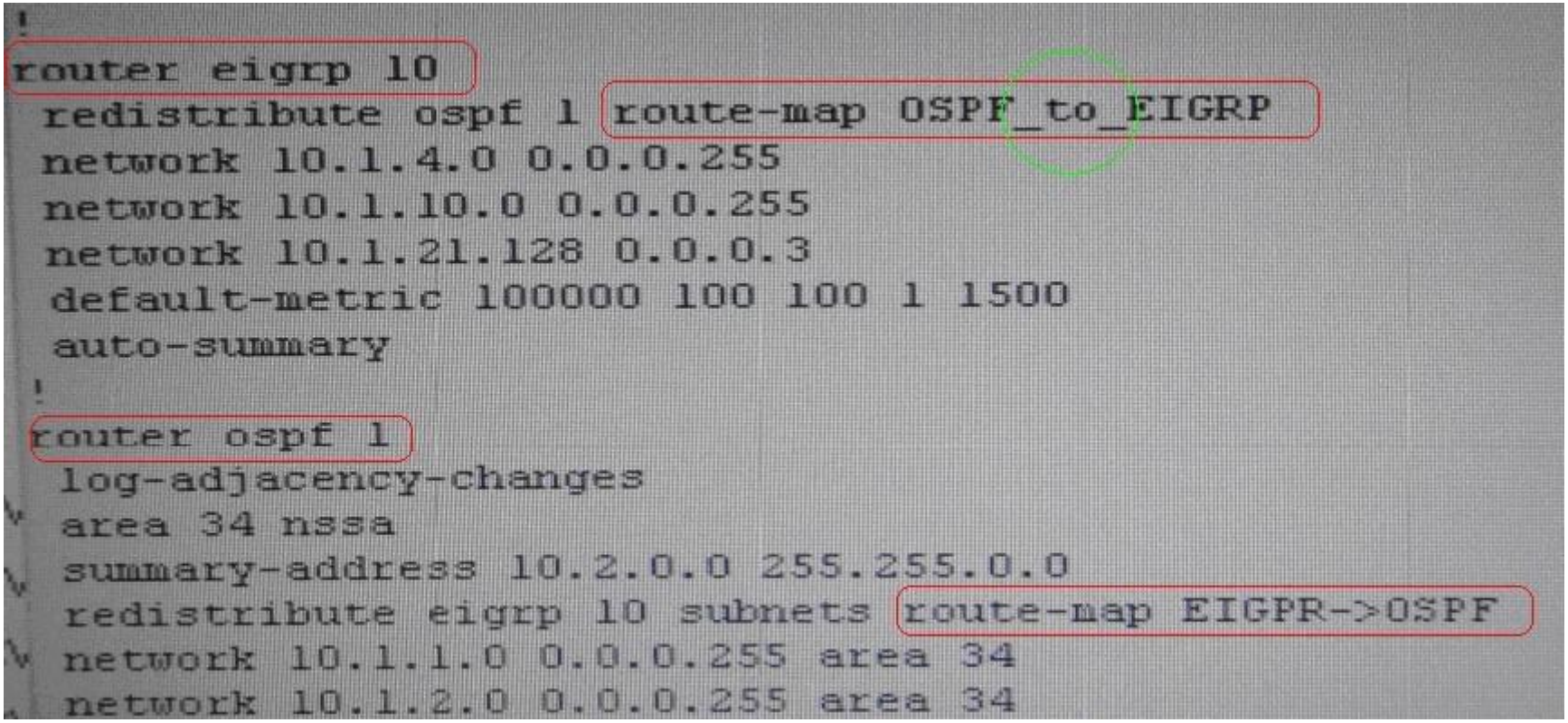
Steps need to follow as below:-

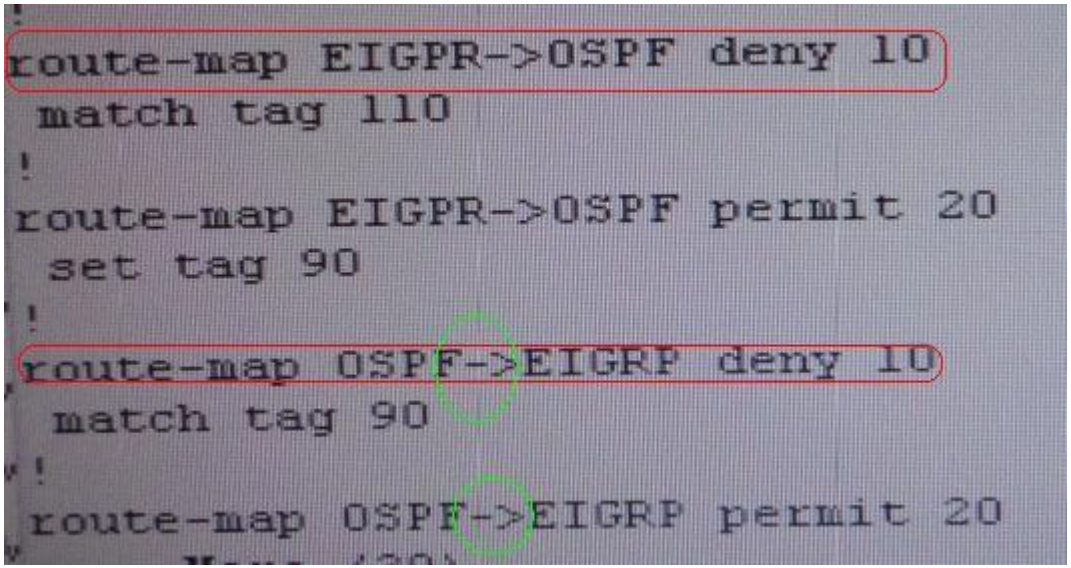
1) When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig----- Client will be receiving IP address 10.2.1.3

2) IP 10.2.1.3 will be able to ping from R4 , but cannot ping from R3, R2, R1

3) This clearly shows problem at R4 since EIGRP is between DSW1, DSW2 & R4 and OSPF protocol is running between R4, R3, R2, R1 so routes from R4 are not propagated to R3, R2, R1

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.





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. Redistrution is enabled where necessary.

