Cisco TSHOOT 300-135

Number: 300-135
Passing Score: 846
Time Limit: 160 min
File Version: 2015-07-21

Exam : Cisco TSHOOT 300-135

Version : 2015-07-21

Exam A: MCQ
Exam B: Ticket 1: Switch Port Trunk
Exam C: Ticket 2: Access VLAN
Exam D: Ticket 3: OSPF Authentication
Exam E: Ticket 4: BGP Neighbor
Exam F: Ticket 5: NAT ACL
Exam G: Ticket 6: ACL
Exam H: Ticket 7: Port Security
Exam I: Ticket 8: Redistribution of OSPF to EIGRP
Exam J: Ticket 9: VLAN Access Map
Exam K: Ticket 10: EIGRP AS number
Exam L: Ticket 11: HSRP Issue
Exam M: Ticket 12: DHCP Issue Topology Overview
Exam N: Ticket 13: EIGRP Passive Interface
Exam O: Ticket 14: IPv6 OSPF
Exam P: Ticket 15: IPv6 GRE Tunnel(IPv4 and IPv6 Interoperability)
Exam Q: Ticket 16: IPv6 RIPng OSPFv3 Redistrobution
Exam R: OSPF Sim
Exam S: HSRP Sim
Exam T: Switch Sim
Exam U: EIGRP Sim

Exam A

QUESTION 1
Exhibit:

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

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

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

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
From the last line “K-value mismatch” we learn that the K values of two EIGRP routers are mismatched and EIGRP neighborship between two routers will not be formed.
Note: EIGRP K values are the metrics that EIGRP uses to calculate routes. Mismatched K values can prevent neighbor relationships from being established. By default K1 & K3 are set to 1 while K2, K4 and K5 are set to 0. We can change the EIGRP K values via the “**metric weights** *tos k1 k2 k3 k4 k5*” command under EIGRP router mode (tos: type of service must always be zero). For example:
Router(config-router)#metric weights 0 20 10 50 40 40

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: (none)
Explanation

Explanation/Reference:
The following list of parameters must match between EIGRP neighbors in order to successfully establish neighbor relationships:
+ Autonomous System number.
+ K-Values (look at the previous lesson).
+ If authentication is used both: the key number, the password, and the date/time the password is valid must match.
+ The neighbors must be on common subnet (all IGPs follow this rule).
Therefore we don't need to check EIGRP hello and hold timers because they don't have to match. We should check if appropriate networks are included in the "network …" command of EIGRP on both routers.

QUESTION 3

Refer to the exhibit.

```
R1#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,

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 direct1v 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
```

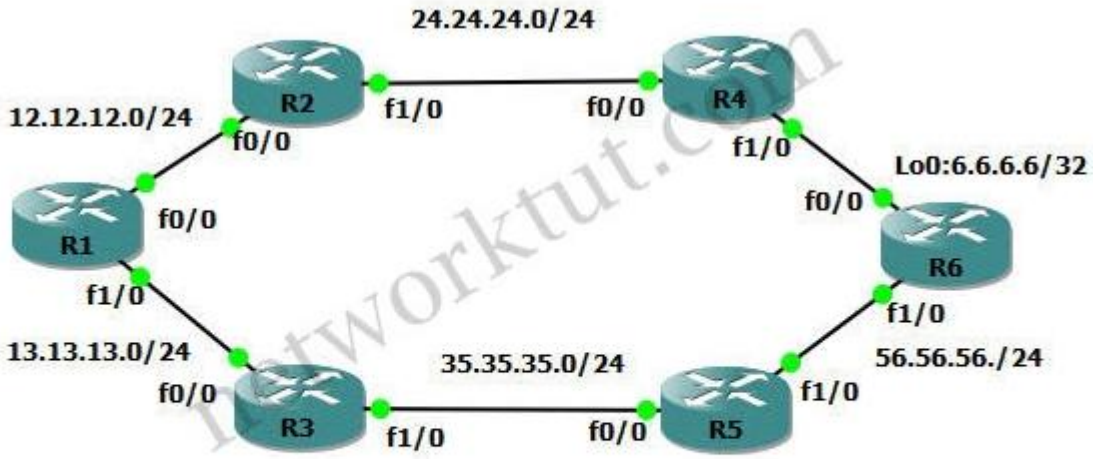
How would you confirm on R1 that load balancing is actually occurring on the default-network (0.0.0.0)?

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: (none)
Explanation

Explanation/Reference:

For example in the topology below, R1 learned the Loopback0 interface of R6 via two equal paths R2-R4 and R3-R5:



The routing table of R1 is shown below:

```
R1#show ip route
<output omitted>
O     6.6.6.6 [110/4] via 13.13.13.3, 00:06:53, FastEthernet1/0
            [110/4] via 12.12.12.2, 00:06:53, FastEthernet0/0
```

And the traceroute command from R1 to R6's loopback0:

```
R1#traceroute 6.6.6.6

Type escape sequence to abort.
Tracing the route to 6.6.6.6

 1 12.12.12.2 36 msec
   13.13.13.3 36 msec
   12.12.12.2 20 msec
 2 35.35.35.5 40 msec
   24.24.24.4 44 msec
   35.35.35.5 40 msec
 3 46.46.46.6 60 msec
```

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: (none)
Explanation

Explanation/Reference:
IPSec transport mode (encrypting an IP GRE tunnel) is a commonly deployed option because it provides all the advantages of using IP GRE, such as IP Multicast protocol support (and, thus, also the support of routing protocols that utilize IP Multicast) and multiprotocol support. Furthermore, this option saves 20 bytes per packet over IPSec tunnel mode (encrypting an IP GRE tunnel) because an additional IP header is not required.
Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/IPSecQoS.html#pgfId-56035

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: (none)
Explanation

Explanation/Reference:
IPSec alone does not support multicast which many dynamic routing protocols use. GRE tunnels helps IPSec overcome this disadvantage by handling the transportation of multiprotocol and IP multicast traffic (from site-to-site VPNs, for example).

With the p2p GRE over IPsec solution, all traffic between sites is encapsulated in a p2p GRE packet before the encryption process, simplifying the access control list used in the crypto map statements. The crypto map statements need only one line permitting GRE (IP Protocol 47).
Reference:
http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE_IPSec/2_p2pGRE_Phase2

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: (none)
Explanation

Explanation/Reference:
With the p2p GRE over IPsec solution, all traffic between sites is encapsulated in a p2p GRE packet before the encryption process, simplifying the access control list used in the crypto map statements.
Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE_IPSec/2_p2pGRE_Phase2.html

Exam B

QUESTION 1
(Ticket 1: Switch Port Trunk)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

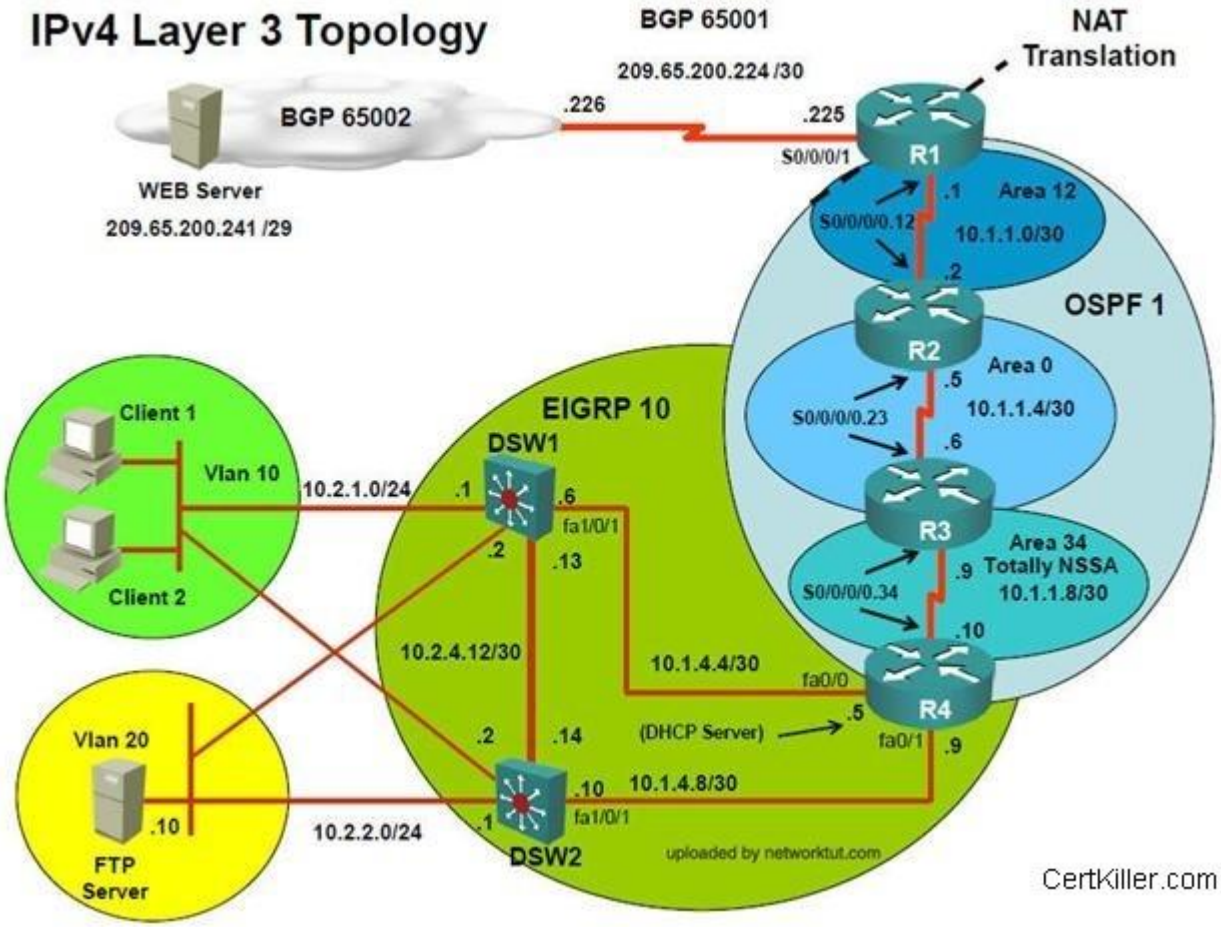


Figure 1

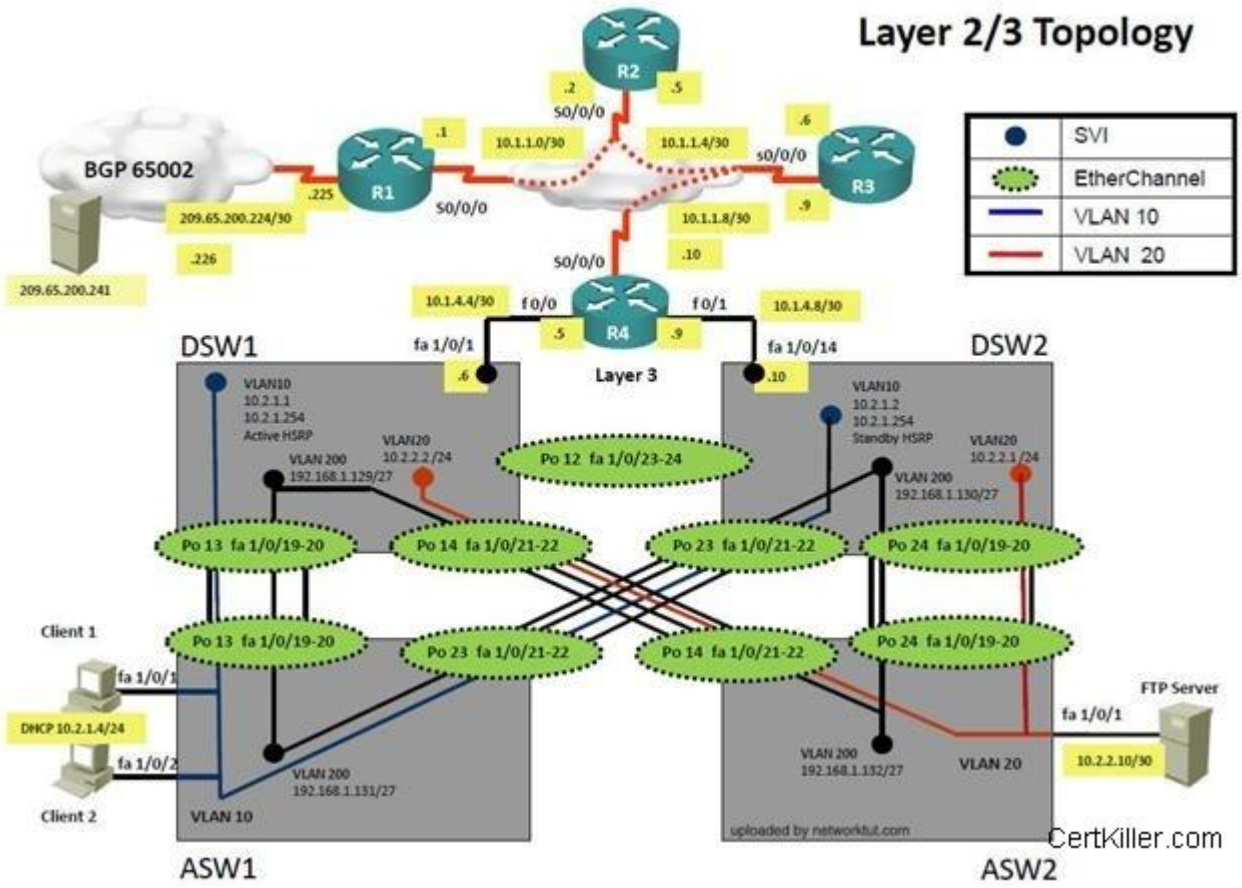


Figure 2

Trouble Ticket Statement

Client 1 and Client 2 are getting a 169.x.x.x IP address and are not able to ping DSW1 or the FTP Server. They are able to ping each other.

Configuration on ASW1

Interface PortChannel13
switchport mode trunk
switchport trunk allowed vlan 20,200
!

```
Interface PortChannel23
switchport mode trunk
switchport trunk allowed vlan 20,200
!
Interface FastEthernet1/0/1
switchport mode access
switchport access vlan 10
!
Interface FastEthernet1/0/2
switchport mode access
switchport access vlan 10
!
```

On Which device is the fault condition located?