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

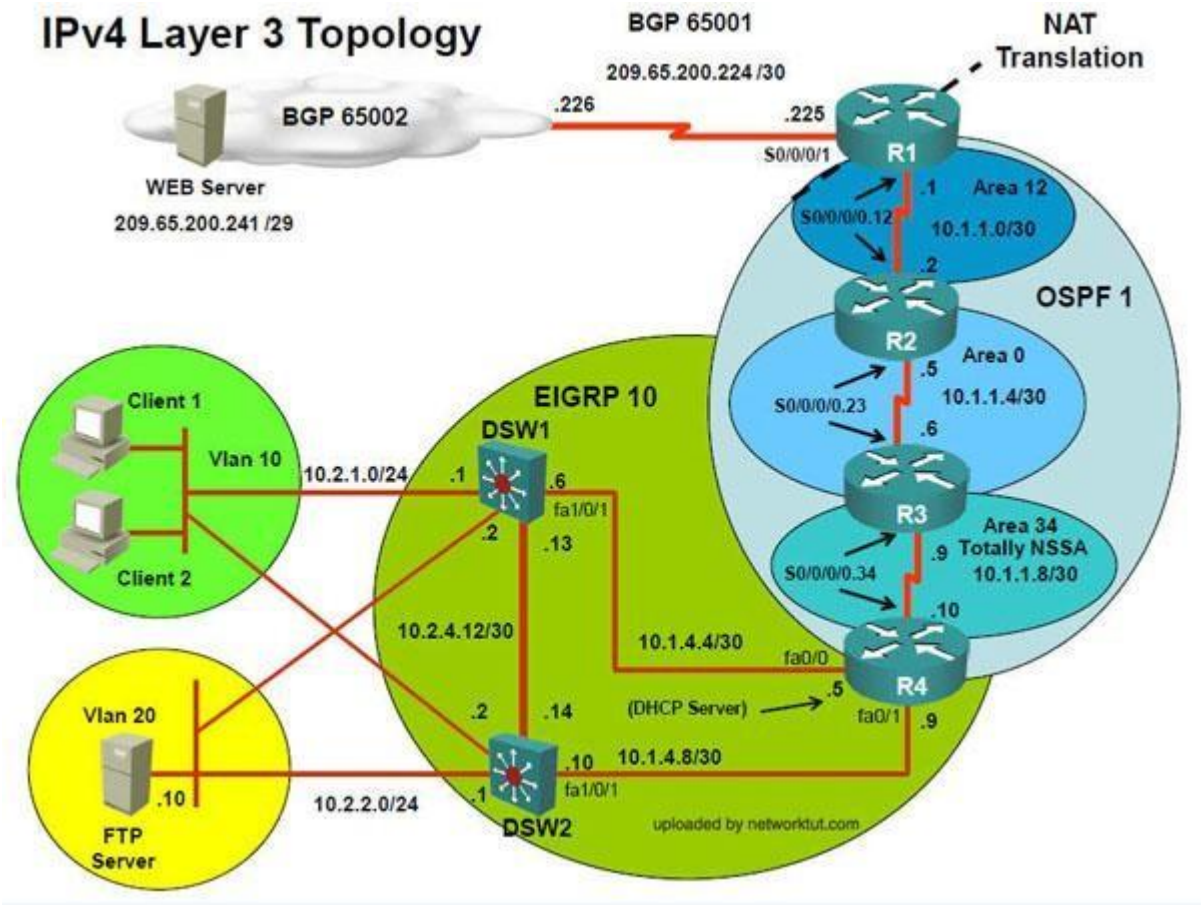
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

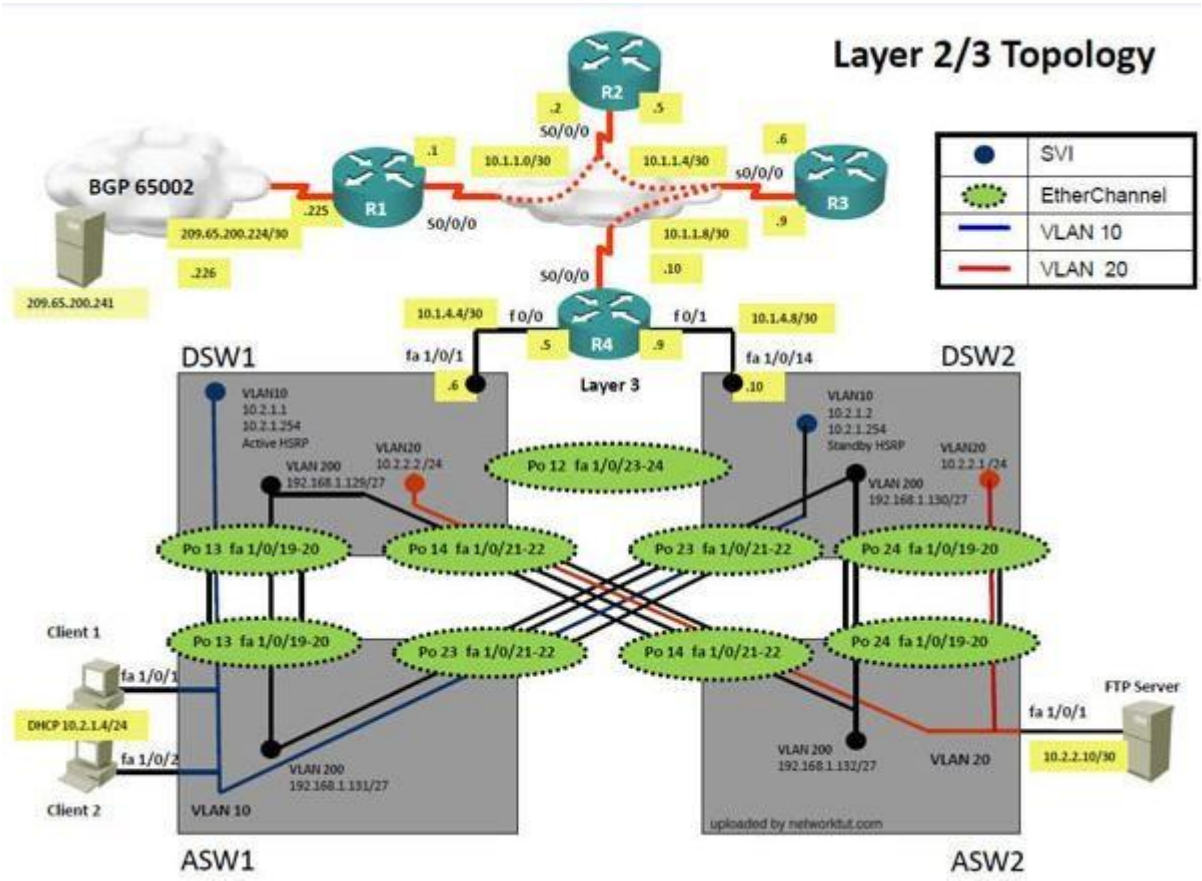
Each ticket has 3 sub questions that need to be answered & topology remains same.

Question-1 Fault is found on which device,

Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution

==========


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



Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

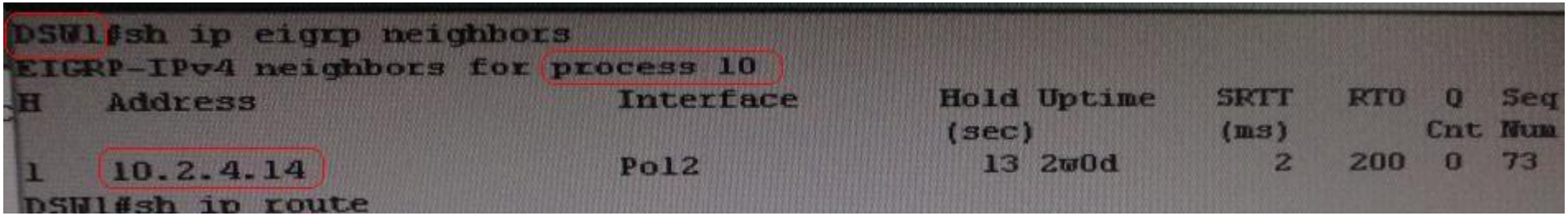
1) When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 ipconfig ----- Client will be receiving IP address 10.2.1.3

2) 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

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...



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
HSRP is running between DSW1 & DSW2 Switches

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

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

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

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

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

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

ASW1 and ASW2 are layer 2 switches.