A. ASW1
B. DSW1
C. Client 1
D. FTP Server
E. ASW2
F. DSW2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: ASW1

QUESTION 2
(Ticket 1: Switch Port Trunk)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

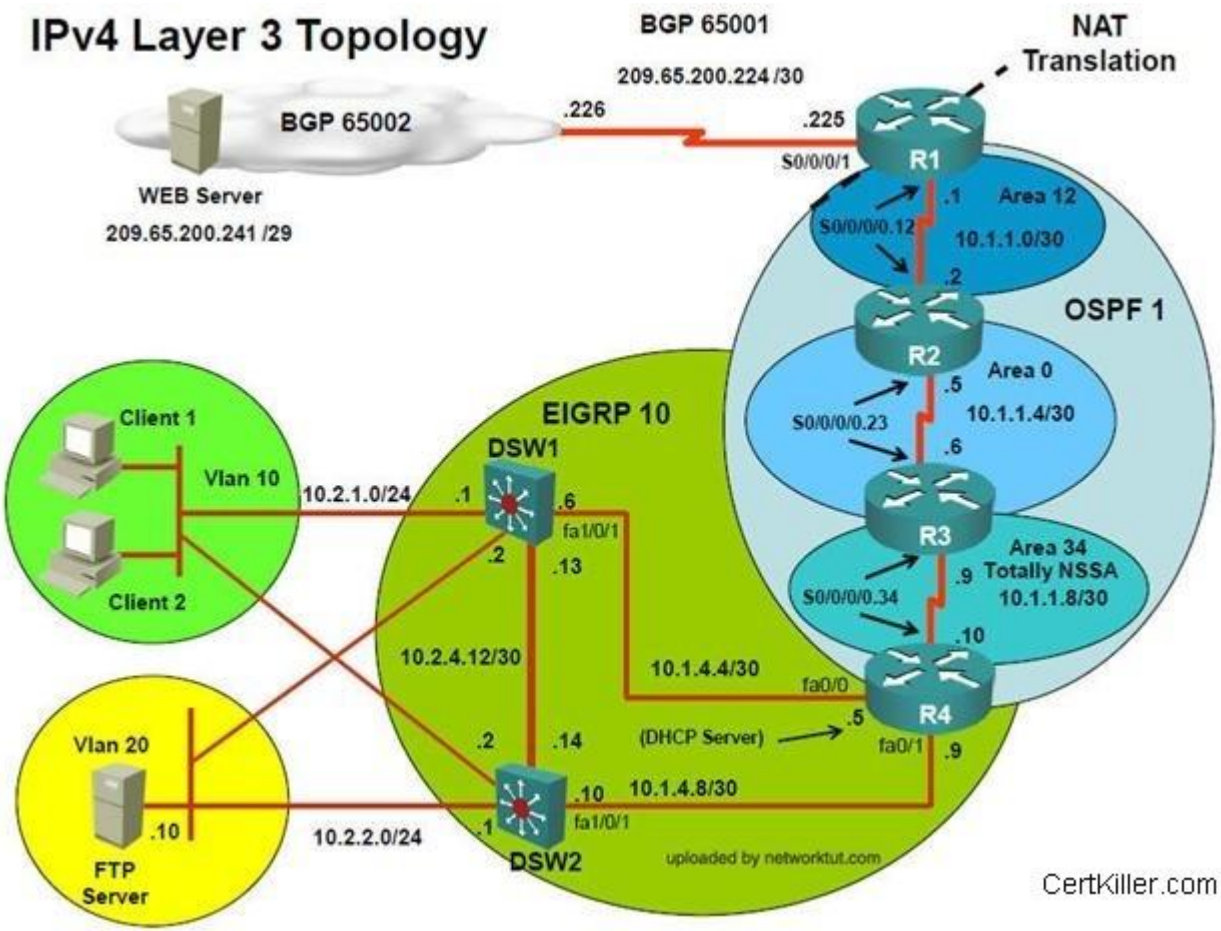


Figure 1

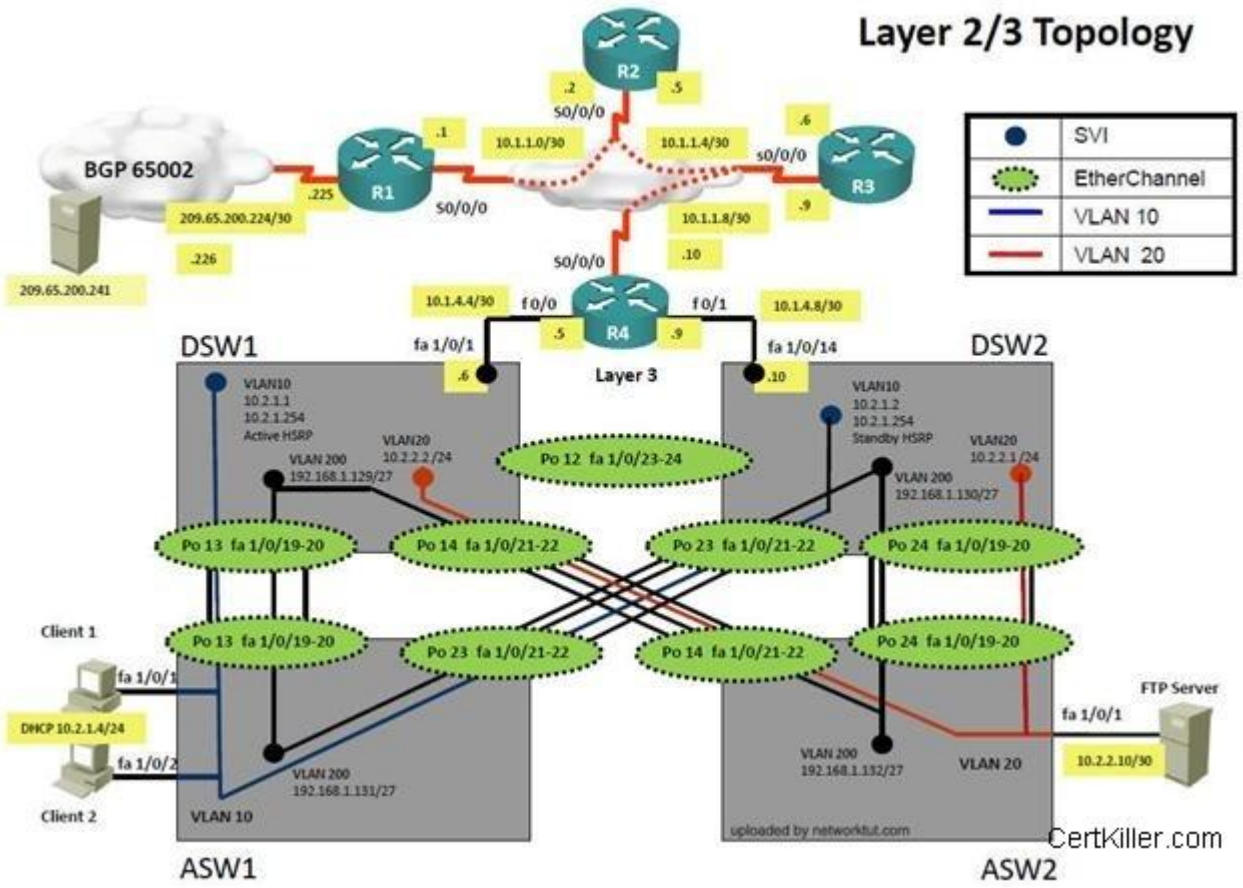


Figure 2

Trouble Ticket Statement

Configurationon ASW1

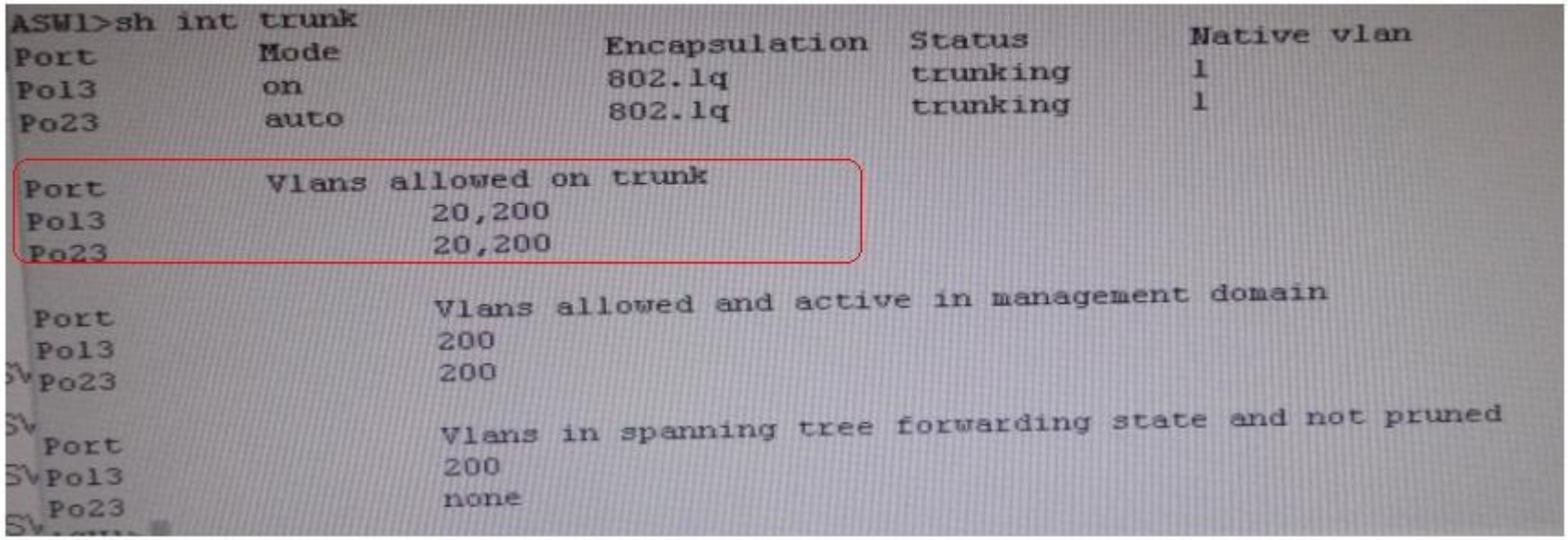
Sh run ------- & check for running config of int fa1/0/1 & fa1/0/2

==========

interface FastEthernet1/0/1switchport mode accessswitchport access vlan 10interface FastEthernet1/0/2switchport mode accessswitchport access vlan 10

==========

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



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: (none)
Explanation

Explanation/Reference:
Answer:
Switch to Switch Connectivity

QUESTION 3
(Ticket 1: Switch Port Trunk)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

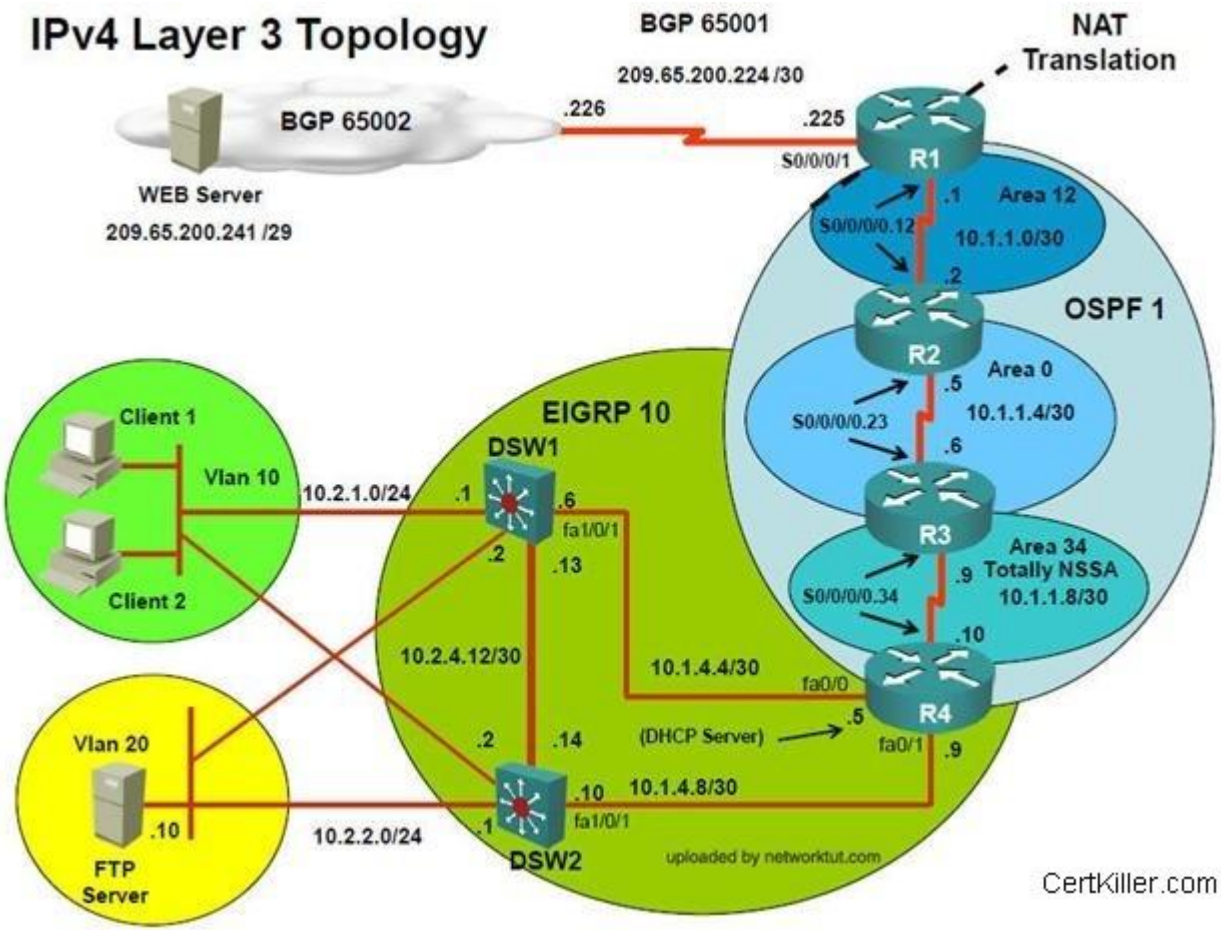


Figure 1

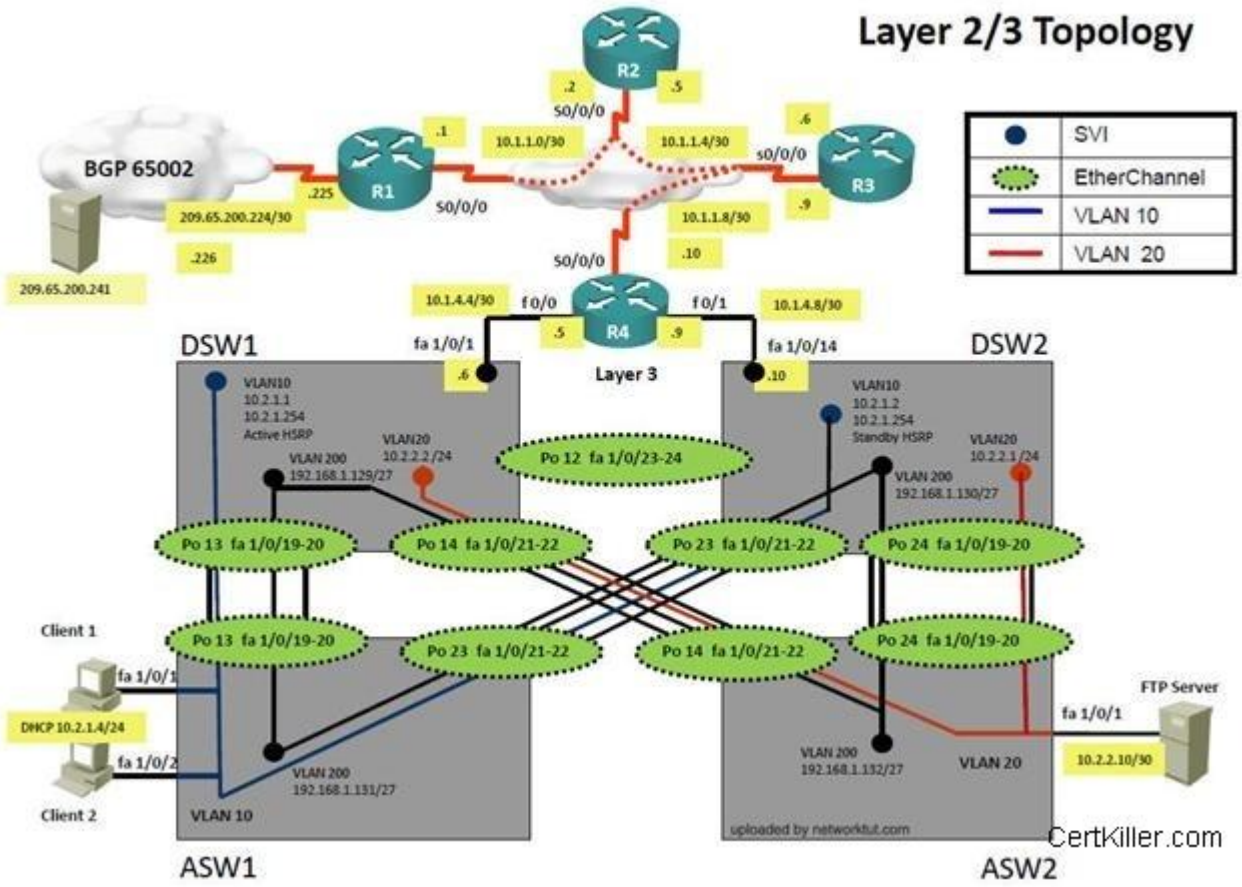


Figure 2

Trouble Ticket Statement

Client 1 and Client 2 are getting a 169.x.x.x IP address and are not able to ping DSW1 or the FTP Server. They are able to ping each other.