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

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

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

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

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

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

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

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

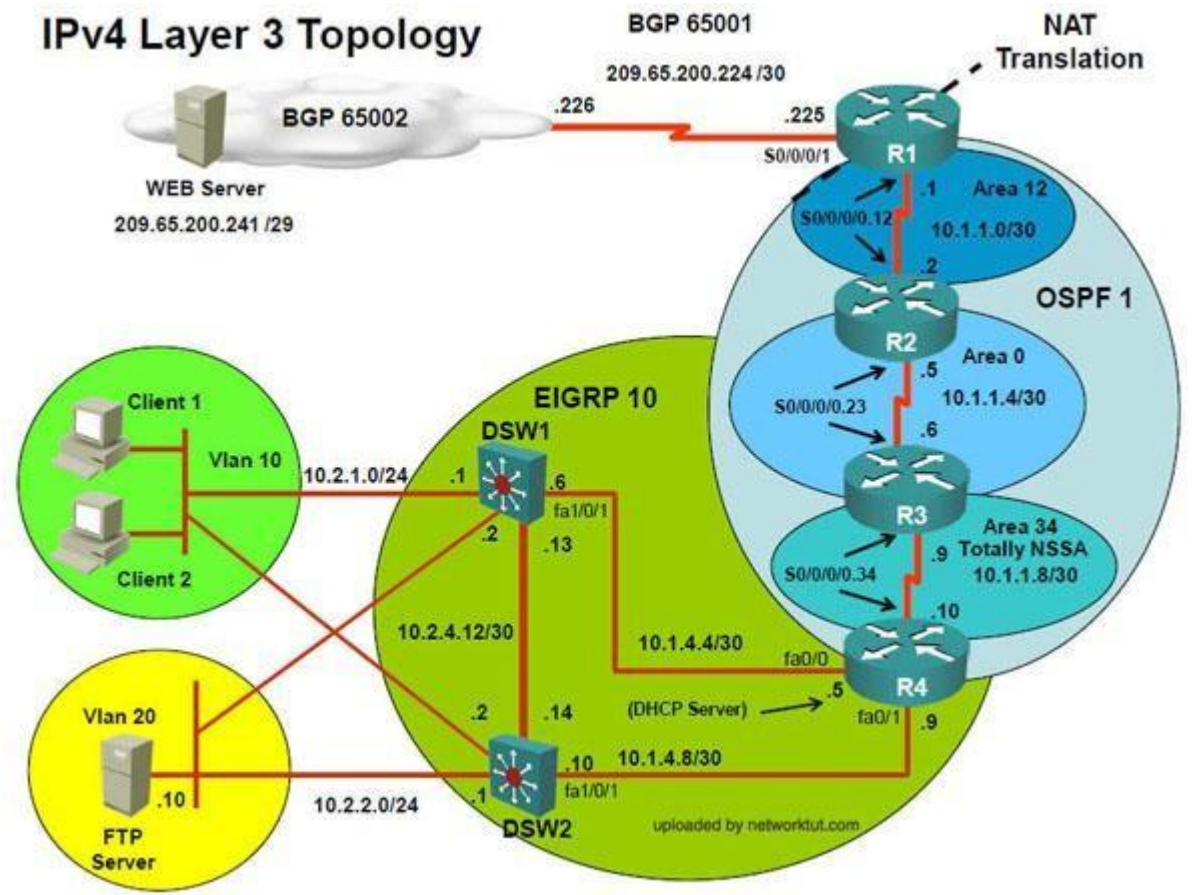
Each ticket has 3 sub questions that need to be answered & topology remains same.

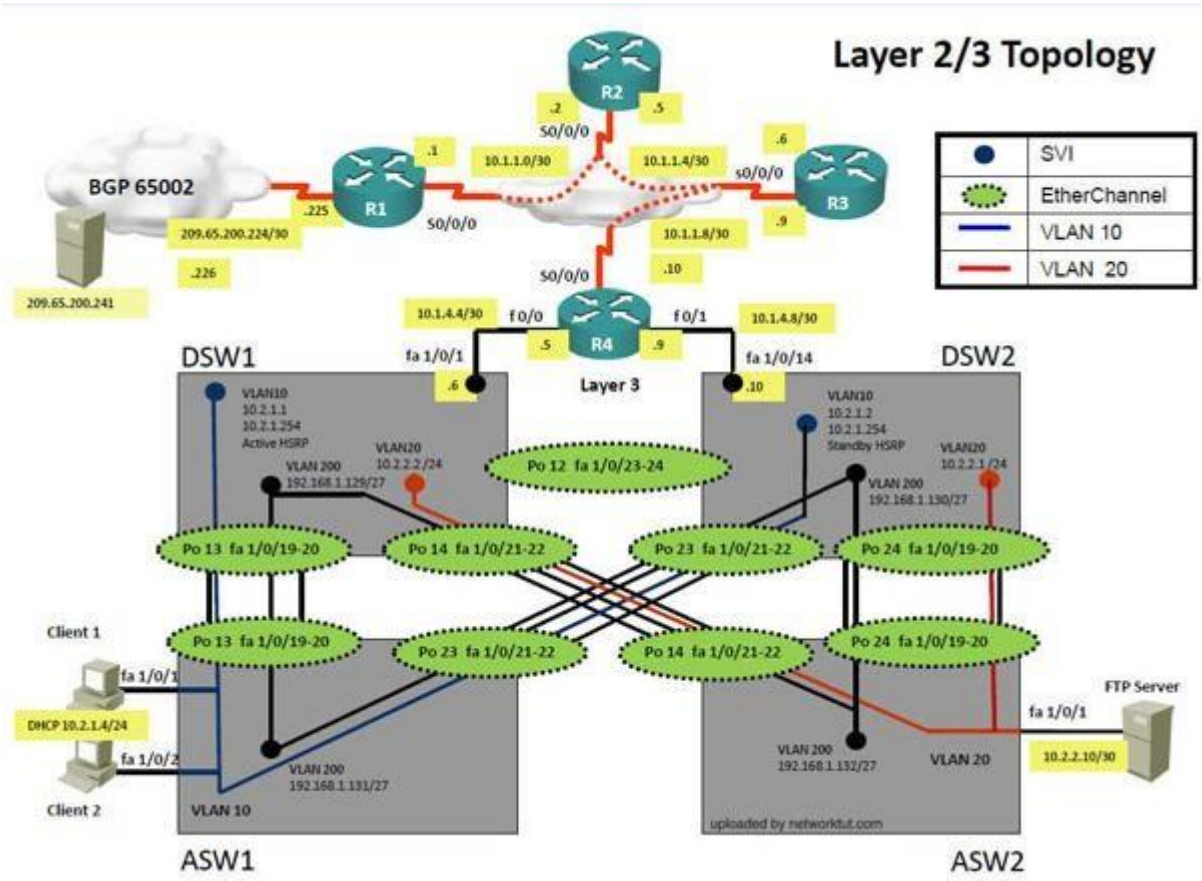
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

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

==========


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



Client 1 is unable to ping IP 209.65.200.241

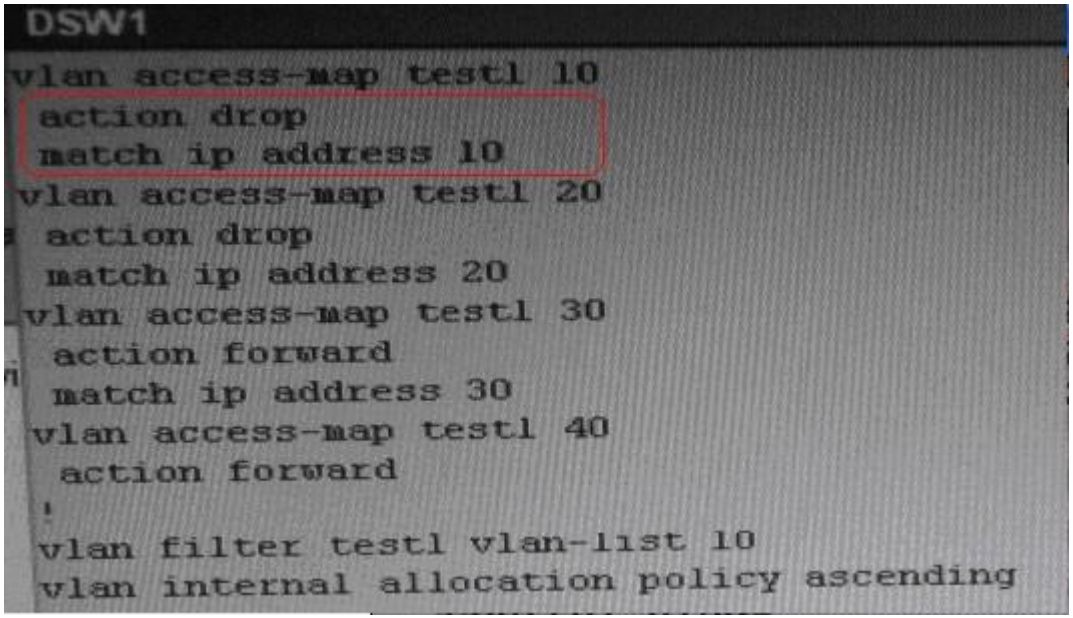
Solution

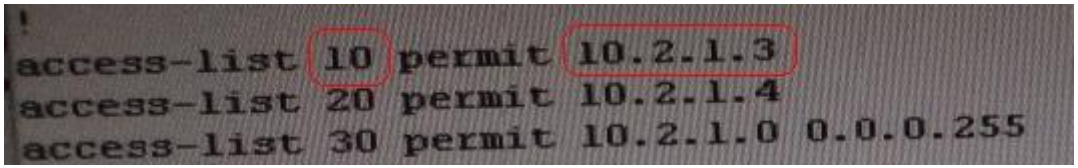
Steps need to follow as below:-

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





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

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 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 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. Redistrution is enabled where necessary.

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

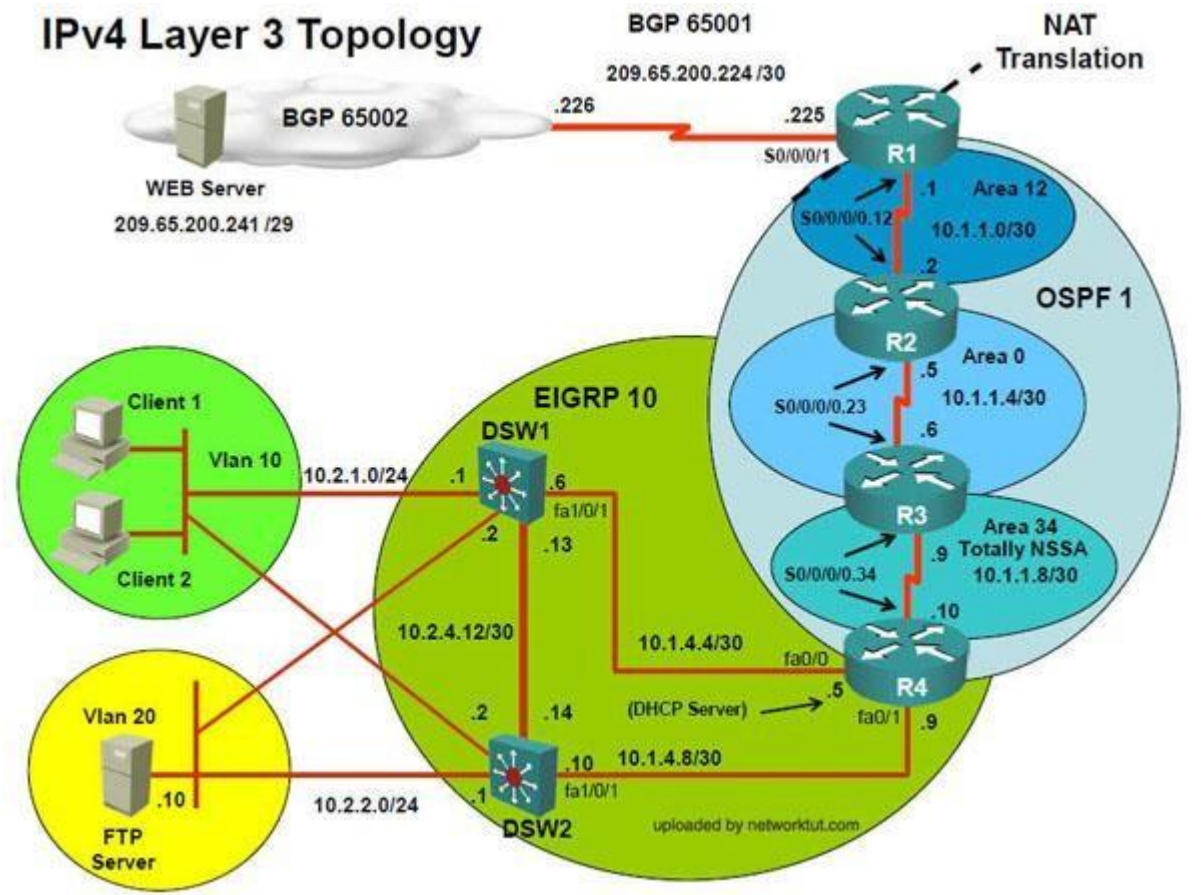
Each ticket has 3 sub questions that need to be answered & topology remains same.

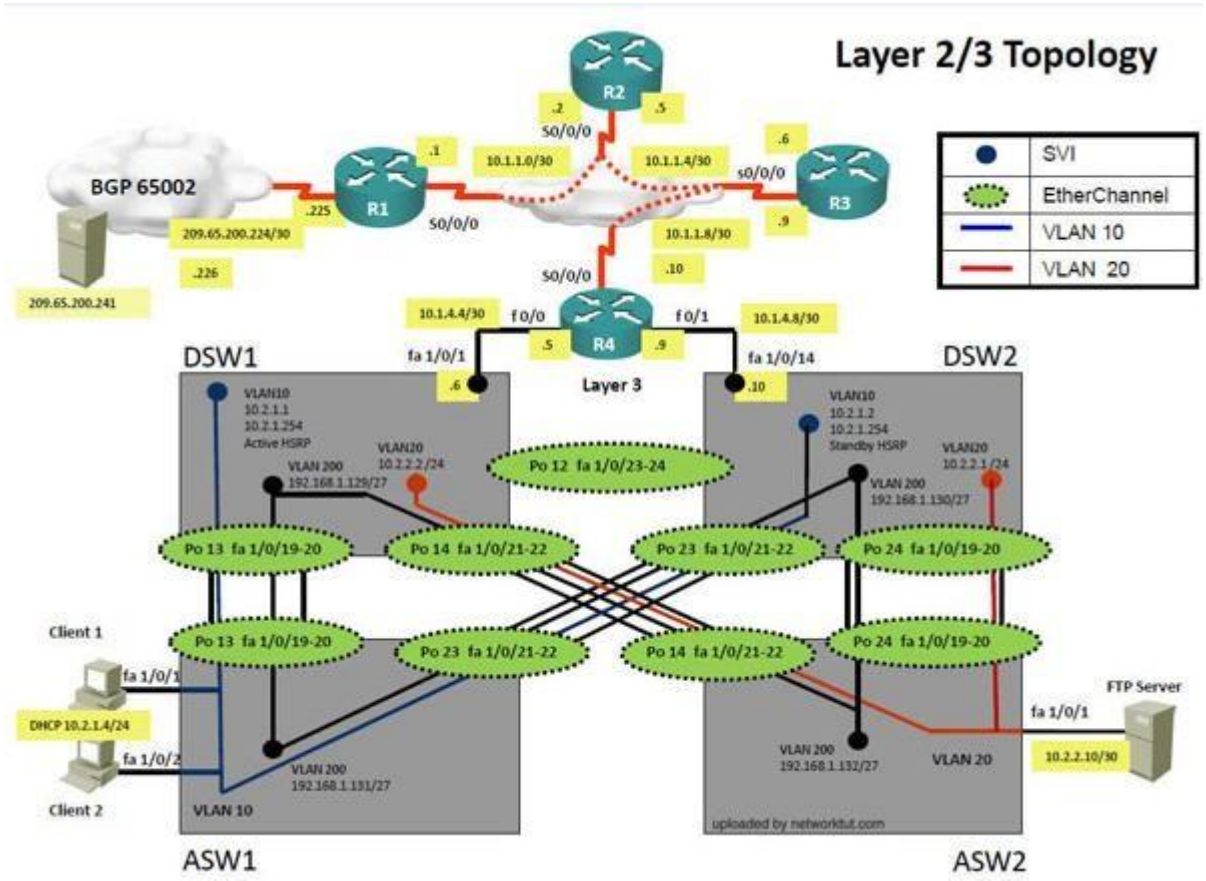
Question-1 Fault is found on which device,