Configuration on ASW1

Interface PortChannel13
switchport mode trunk

```
switchport trunk allowed vlan 20,200
!
Interface PortChannel23
switchport mode trunk
switchport trunk allowed vlan 20,200
!
Interface FastEthernet1/0/1
switchport mode access
switchport access vlan 10
!
Interface FastEthernet1/0/2
switchport mode access
switchport access vlan 10
!
```

What is the solution of the fault condition?

A. Change the VLAN assignment on fa1/0/1 and fa1/0/2 on ASW1 to VLAN 1
B. Change the IP Address of VLAN 10 on DSW1
C. In Configuration mode, on interface portchannel13 and portchanngel23 then switchport trunk allowed vlan none, switchport trunk allowed vlan 10,200 command on ASW1
D. In Configuration mode, on interface portchannel13 and portchanngel23 then switchport trunk allowed vlan none on ASW1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: In Configuration mode, on interface portchannel13 and portchanngel23 then switchport trunk allowed vlan none, switchport trunk allowed vlan 10,200 command on ASW1

Exam C

QUESTION 1
(Ticket 2: Access VLAN)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

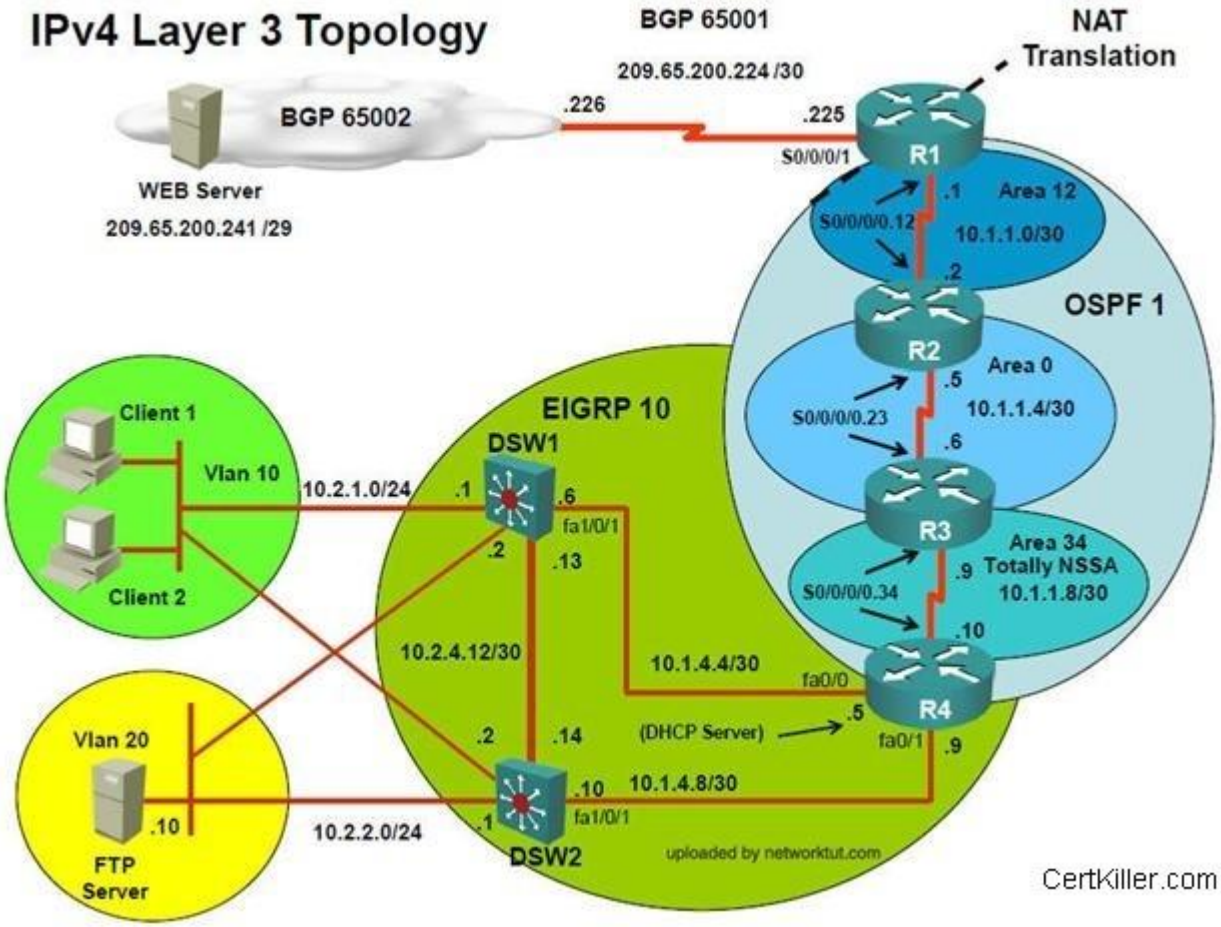


Figure 1

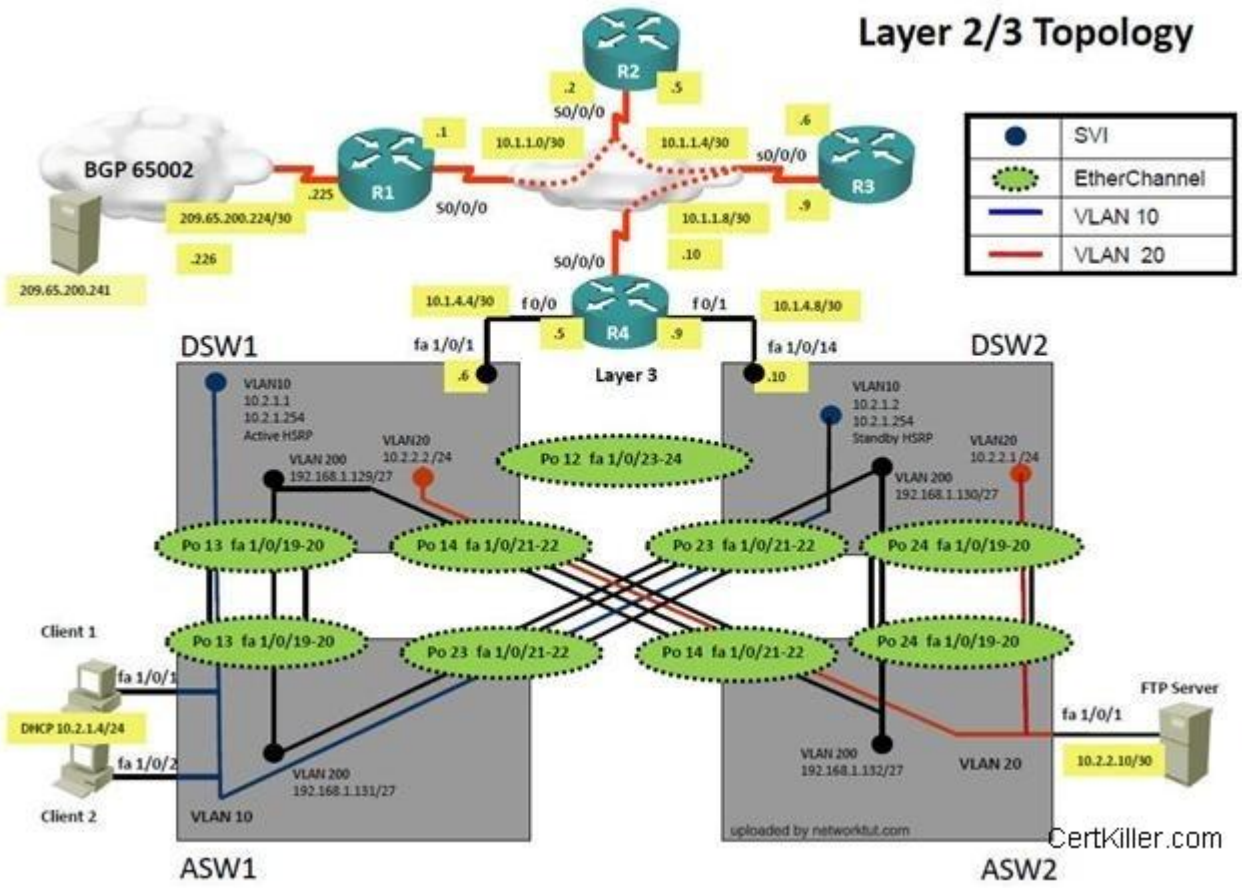


Figure 2

Trouble Ticket Statement

Client 1 and Client 2 are getting a 169.x.x.x IP address and are not able to ping DSW1 or the FTP Server. They are able to ping each other.

Configuration on ASW1

Interface FastEthernet1/0/1
switchport mode access
switchport access vlan 1
!
Interface FastEthernet1/0/2

switchport mode access
switchport access vlan 1

On which device is the fault condition located?

A. DSW1
B. ASW1
C. Client 1
D. FTP Server
E. DSW2
F. ASW2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: ASW1

QUESTION 2
(Ticket 2: Access VLAN)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