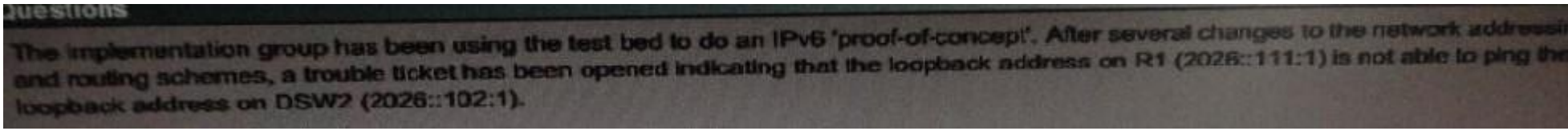
Question-2 Fault condition is related to,

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

==========


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





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

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

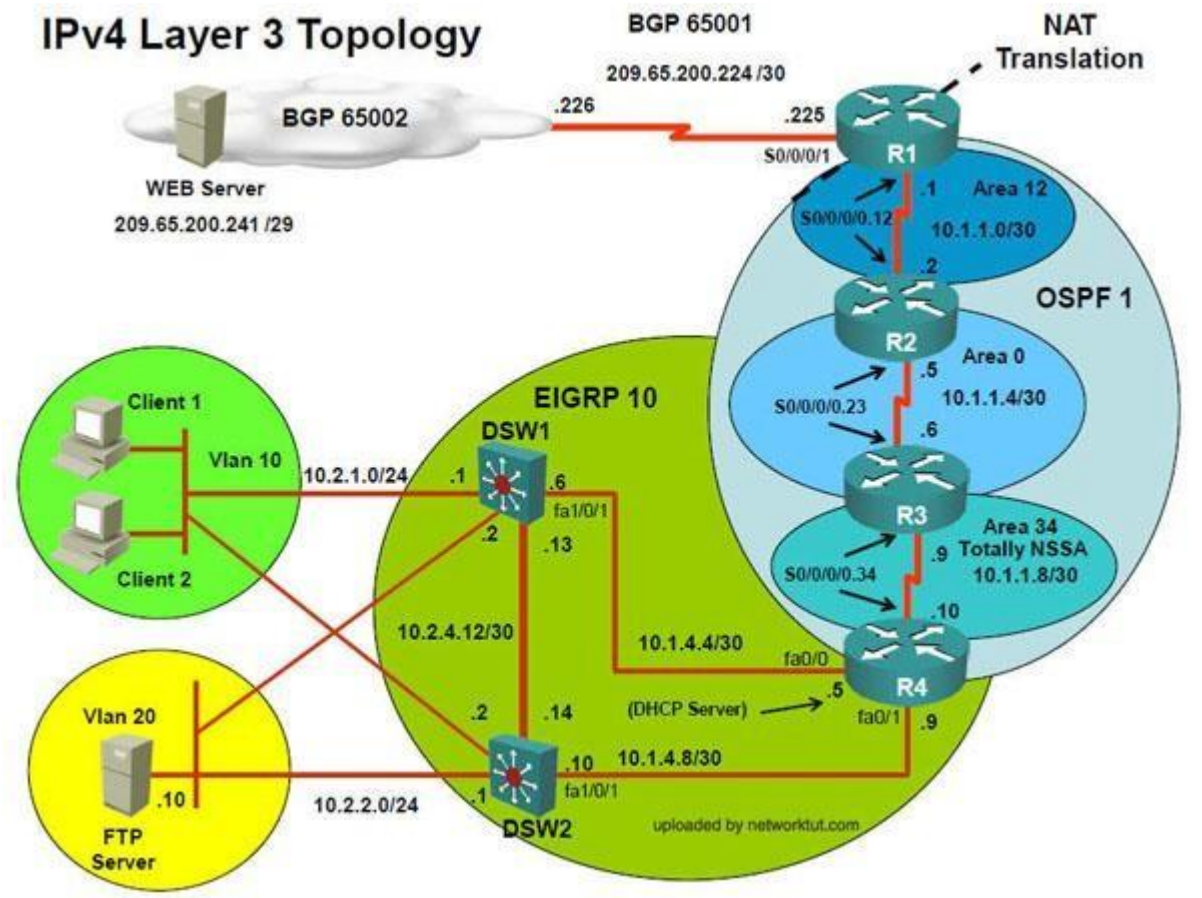
Each ticket has 3 sub questions that need to be answered & topology remains same.

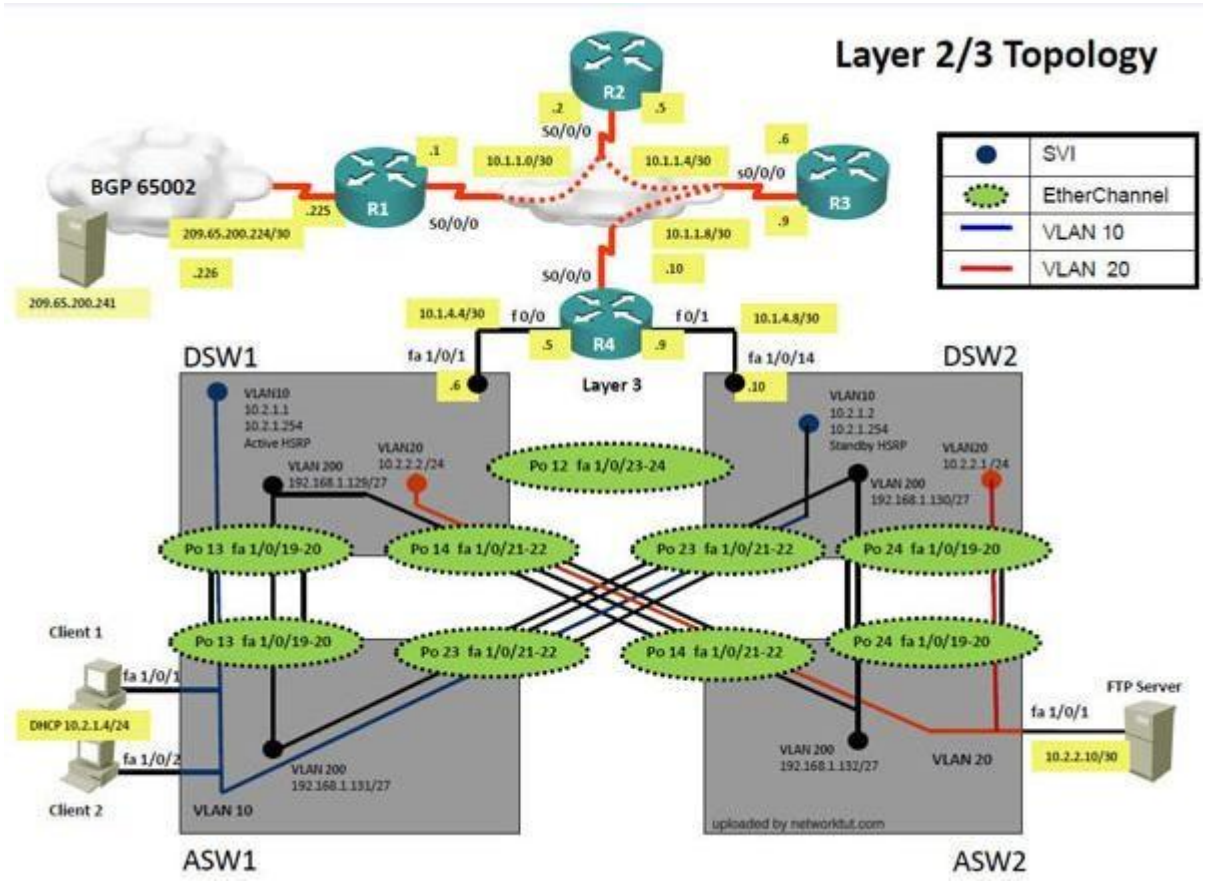
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