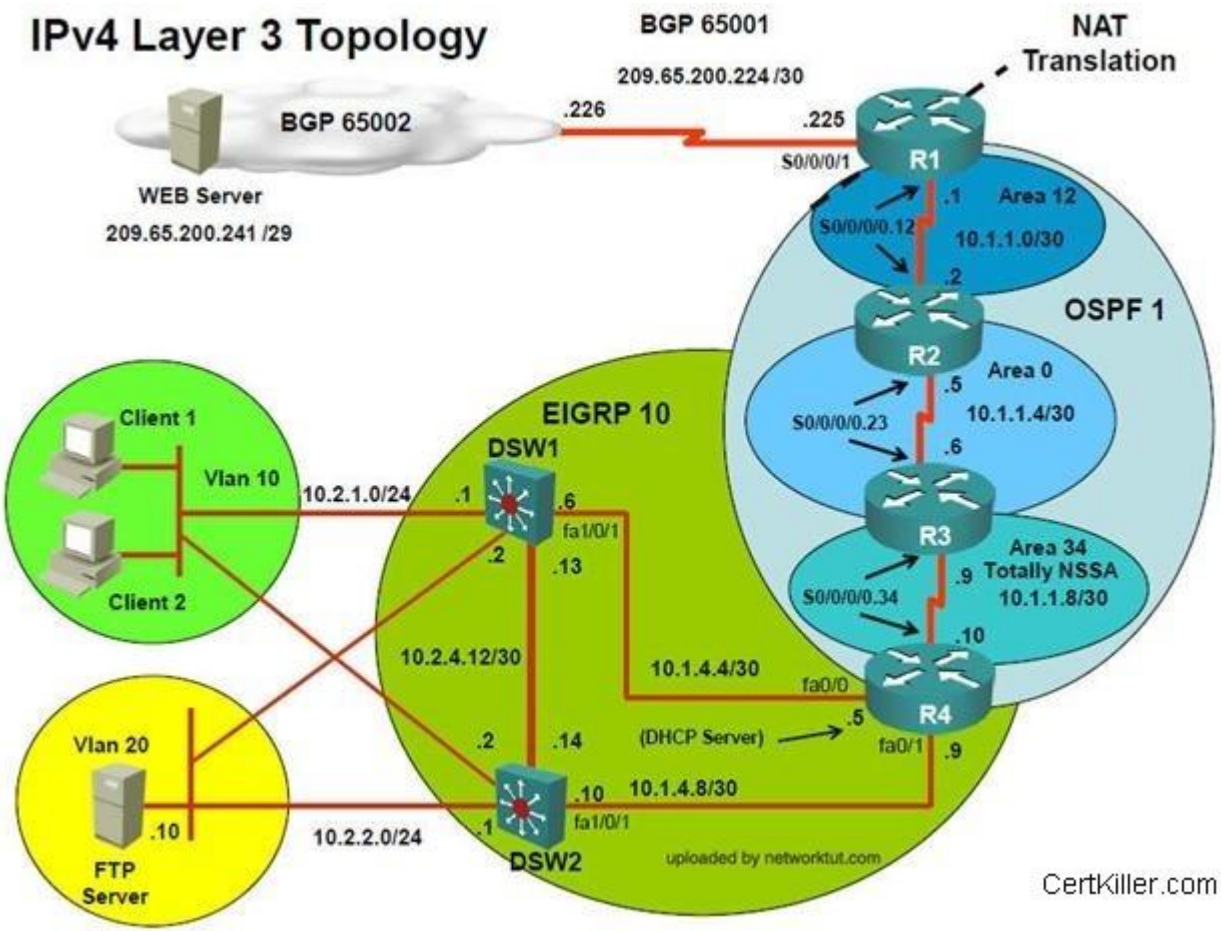

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

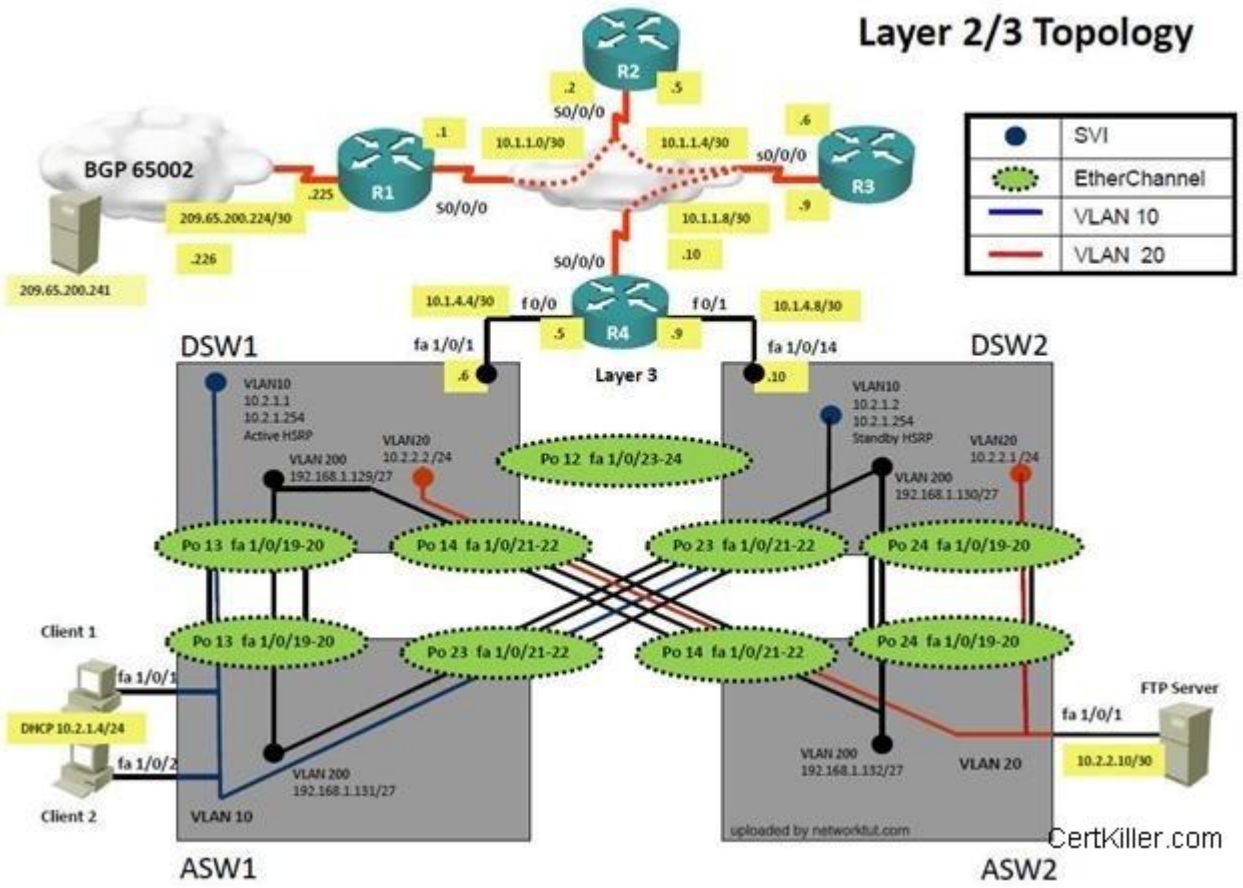
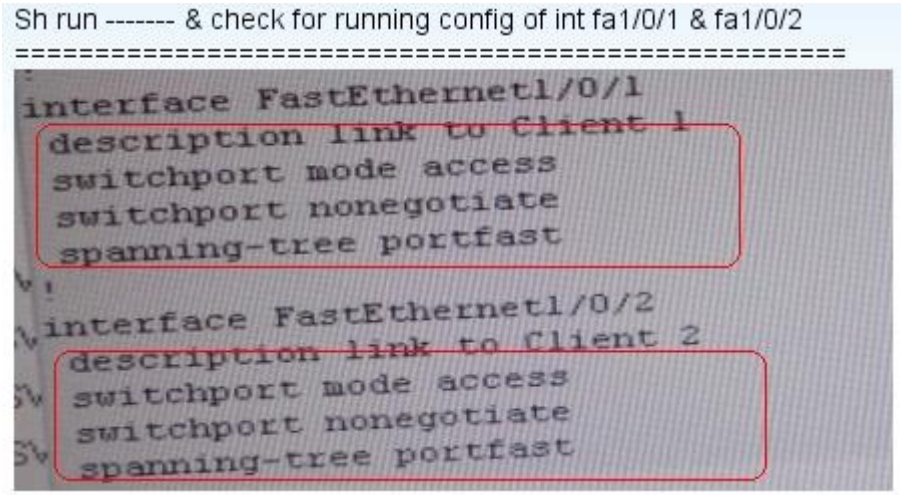


Figure 2

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

Configuration on ASW1



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: (none)
Explanation

Explanation/Reference:
Answer:
Access Vlans

QUESTION 3
(Ticket 2: Access VLAN)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

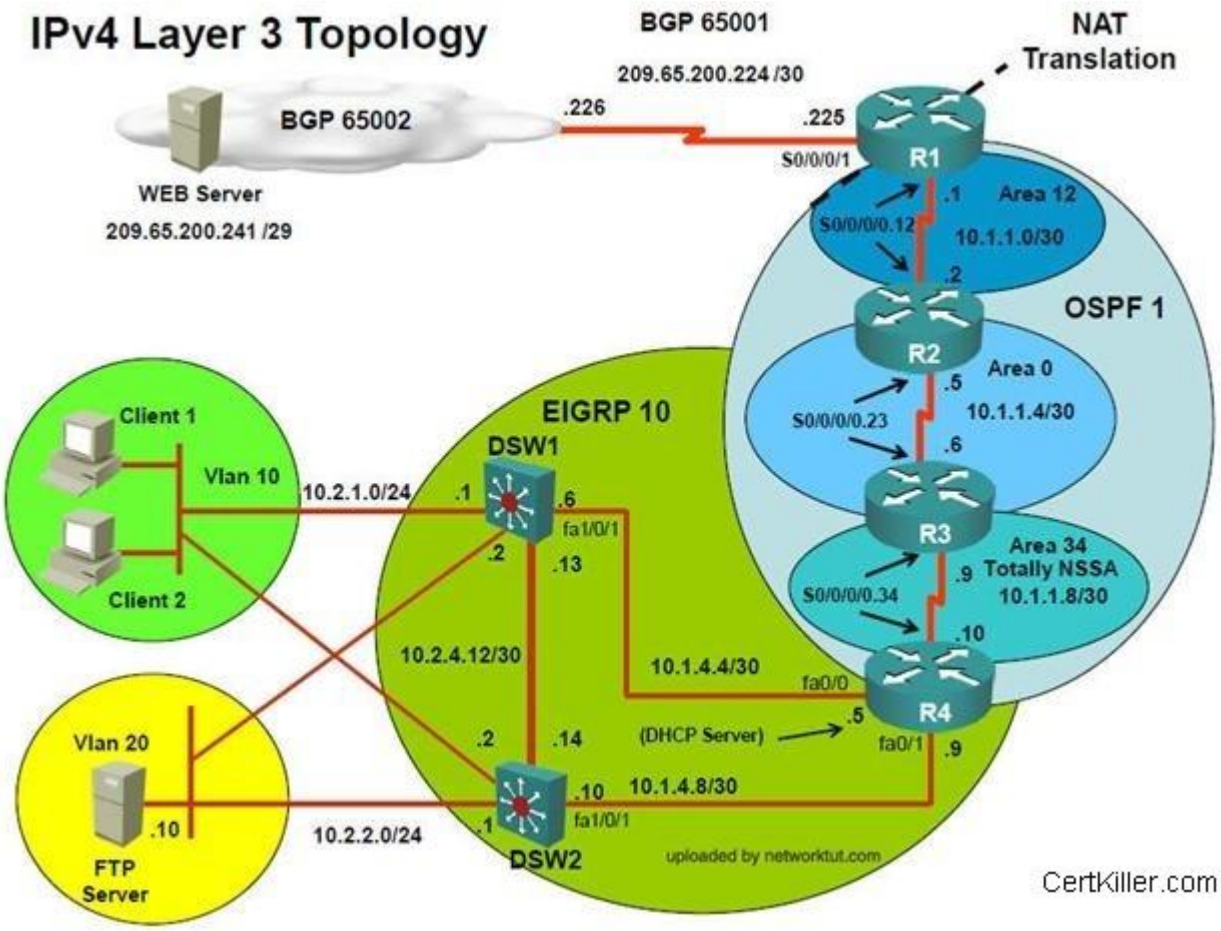

IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT
Translation
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.2
.13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

Figure 1

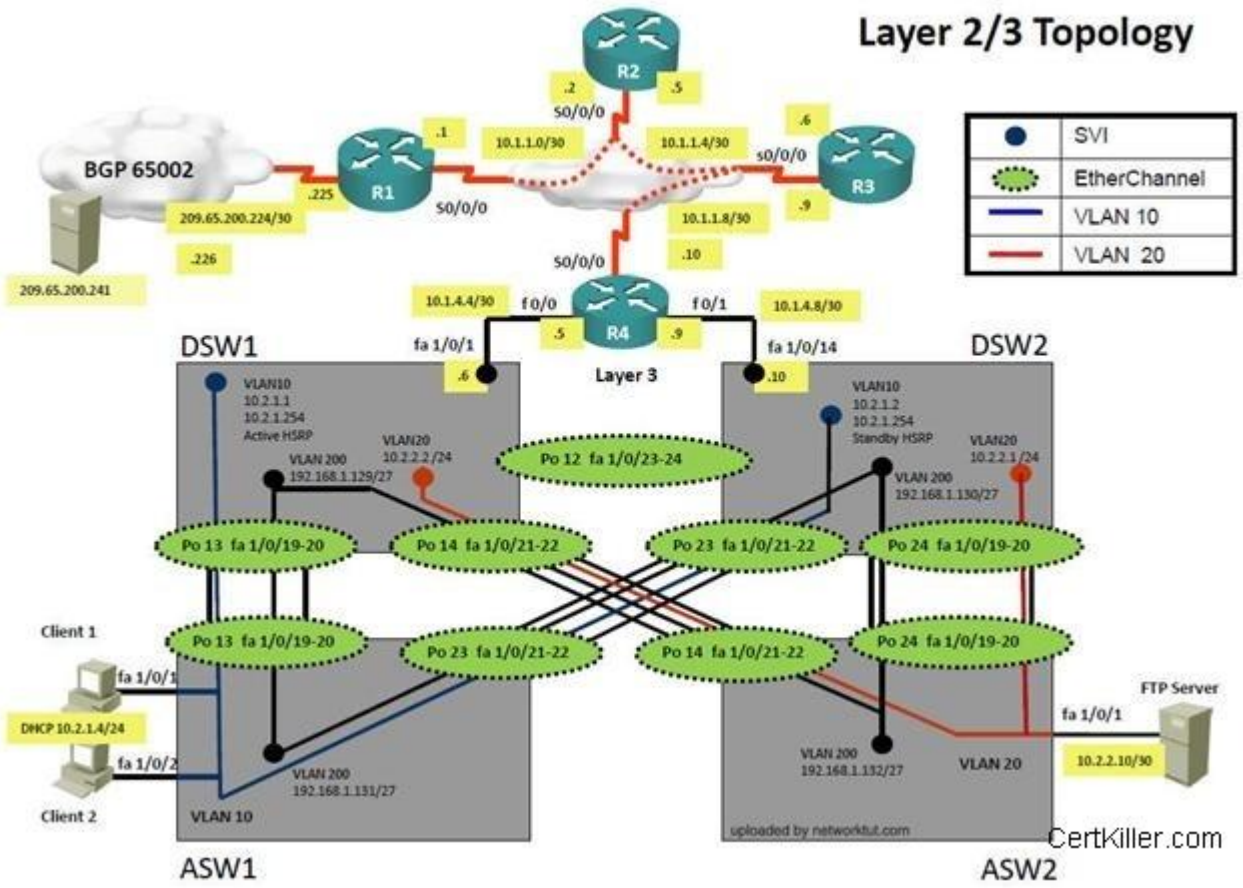
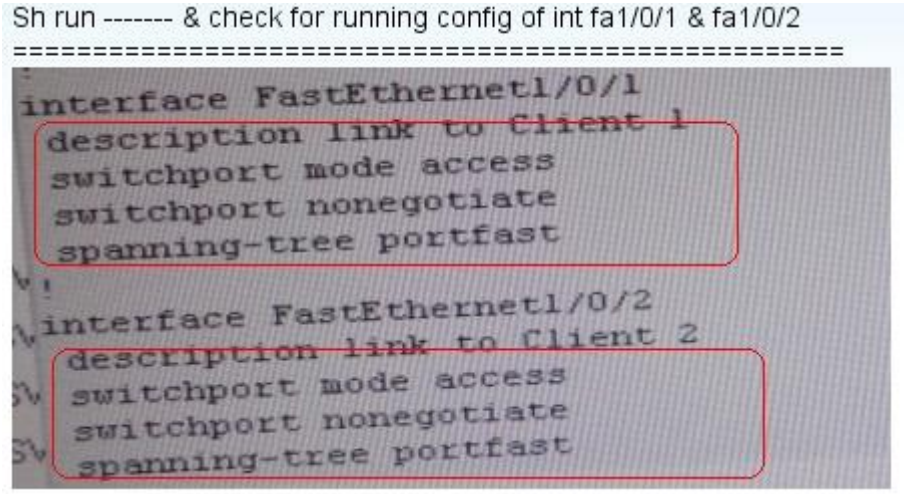


Figure 2

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

Configuration on ASW1



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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer:
In Configuration mode, using the interface rante Fastethernet 1/0/1 - 2, then switchport access vlan 10 command.

Exam D

QUESTION 1
(Ticket 3: OSPF Authentication)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