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

==========





The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the W 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
```

```
!
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 Vlans

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
HSRP is running between DSW1 & DSW2 Switches

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

This network consists of four routers, two layer 3 switches and two layer 2 switches. In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.

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

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

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

ASW1 and ASW2 are layer 2 switches.

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

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

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

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

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

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

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

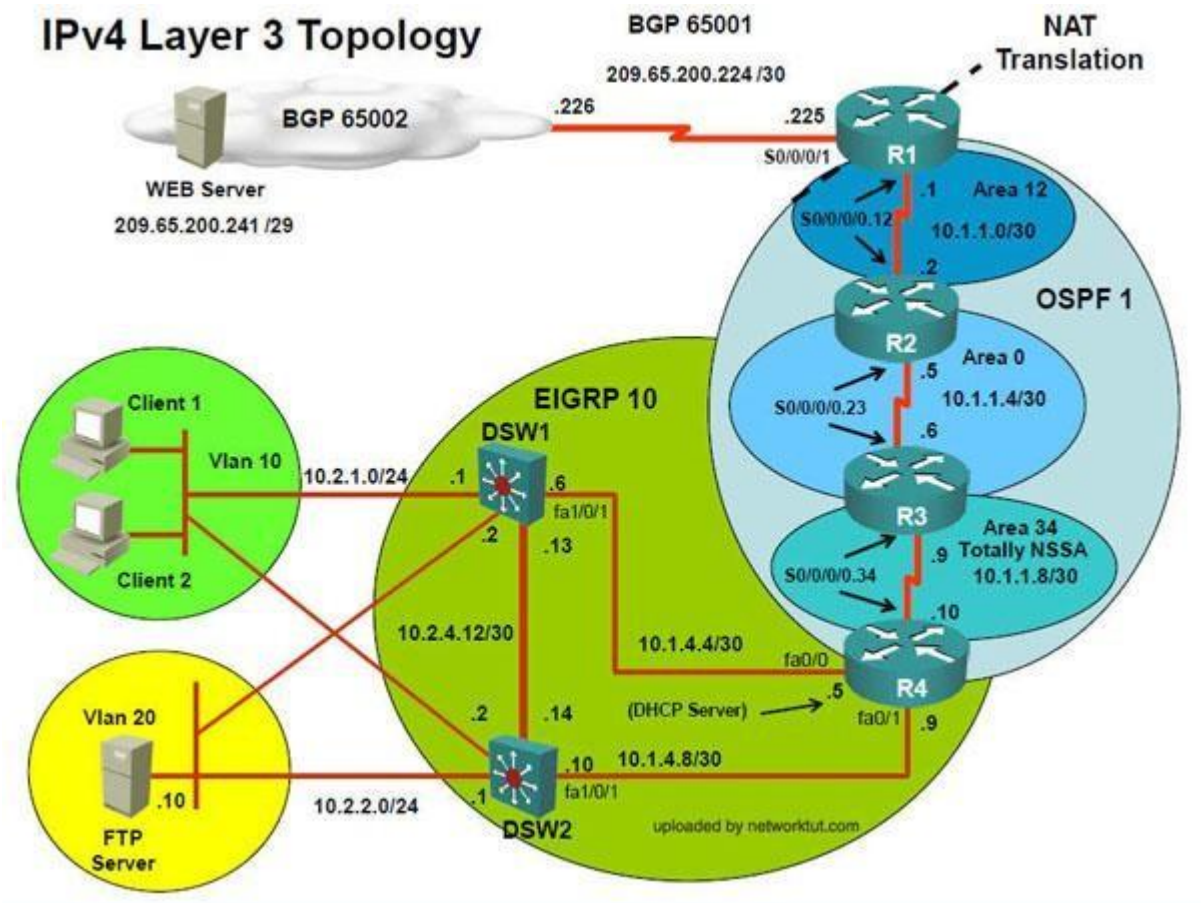
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

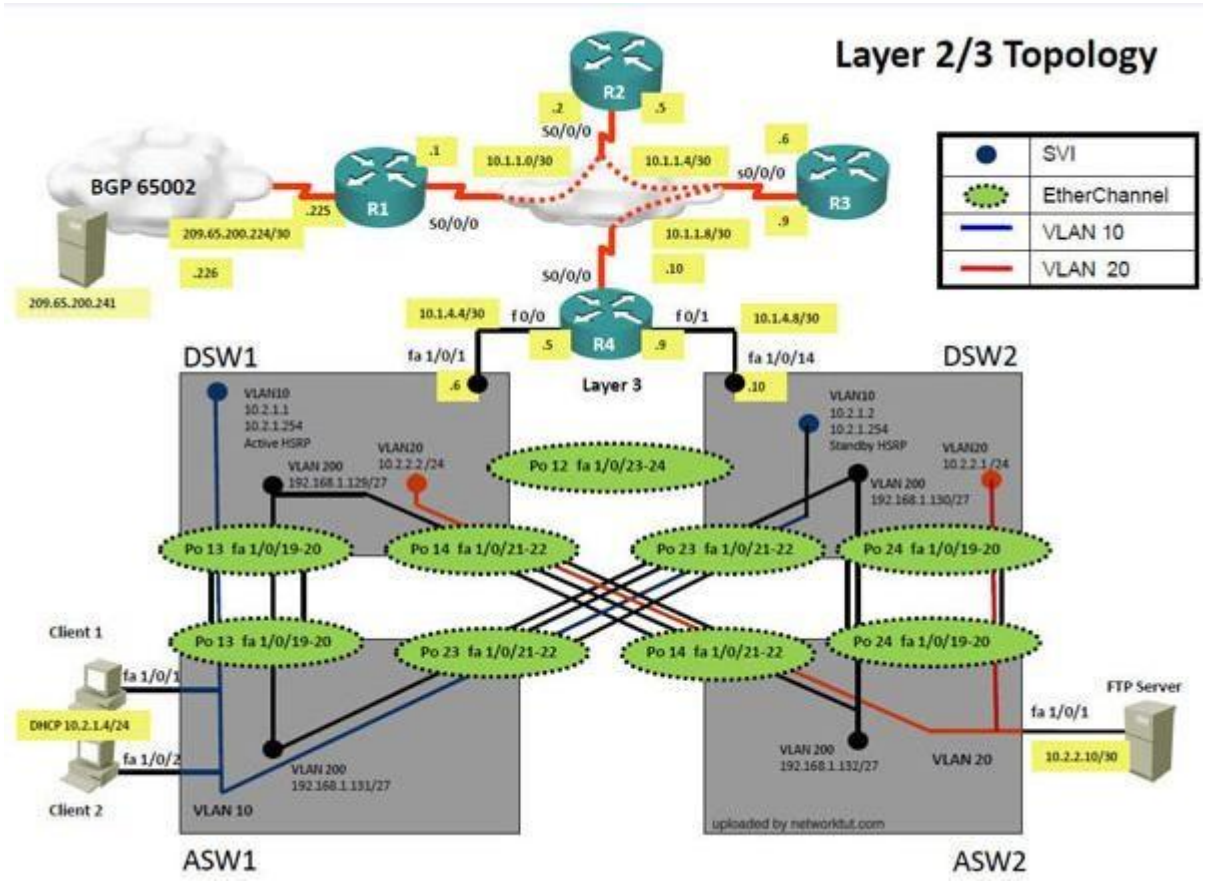
Each ticket has 3 sub questions that need to be answered & topology remains same.