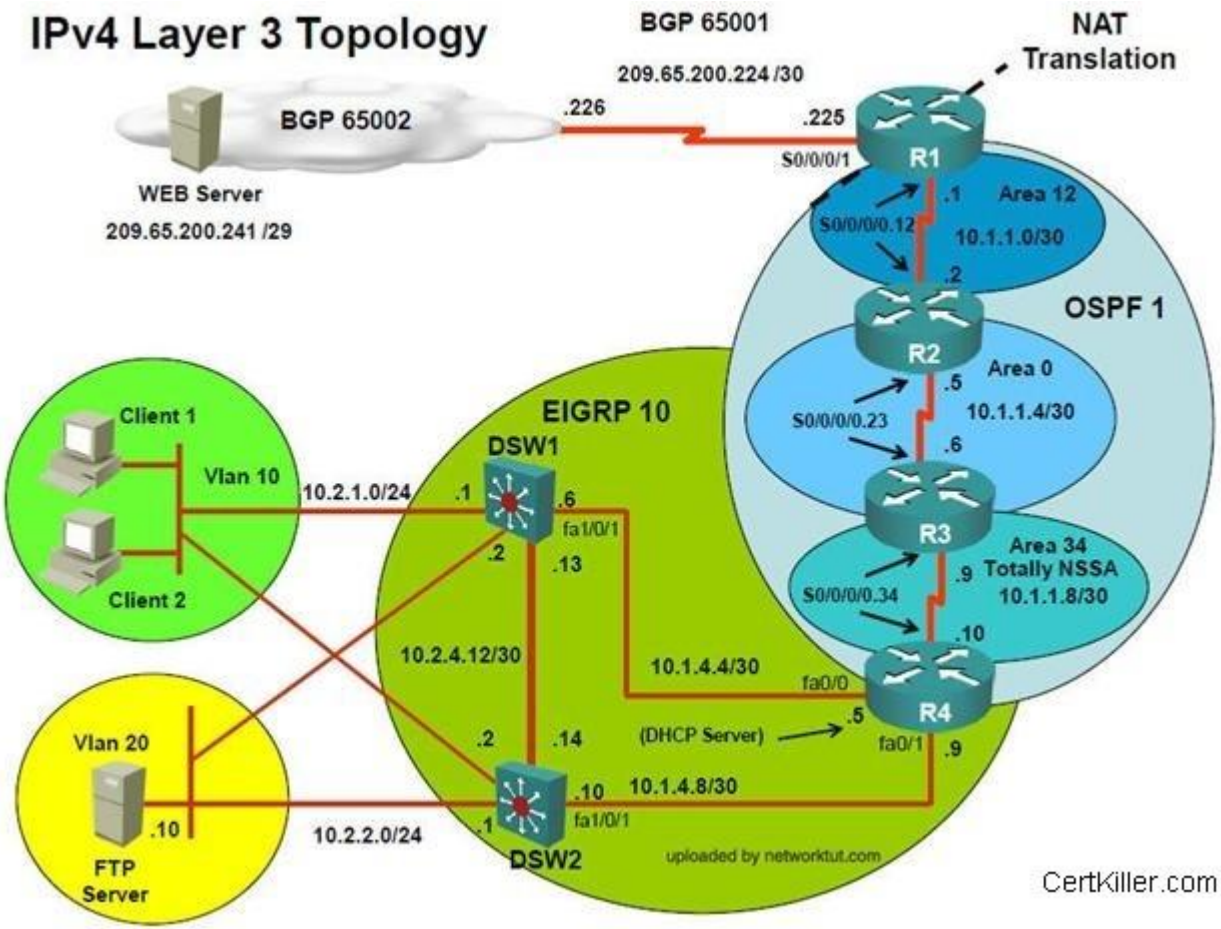


Figure 1

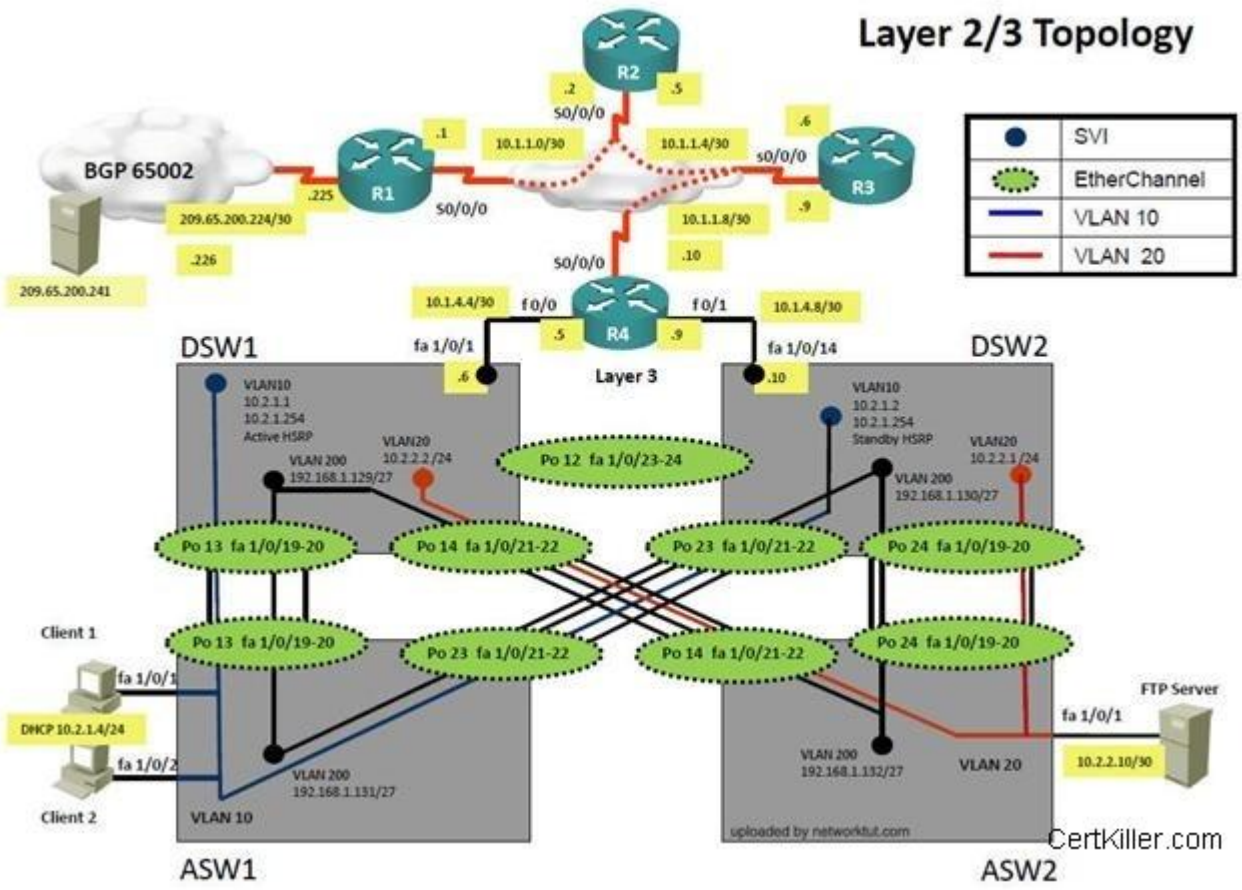
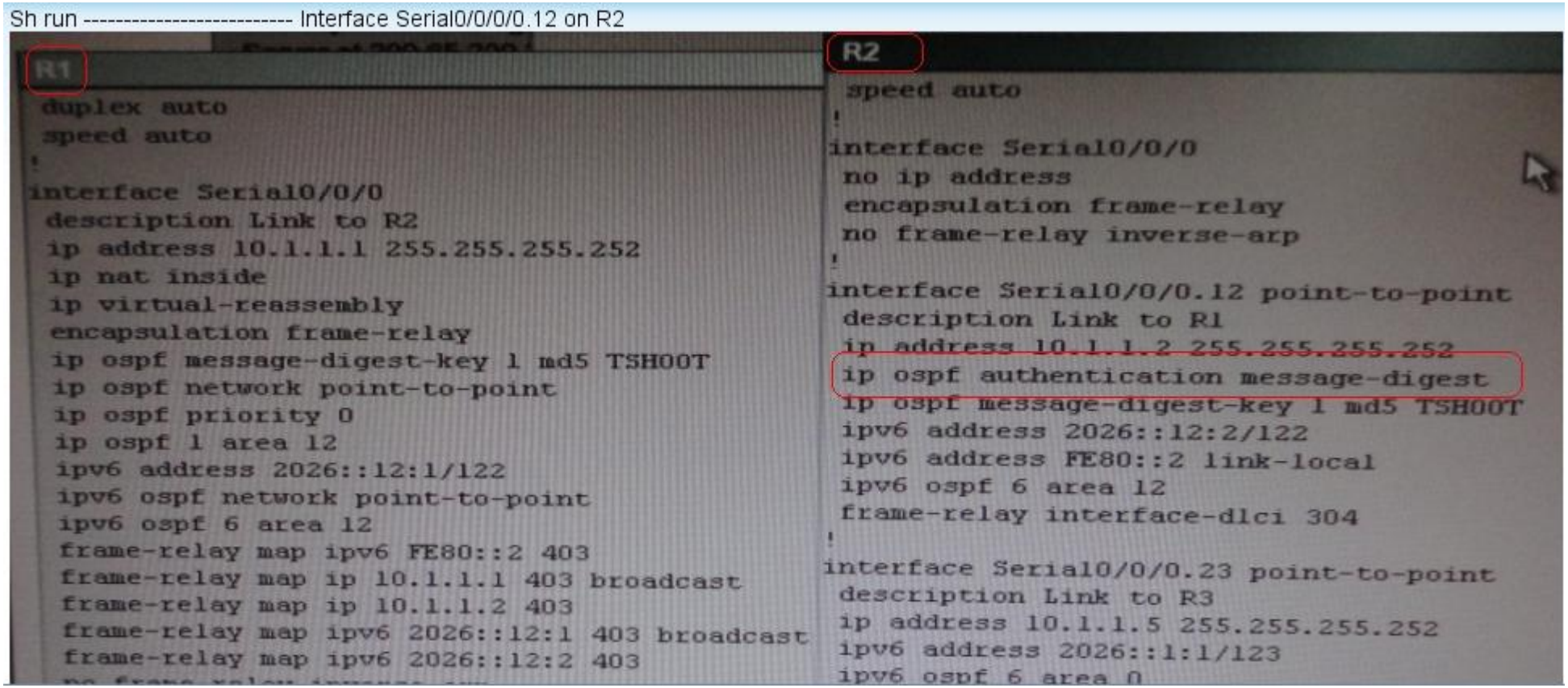


Figure 2

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

Configuration on R1 and R2



On which 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: (none)
Explanation

Explanation/Reference:
Answer: R1

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0
R1(config-if)#ip ospf authentication message-digest
*Mar 1 00:21:26.591: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0 from LOADING to FULL, Loading Doneend
R1#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.1.1.2	0	FULL/ -	00:00:33	10.1.1.2	Serial0/0

QUESTION 2
(Ticket 3: OSPF Authentication)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

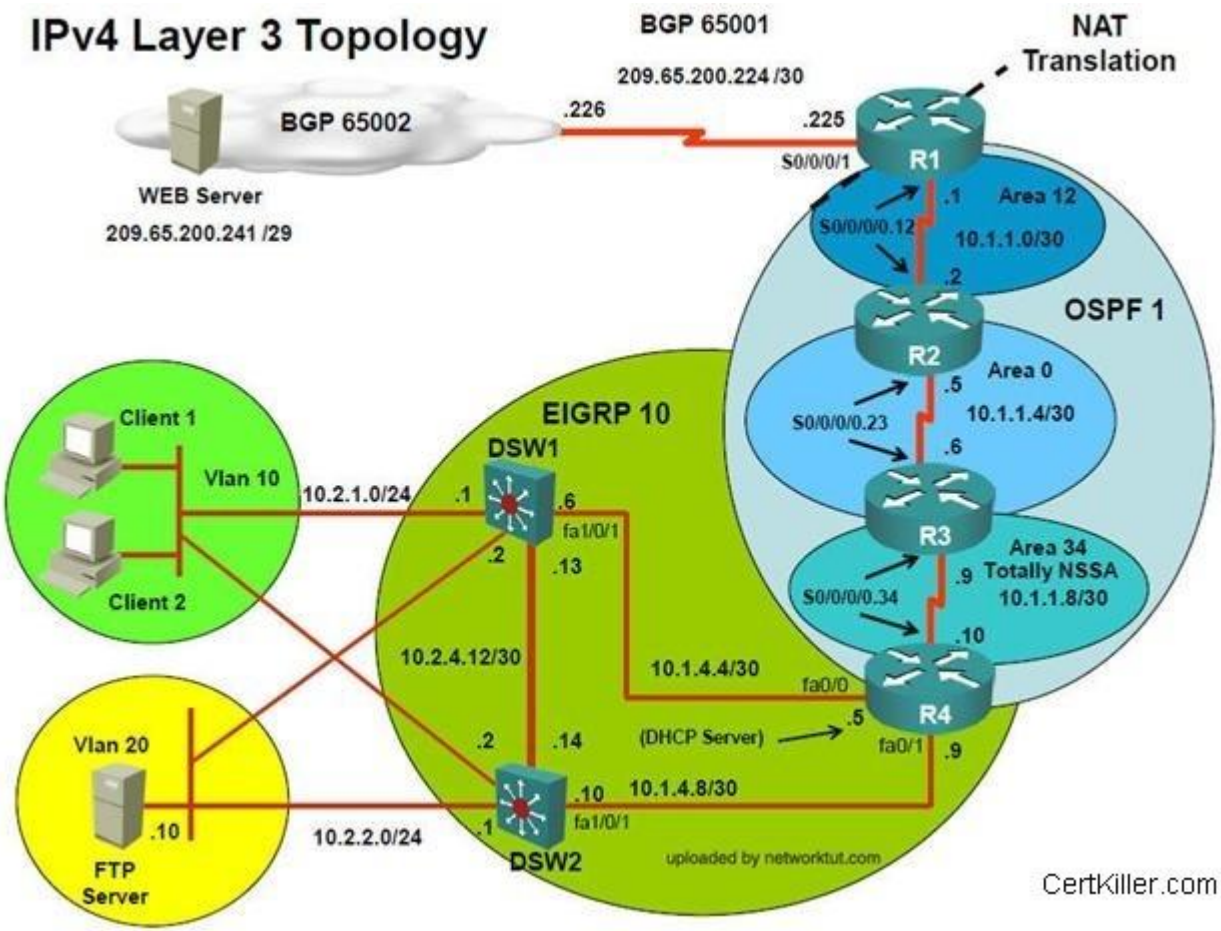

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

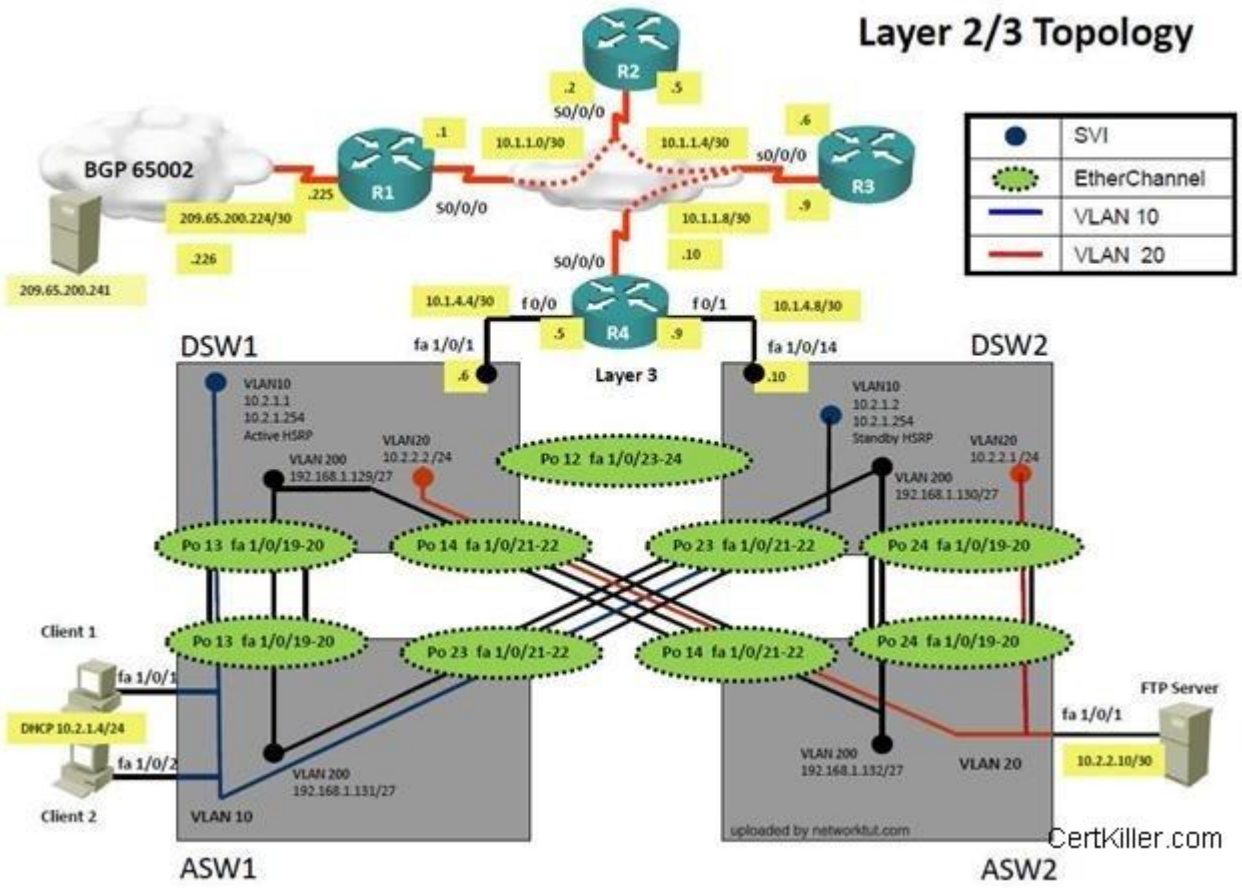
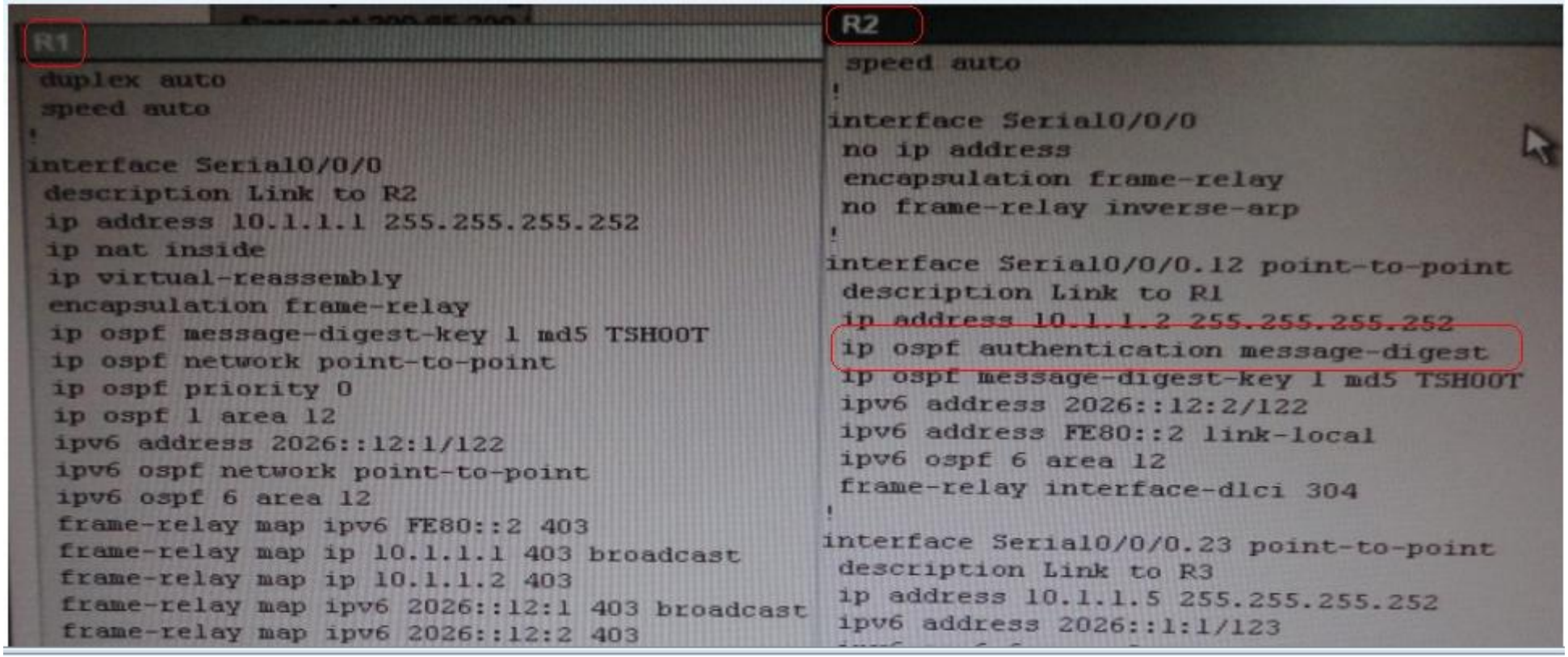


Figure 2

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

Configuration on R1 and R2



The fault condition is related to which techonology?

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: (none)
Explanation

Explanation/Reference:
Answer:
IPv4 OSPF Routing

QUESTION 3
(Ticket 3: OSPF Authentication)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

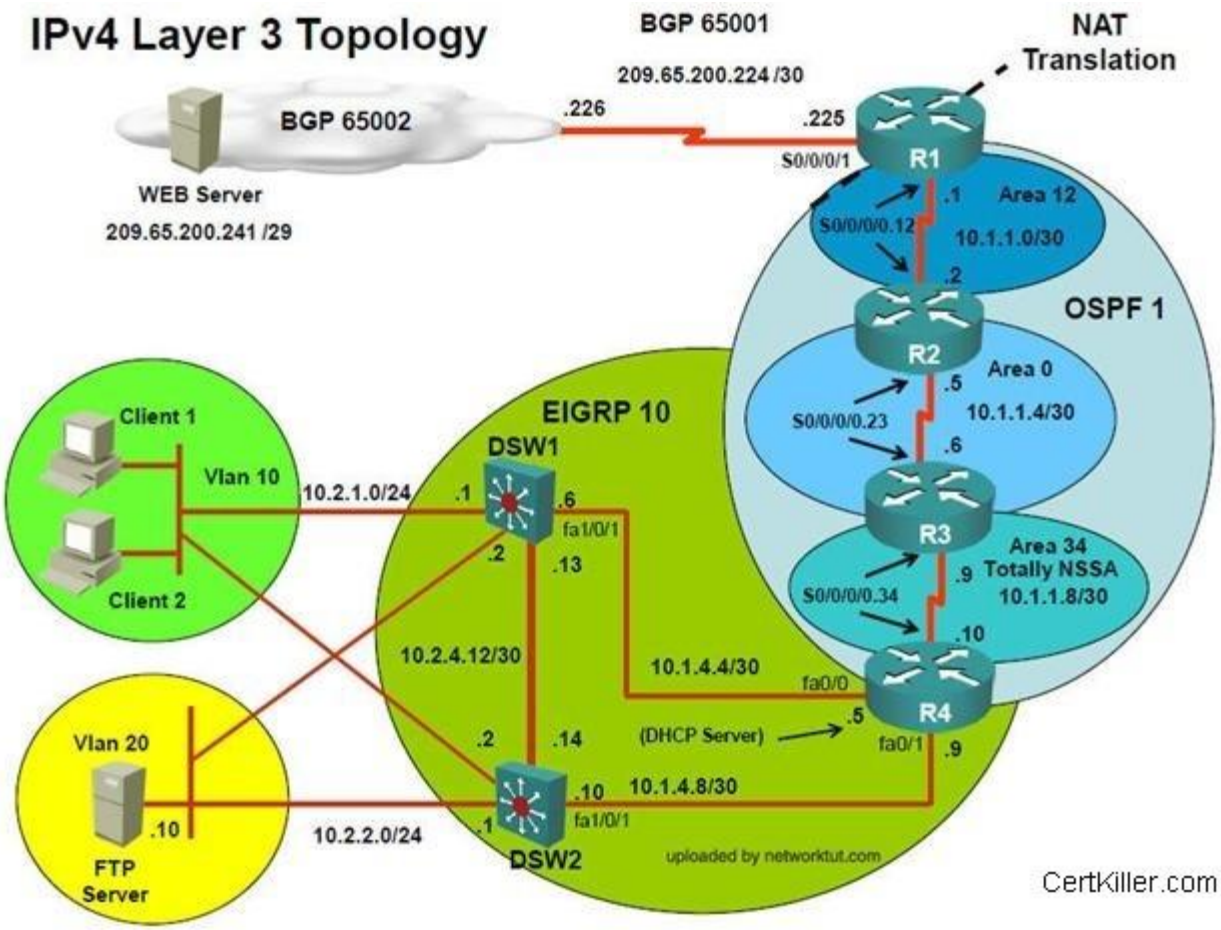


Figure 1

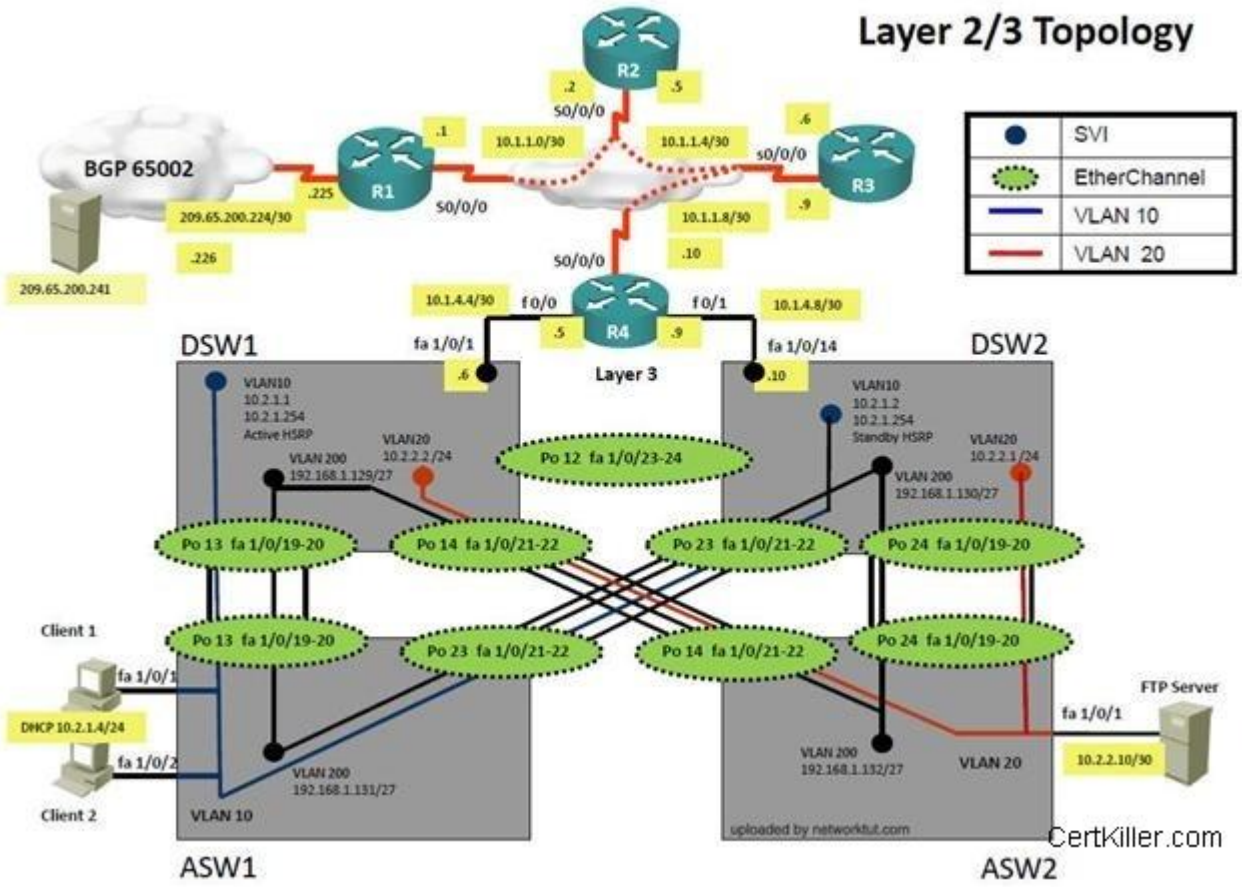


Figure 2

Trouble Ticket Statement:

Client 1 is able to ping 10.1.1.2 but not 10.1.1.1. Initial troubleshooting shows that R1 does not have any OSPF neighbors or any OSPF routes

Configuration on R1:

```
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.3 area 12
default-information originate always
!
interfaceSerial0/0/0/0.12 point-to-point
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip ospf message-digest-key 1 md5 TSHOOT
```

Configuration on R2:

```
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.3 area 12
!
interfaceSerial0/0/0/0.12 point-to-point
ip address 10.1.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 TSHOOT
```

What is the solution of the fault condition?

A. ip ospf authentication message-digest command has to be added on S0/0/0/0.12
B. ip ospf authentication message-digest command has to be added under the OSPF routing process
C. A static route to 10.1.1.4 must be added on R1
D. ip nat outside must be added on S0/0/0/0.12
E. ip ospf authentication command has to be added on router ospf 1 on R1
F. ip ospf authentication command has to be added on router ospf 1 on R2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: ip ospf authentication message-digest command has to be added on S0/0/0/0.12

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0
R1(config-if)#ip ospf authentication message-digest
*Mar  1 00:21:26.591: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0 from LOADING to FULL, Loading Doneend
```

```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.2          0   FULL/  -        00:00:33    10.1.1.2        Serial0/0
```

Exam E

QUESTION 1
(Ticket 4: BGP Neighbor)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

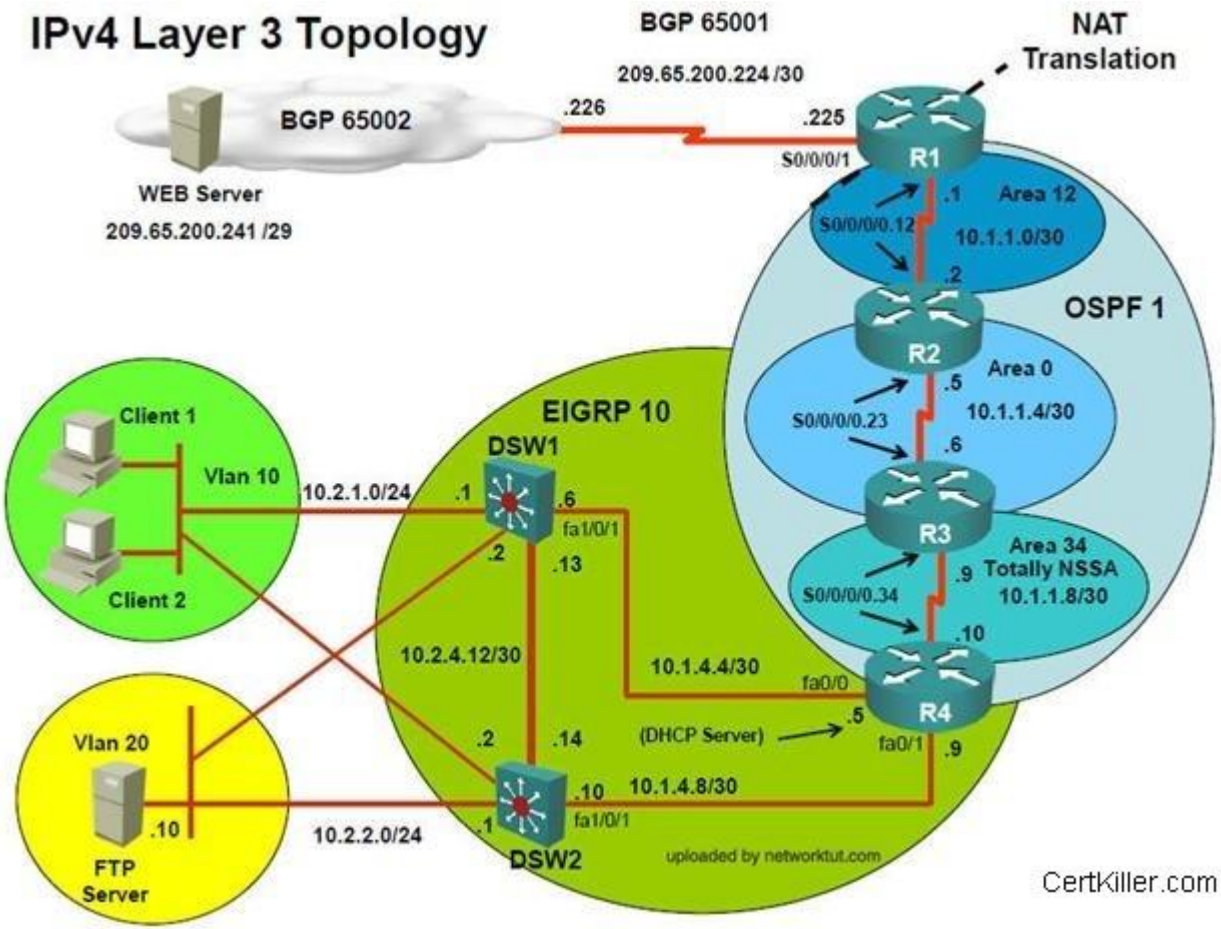


Figure 1

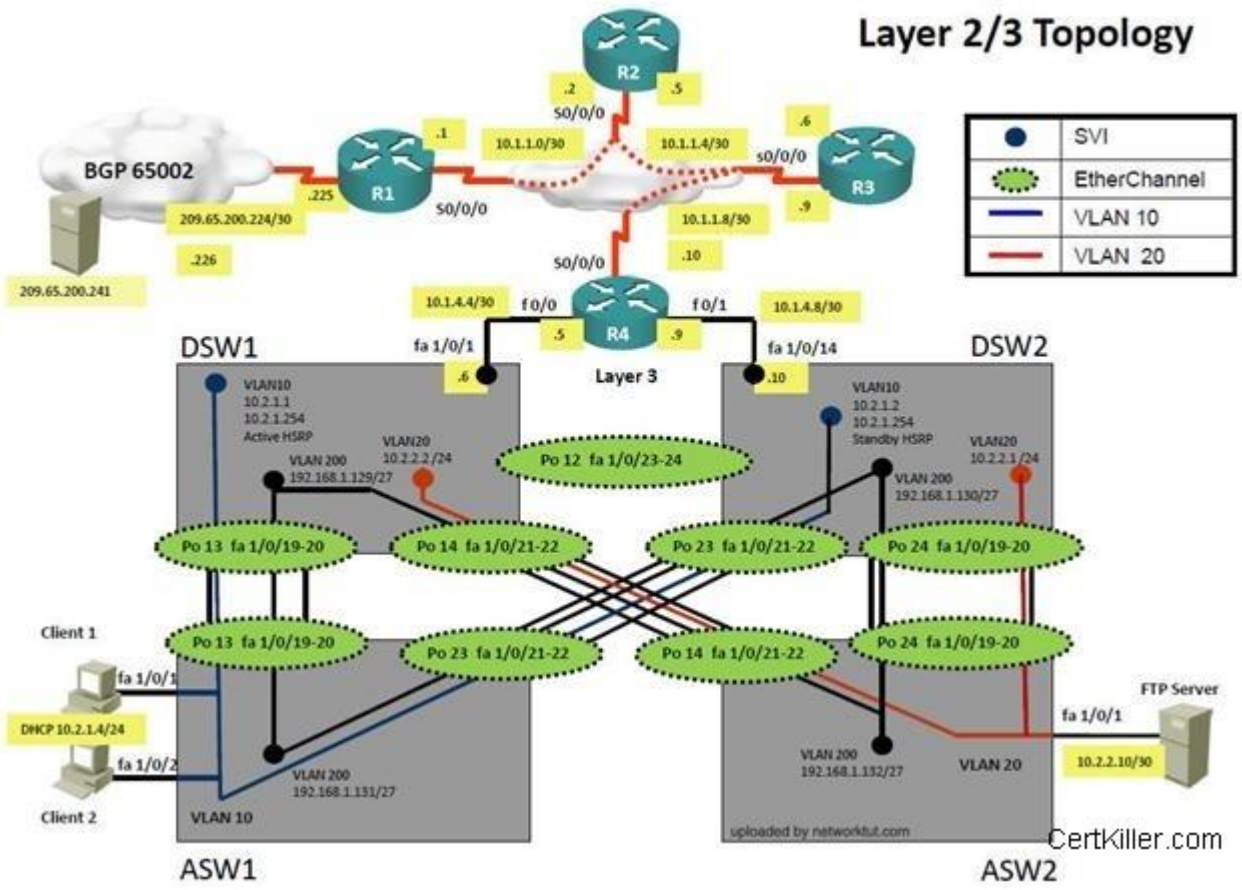
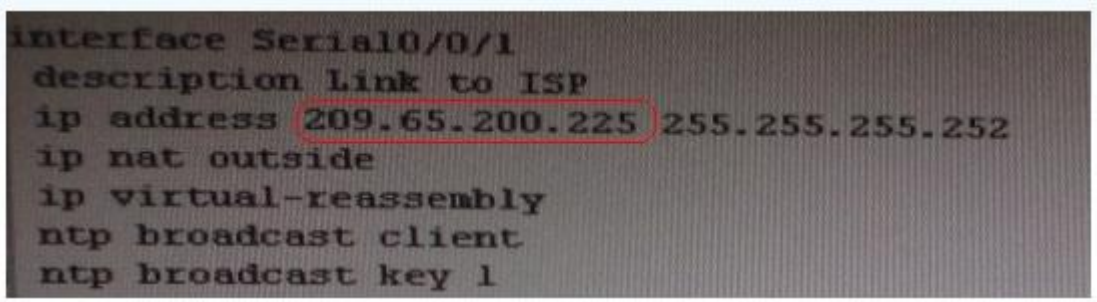
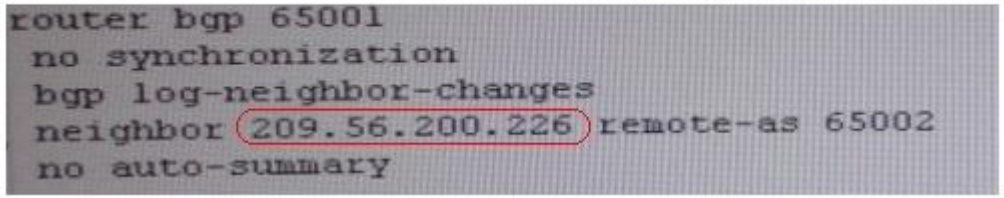


Figure 2

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

Configuration on R1





On which 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: (none)
Explanation

Explanation/Reference:
Answer: R1

R1#conf t
router bgp 65001
no neighbor 209.56.200.226 remote-as 65002

```
 neighbor 209.65.200.226 remote-as 65002
!
R1#*Mar  1 00:11:08.475: %BGP-5-ADJCHANGE: neighbor 209.65.2!
R1#sh bgp ipv4 unicast neighbors
BGP neighbor is 209.65.200.226,  remote AS 65002, external link
  BGP version 4, remote router ID 209.65.200.226
  BGP state = Established, up for 00:00:34
  Last read 00:00:34, last write 00:00:34, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          1
    Keepalives:             3          3
    Route Refresh:          0          0
    Total:                  5          5
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3/0
  Output queue size: 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                             Sent       Rcvd
  Prefix activity:           ----       ----
    Prefixes Current:           1          2 (Consumes 104 bytes)
    Prefixes Total:             1          2
    Implicit Withdraw:          0          0
    Explicit Withdraw:          0          0
    Used as bestpath:           n/a        1
    Used as multipath:          n/a        0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Bestpath from this peer:          1        n/a
    Total:                            1          0
  Number of NLRIs in the update sent: max 1, min 1

  Connections established 1; dropped 0
```

Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 1
Local host: 209.65.200.225, Local port: 179
Foreign host: 209.65.200.226, Foreign port: 43724
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xAD5B4):

Timer	Starts	Wakeups	Next
Retrans	3	0	0x0
TimeWait	0	0	0x0
AckHold	3	1	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0
Linger	0	0	0x0
ProcessQ	0	0	0x0

iss: 4241709572 snduna: 4241709728 sndnxt: 4241709728 sndwnd: 16229
irs: 2155992730 rcvnxt: 2155992891 rcvwnd: 16224 delrcvwnd: 160

SRTT: 99 ms, RTTO: 1539 ms, RTV: 1440 ms, KRTT: 0 ms
minRTT: 52 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 7 (out of order: 0), with data: 5, total data bytes: 160
Sent: 7 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 5, total data bytes: 155
Packets received in fast path: 0, fast processed: 0, slow path: 0
Packets send in fast path: 0
fast lock acquisition failures: 0, slow path: 0

QUESTION 2
(Ticket 4: BGP Neighbor)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

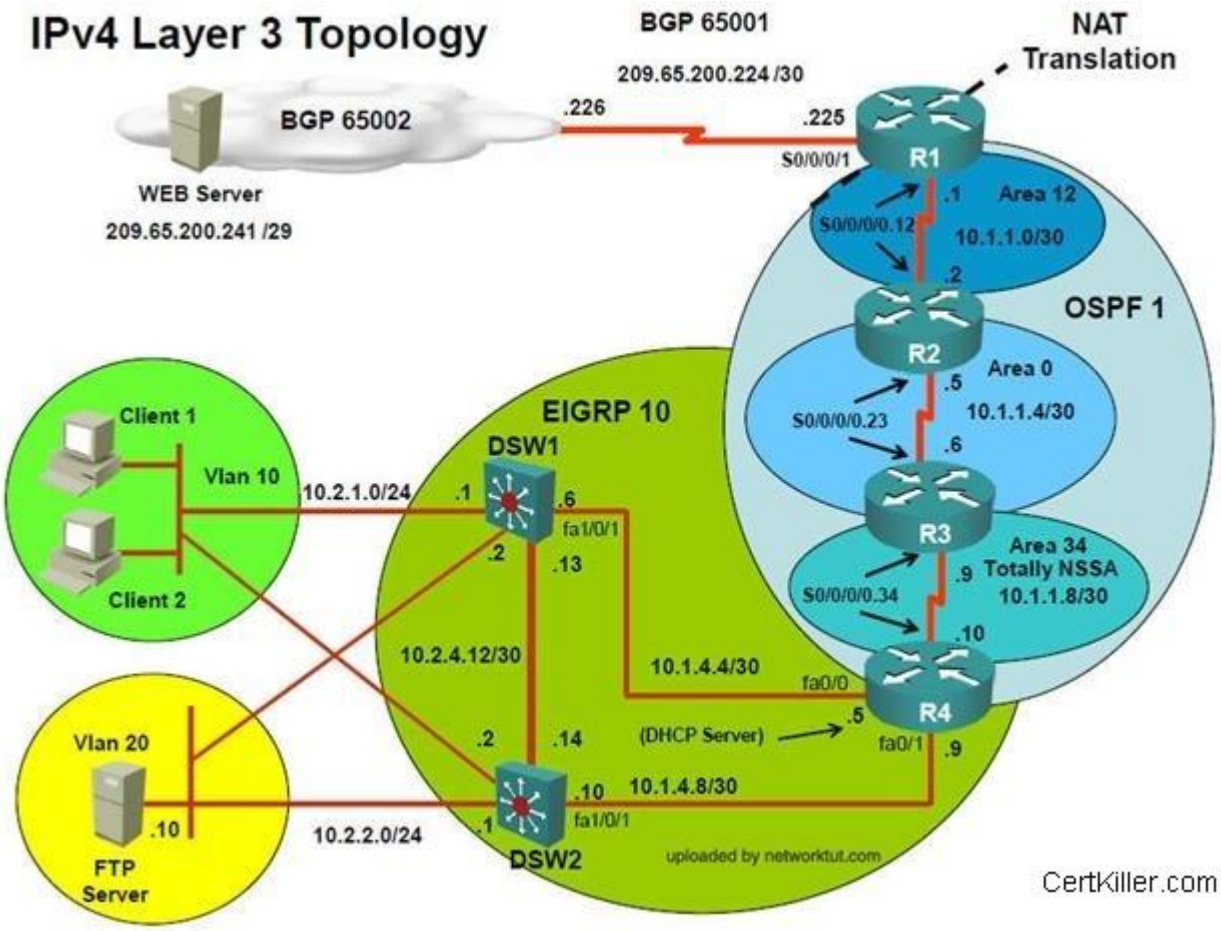

IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT
Translation
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
.5
Area 0
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
.2
.13
Area 34
Totally NSSA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

Figure 1

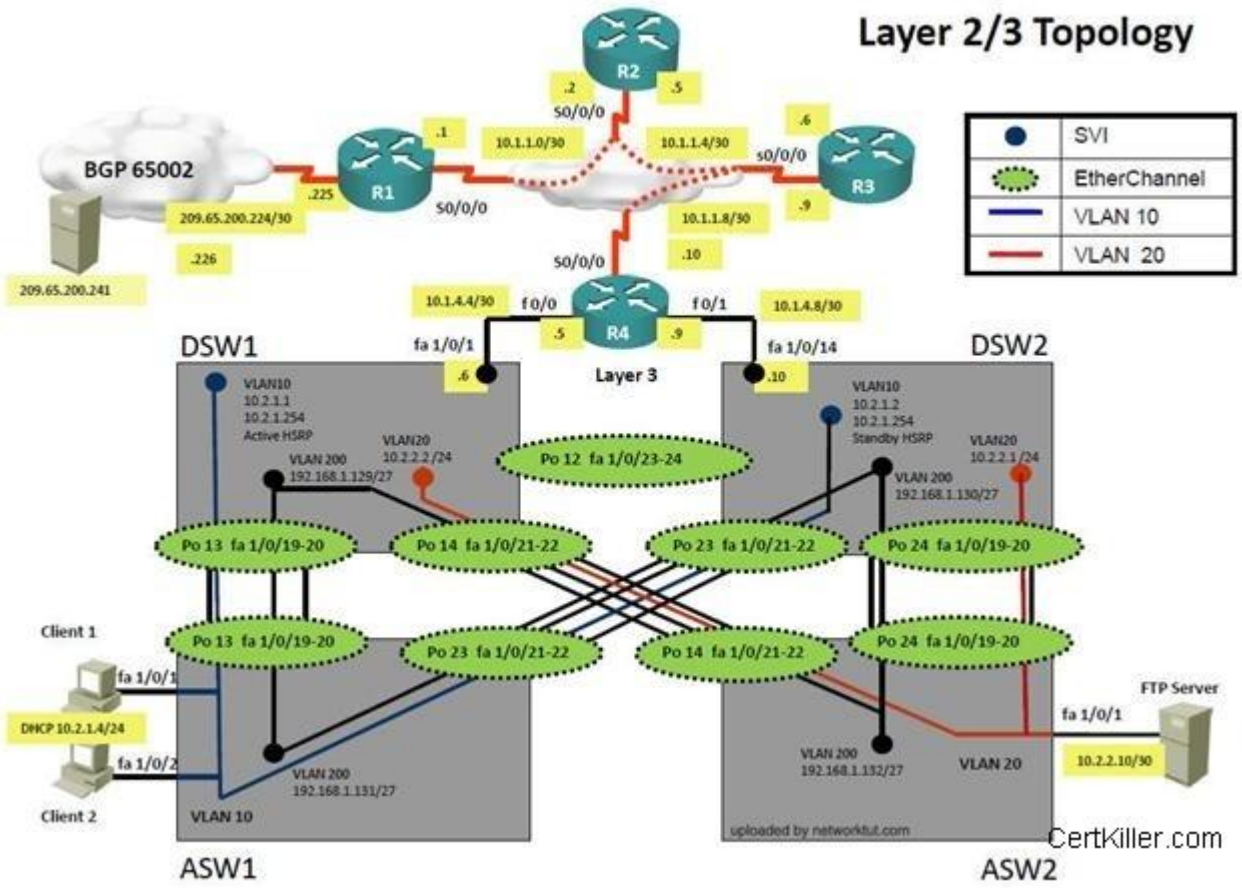


Figure 2

Trouble Ticket Statement

Client 1 is able to ping 209.65.200.226 but not the Web Server at 209.65.200.241. Initial troubleshooting shows and R1 does not have any BGP routes. R1 also does not show any active BGP neighbor

Configuration on R1

router bgp 65001
no synchronization
bgp log-neighbor-changes