Question-1 Fault is found on which device,
Question-2 Fault condition is related to,

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

==========





The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the W 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:
LevelLevel NameDescription
0 Emergencies System is unusable
1 Alerts Immediate action needed
2 Critical Critical conditions
3 Errors Error conditions
4 Warnings Warning conditions
5 Notifications Informational messages
6 Informational Normal but significant conditions
7 Debugging Debugging messages

When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case we can see that logging level of 3 (as seen by the 3 in “LINK-3-UPDOWN”) and level 5 (as seen by the 5 in “LINEPROTO-5-UPDOWN”) are shown, which means that logging level 5 must have been configured. As shown by the table, logging level 5 is Notifications.

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 a 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

QUESTION 66
Refer to the configuration statements shown in the graphic above.

R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1 R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1 R1(config)#end R1#debug ip packet 199 detail

Which statement reflects what the effect is of this configuration sequence?

A. These commands will generate an error message because you cannot use an access list with any debug commands.
B. These commands will have no effect at all. The debug ip packet command will work as normal and display info for all IP packets.
C. These commands turn on debug ip packet only for packets between hosts 10.1.1.1 and 172.16.1.1.
D. These commands will only work when you specify only one host rather than two.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
What is the result if you configure two devices with the ntp server command?

A. Nothing will happen until one of the devices is configured with the prefer parameter.
B. The NTP protocol will determine which server is most reliable and will synchronize to that server.
C. The device with the highest priority will become the active server and the other device will become the backup server.
D. The device with the lowest MAC address will become the active server and the other device will become the backup server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
A technician is troubleshooting connectivity problems between two routers that are directly connected through a serial line. The technician notices that the serial line is up, but cannot see any neighbors displayed in the output of the show cdp neighbors command.

In which OSI layer is the problem most likely occurring?

A. physical
B. data link
C. network
D. transport
E. application

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
What are two approaches to maintaining a network?(Choose two.)

A. PPDIOO
B. structured
C. bottoms up
D. interrupt-driven

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Which two statements about the Cisco Aironet Desktop Utility (ADU) are true? (Select two)

A. The Aironet Desktop Utility (ADU) profile manager feature can create and manage only one profile for the wireless client adapter.
B. The Aironet Desktop Utility (ADU) can support only one wireless client adapter installed and used at a time.
C. The Aironet Desktop Utility (ADU) can be used to establish the association between the client adapter and the access point, manage authentication to the wireless network, and enable encryption.
D. The Aironet Desktop Utility (ADU) and the Microsoft Wireless Configuration Manager can be used at the same time to configure the wireless client adapter.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You can configure your Cisco Aironet Wireless LAN Client Adapter through the Cisco ADU or a third-party tool, such as the Microsoft Wireless Configuration Manager. Because third-party tools may not provide all the functionality available in ADU, Cisco recommends that you use ADU.
The Aironet Desktop Utility (ADU) can support only one wireless client adapter as well as Aironet Desktop Utility establish the association between the client adapter and Access Point, allows to authenticate wireless client, allows to configure encryption by setting static WEP, WPA/WPA2 passphrase.

QUESTION 71
At which layer of the OSI model does the Spanning Tree Protocol (STP) operate at?

A. Layer 5
B. Layer 4
C. Layer 3
D. Layer 2
E. Layer 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Spanning-Tree Protocol (STP) is a Layer 2 (L2) protocol designed to run on bridges and switches. The specification for STP is called 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. Loops are deadly to a network.

QUESTION 72
In computer networking a multicast address is an identifier for a group of hosts that have joined a multicast group. Multicast addressing can be used in the Link Layer (OSI Layer 2), such as Ethernet Multicast, as well as at the Internet Layer (OSI Layer 3) as IPv4 or IPv6 Multicast. Which two descriptions are correct regarding multicast addressing?

A. The first 23 bits of the multicast MAC address are 0x01-00-5E. This is a reserved value that indicates a multicast application.
B. The last 3 bytes (24 bits) of the multicast MAC address are 0x01-00-5E. This is a reserved value that indicates a multicast application.
C. To calculate the Layer 2 multicast address, the host maps the last 23 bits of the IP address into the last 24 bits of the MAC address. The high-order bit is set to 0.
D. The first 3 bytes (24 bits) of the multicast MAC address are 0x01-00-5E. This is a reserved value that indicates a multicast application.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The point of this question is the form of multicast MAC address, and the conversion between the multicast MAC address and IP address.
The multicast MAC address is 6 bytes(48 bits), the first 3 bytes (24 bits) of the multicast MAC address are 0x01-00-5E, the last 3 bytes(24 bits) of the multicast MAC address =0 + 23 bit(the last 23 bit of the IP address). "0x01-00-5E" is a reserved value that indicates a multicast application.

QUESTION 73
EIGRP is being used as the routing protocol on the Company network. While troubleshooting some network connectivity issues, you notice a large number of EIGRP SIA (Stuck in Active) messages. What causes these SIA routes? (Select two)

A. The neighboring router stops receiving ACK packets from this router.
B. The neighboring router starts receiving route updates from this router.
C. The neighboring router is too busy to answer the query (generally caused by high CPU utilization).
D. The neighboring router is having memory problems and cannot allocate the memory to process the query or build the reply packet.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

SIA routes are due to the fact that reply packets are not received. This could be caused by a router which is unable to send reply packets. The router could have reached the limit of its capacity, or it could be malfunctioning.
Incorrect Answers
A:Missing replies, not missing ACKs, cause SIA.
B:Routes updates do not cause SIA.
Notes: If a router does not receive a reply to all outstanding queries within 3 minutes, the route goes to the stuck in active (SIA) state. The router then resets the neighbors that fail to reply by going active on all routes known through that neighbor, and it re-advertises all routes to that neighbor.
References:

QUESTION 74
You want to enhance the security within the Company LAN and prevent VLAN hopping. What two steps can be taken to help prevent this? (Select two)

A. Enable BPD guard
B. Disable CDP on ports where it is not necessary
C. Place unused ports in a common unrouted VLAN
D. Prevent automatic trunk configuration
E. Implement port security

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To prevent VLAN hoping you should disable unused ports and put them in an unused VLAN, or a separate unrouted VLAN. By not granting connectivity or by placing a device into a VLAN not in use, unauthorized access can be thwarted through fundamental physical and logical barriers. Another method used to prevent VLAN hopping is to prevent automatic trunk configuration. Hackers used 802.1Q and ISL tagging attacks, which are malicious schemes

that allow a user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port.
References:

QUESTION 75
The Company network is being flooded with invalid Layer 2 addresses, causing switch CAM tables to be filled and forcing unicast traffic to be transmitted out all switch ports. Which type of Layer 2 attack is being used here?