```
network 209.65.200.224 mask 255.255.255.252
neighbor 209.56.200.226 remote-as 65002
no auto-summary

R1#sh bgp ipv4 unicast neighbors
BGP neighbor is 209.56.200.226,  remote AS 65002, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 00:00:20, last write 00:00:20, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Total:                  0          0
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 0/0
  Output queue size: 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                           Sent       Rcvd
  Prefix activity:         ----       ----
    Prefixes Current:         0          0
    Prefixes Total:           0          0
    Implicit Withdraw:        0          0
    Explicit Withdraw:        0          0
    Used as bestpath:         n/a        0
    Used as multipath:        n/a        0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                        0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 0; dropped 0
  Last reset never
  External BGP neighbor not directly connected.
  No active TCP connection
```

The Fault Condition is related to which technology?

A. EIGRP
B. HSRP
C. BGP
D. OSPF
E. OSPFv3
F. RIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: BGP

```
R1#conf t
router bgp 65001
 no  neighbor 209.56.200.226 remote-as 65002
 neighbor 209.65.200.226 remote-as 65002
!
R1#*Mar  1 00:11:08.475: %BGP-5-ADJCHANGE: neighbor 209.65.2!
R1#sh bgp ipv4 unicast neighbors
BGP neighbor is 209.65.200.226,  remote AS 65002, external link
  BGP version 4, remote router ID 209.65.200.226
  BGP state = Established, up for 00:00:34
  Last read 00:00:34, last write 00:00:34, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          1
    Keepalives:             3          3
    Route Refresh:          0          0
    Total:                  5          5
  Default minimum time between advertisement runs is 30 seconds
```

```
 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3/0
  Output queue size: 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                           Sent       Rcvd
  Prefix activity:         ----       ----
    Prefixes Current:         1          2 (Consumes 104 bytes)
    Prefixes Total:           1          2
    Implicit Withdraw:        0          0
    Explicit Withdraw:        0          0
    Used as bestpath:       n/a          1
    Used as multipath:      n/a          0

                           Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Bestpath from this peer:          1        n/a
    Total:                            1          0
  Number of NLRIs in the update sent: max 1, min 1

  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 1
Local host: 209.65.200.225, Local port: 179
Foreign host: 209.65.200.226, Foreign port: 43724
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xAD5B4):
Timer          Starts    Wakeups            Next
Retrans             3          0             0x0
TimeWait            0          0             0x0
AckHold             3          1             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
ProcessQ            0          0             0x0
```

iss: 4241709572 snduna: 4241709728 sndnxt: 4241709728 sndwnd: 16229
irs: 2155992730 rcvnxt: 2155992891 rcvwnd: 16224 delrcvwnd: 160

SRTT: 99 ms, RTTO: 1539 ms, RTV: 1440 ms, KRTT: 0 ms
minRTT: 52 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 7 (out of order: 0), with data: 5, total data bytes: 160
Sent: 7 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 5, total data bytes: 155
 Packets received in fast path: 0, fast processed: 0, slow path: 0
 Packets send in fast path: 0
 fast lock acquisition failures: 0, slow path: 0

QUESTION 3
(Ticket 4: BGP Neighbor)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

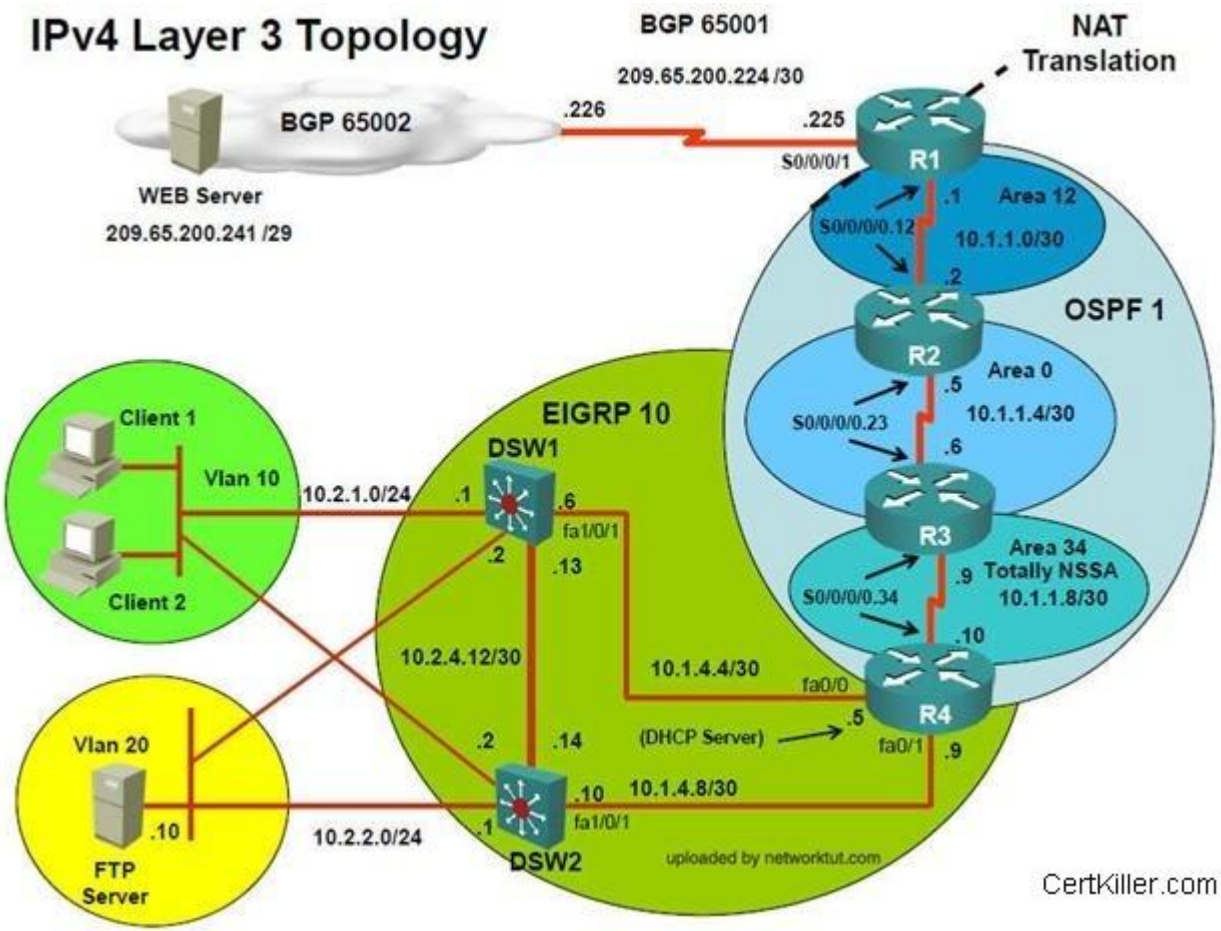

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

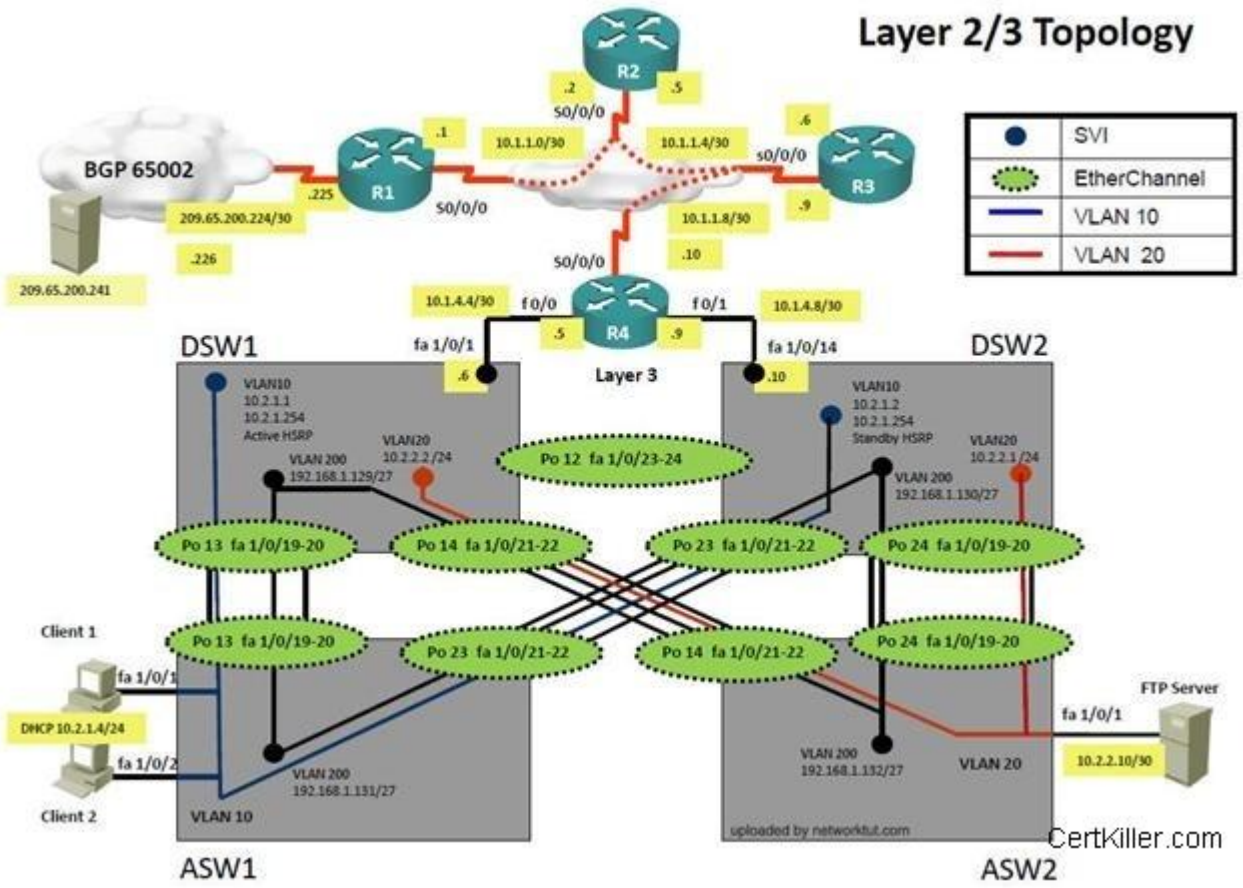
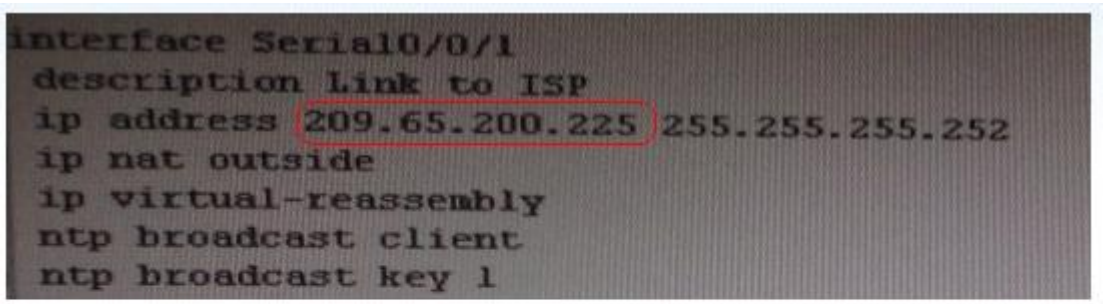
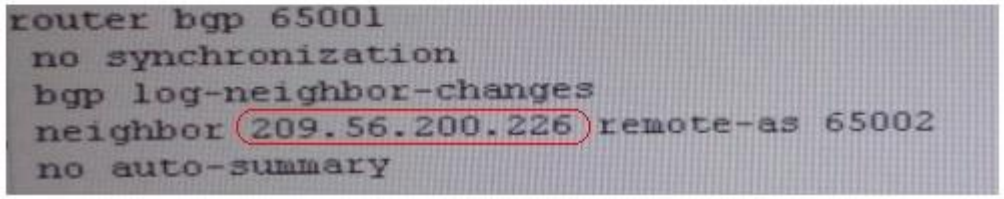


Figure 2

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

Configuration on R1





What is the solution to the fault condition?

A. Under the BGP process, enter the bgp redistribute-internal command.
B. Under the BGP process, bgp confederation identifier 65001 command.
C. Delete the current BGP process and reenter all of the commands 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: (none)
Explanation

Explanation/Reference:
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.

R1#conf t
router bgp 65001
no neighbor 209.56.200.226 remote-as 65002
neighbor 209.65.200.226 remote-as 65002
!
R1#*Mar 1 00:11:08.475: %BGP-5-ADJCHANGE: neighbor 209.65.2!

```
R1#sh bgp ipv4 unicast neighbors
BGP neighbor is 209.65.200.226,  remote AS 65002, external link
  BGP version 4, remote router ID 209.65.200.226
  BGP state = Established, up for 00:00:34
  Last read 00:00:34, last write 00:00:34, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          1
    Keepalives:             3          3
    Route Refresh:          0          0
    Total:                  5          5
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3/0
  Output queue size: 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                           Sent       Rcvd
  Prefix activity:         ----       ----
    Prefixes Current:         1          2 (Consumes 104 bytes)
    Prefixes Total:           1          2
    Implicit Withdraw:        0          0
    Explicit Withdraw:        0          0
    Used as bestpath:       n/a          1
    Used as multipath:      n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Bestpath from this peer:            1        n/a
    Total:                              1          0
  Number of NLRIs in the update sent: max 1, min 1

  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 1
```

Local host: 209.65.200.225, Local port: 179
Foreign host: 209.65.200.226, Foreign port: 43724
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xAD5B4):

Timer	Starts	Wakeups	Next
Retrans	3	0	0x0
TimeWait	0	0	0x0
AckHold	3	1	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0
Linger	0	0	0x0
ProcessQ	0	0	0x0

iss: 4241709572 snduna: 4241709728 sndnxt: 4241709728 sndwnd: 16229
irs: 2155992730 rcvnxt: 2155992891 rcvwnd: 16224 delrcvwnd: 160

SRTT: 99 ms, RTTO: 1539 ms, RTV: 1440 ms, KRTT: 0 ms
minRTT: 52 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 7 (out of order: 0), with data: 5, total data bytes: 160
Sent: 7 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 5, total data bytes: 155
 Packets received in fast path: 0, fast processed: 0, slow path: 0
 Packets send in fast path: 0
 fast lock acquisition failures: 0, slow path: 0

Exam F

QUESTION 1
(Ticket 5: NAT ACL)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