A. MAC spoofing
B. VLAN hopping
C. MAC address flooding
D. DHCP flooding
E. Session hijacking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Port security is especially useful in the face of MAC address flooding attacks. In these attacks, an attacker tries to fill up a switch's CAM tables by sending a large number of frames to it with source MAC addresses that the switch is unaware of at that time. The switch learns about these MAC addresses and puts them in its CAM table, thinking that these MAC addresses actually exist on the port on which it is receiving them. In reality, this port is under the attacker's control and a machine connected to this port is being used to send frames with spoofed MAC addresses to the switch. If the attacker keeps sending these frames in a large-enough quantity, and the switch continues to learn of them, eventually the switch's CAM table becomes filled with entries for these bogus MAC addresses mapped to the compromised port. Under normal operations, when a machine receiving a frame responds to it, the switch learns that the MAC address associated with that machine sits on the port on which it has received the response frame. It puts this mapping in its CAM table, allowing it to send any future frames destined for this MAC address directly to this port rather than flood all the ports on the VLAN. However, in a situation where the CAM table is filled up, the switch is unable to create this CAM entry. At this point, when the switch receives a legitimate frame for which it does not know which port to forward the frame to, the switch floods all the connected ports belonging to the VLAN on which it has received the frame. The switch continues to flood the frames with destination addresses that do not have an entry in the CAM tables to all the ports on the VLAN associated with the port it is receiving the frame on.
References:

QUESTION 76
A MAC address flood attack is occurring on the Company LAN. During this attack, numerous frames are forwarded to a switch which causes the CAM table to fill to capacity. How does this action benefit the attacker?

A. All traffic is tagged with a specific VLAN ID from the VLAN of the attacker and is now viewable.
B. Clients will forward packets to the attacking device, which will in turn send them to the desired destination but not before recording the traffic

patterns.

C. All traffic is redirected to the VLAN that the attacker used to flood the CAM table.
D. All traffic is flooded out all ports and an attacker is able to capture all data.
E. None of the other alternatives apply

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
MAC flooding basically involves bombarding the switch with spoofed ARP requests in the hope of making the switch "fail open". This, in essence, makes the switch display the characteristics of a hub, where it sends packets to all ports. A MAC flooding attack looks like traffic from thousands or computers moving into one port, but it's actually the attacker spoofing the MAC address of thousands of non-existent hosts. The goal is to flood the switches CAM (content addressable memory) table, or port/MAC table with these bogus requests, and once flooded, the switch will broadcast openly onto a LAN, allowing the attacker to start sniffing. The success of this attack is almost completely dependant on the model and manufacturer of the switch.
References:

QUESTION 77
Which of the following characteristics describe the BPDU Guard feature? (Choose all that apply.)

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

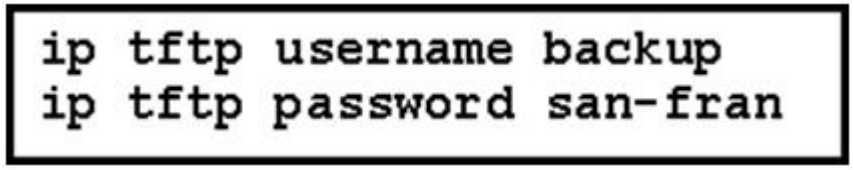
Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78
Refer to the graphic above.

Which command sequences, shown below, would accomplish the same task as that shown in the graphic?

A.


B.


C.


D.


Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following are valid modes of accessing the data plane? (Choose all that apply.)

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

Correct Answer: ABDEF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 80
You have 2 NTP servers in your network - 10.1.1.1 and 10.1.1.2. You want to configure a Cisco router to use 10.1.1.2 as its NTP server before falling back to 10.1.1.1. Which commands will you use to configure the router?

A. ntp server 10.1.1.1ntp server 10.1.1.2
B. ntp server 10.1.1.1ntp server 10.1.1.2 primary
C. ntp server 10.1.1.1ntp server 10.1.1.2 prefer
D. ntp server 10.1.1.1 fallbackntp server 10.1.1.2

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Preferred server
A router can be configured to prefer an NTP source over another. A preferred server's responses are discarded only if they vary dramatically from the other time sources. Otherwise, the preferred server is used for synchronization without consideration of the other time sources. Preferred servers are usually specified when they are known to be extremely accurate. To specify a preferred server, use the prefer keyword appended to the ntp server command. The following example tells the router to prefer TimeServerOne over TimeServerTwo:
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server TimeServerOne prefer
Router(config)#ntp server TimeServerTwo
Router(config)#^Z

QUESTION 81
The following command is issued on a Cisco Router:

Router(configuration)#logging console warnings

Which alerts will be seen on the console?

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

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Cisco routers prioritize log messages into 8 levels (0-7), as shown below:
LevelLevel NameDescription
0 Emergencies System is unusable
1 Alerts Immediate action needed
2 Critical Critical conditions
3 Errors Error conditions
4 Warnings Warning conditions
5 Notifications Informational messages
6 Informational Normal but significant conditions
7 Debugging Debugging messages

When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case, when you enable console logging of warning messages (level 4), it will log levels 0-4, making the correct answer warnings, errors, critical, alerts, and emergencies.

QUESTION 82
FCAPS is a network maintenance model defined by ISO. It stands for which of the following ?

A. Fault Management
B. Action Management
C. Configuration Management

D. Protocol Management
E. Security Management

Correct Answer: ACE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The FCAPS maintenance model consists of the following:
FCAPS Maintenance Tasks:

QUESTION 83
Which three management categories are contained in the FCAPS network maintenance model? (Choose three.)

A. Config
B. Fault
C. Storage
D. Accounting
E. Redundancy
F. Telecommunications

Correct Answer: ABD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
What is the result of configuring the logging console warning command?

A. Messages with a severity level of 4 and higher will be logged to all available TTY lines.
B. Only warning messages will be logged on the console.
C. Warning, error, critical, and informational messages will be logged on the console.
D. Warning, critical, alert, and emergency messages will be logged on the console.
E. The logging console warning command needs to be followed in the configuration with logging buffered byte size to specify the message buffer size for the console.

Correct Answer: D

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
Which of the following is not an essential prerequisite for AutoQoS to be correctly applied to an interface? (Choose all that apply.)

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

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
Which of the following topology situations would be a qood candidate for configuring DMVPN?

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

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
Which of the following is not considered a common approach to narrow the field of potential problem causes? (Choose the best answer.)

A. Following the traffic path
B. Top-down
C. Comparing configurations
D. Bottom-up
E. Divide and conquer
F. Examine SLAs

Correct Answer: F
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
Which of the following best describes the following command: ip flow-export destination 192.168.1.50 1500?

A. it is not a valid NetFlow command.
B. it is an SNMP command that exports 1500-byte packets to IP address 192.168.1.50.
C. it is a NetFlov/ command that v/ill export 1500-byte packets to IP address 192.168.1.50.
D. it is a NetFlov/ command that allows IP address 192.168.1.50 to send traffic to port 1500.
E. It is a NetFlov/ command that v/ill specify that the NetFlov/ collector's IP address is 192.168.1.50 over UDP port 1500.
F. It is an SNMP command that exports flows to destination address 1Q2.168.1.50 for packets up to an MTU of 1500.

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
Which of the following are valid methods of providing a router with information concerning the location of the RP? (Choose all that apply.)

A. Statically defined RP
B. Bootstrap Router

C. Auto-RP
D. RP Discovery Protocol (RDP)
E. RP Helios
F. RPARP(RARP)

Correct Answer: ABC
Section: Mix Questions
Explanation

Explanation/Reference:
Topic 2, Drag Drop Questions

QUESTION 90
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: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
The implementations group has been using the test bed to do a ,,proof-of-concept that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing 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: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
The implementations group has been using the test bed to do a ,,proof-of-concept that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolate the cause of this fault and answer the following question.

What is the solution to the fault condition?

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

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

Explanation: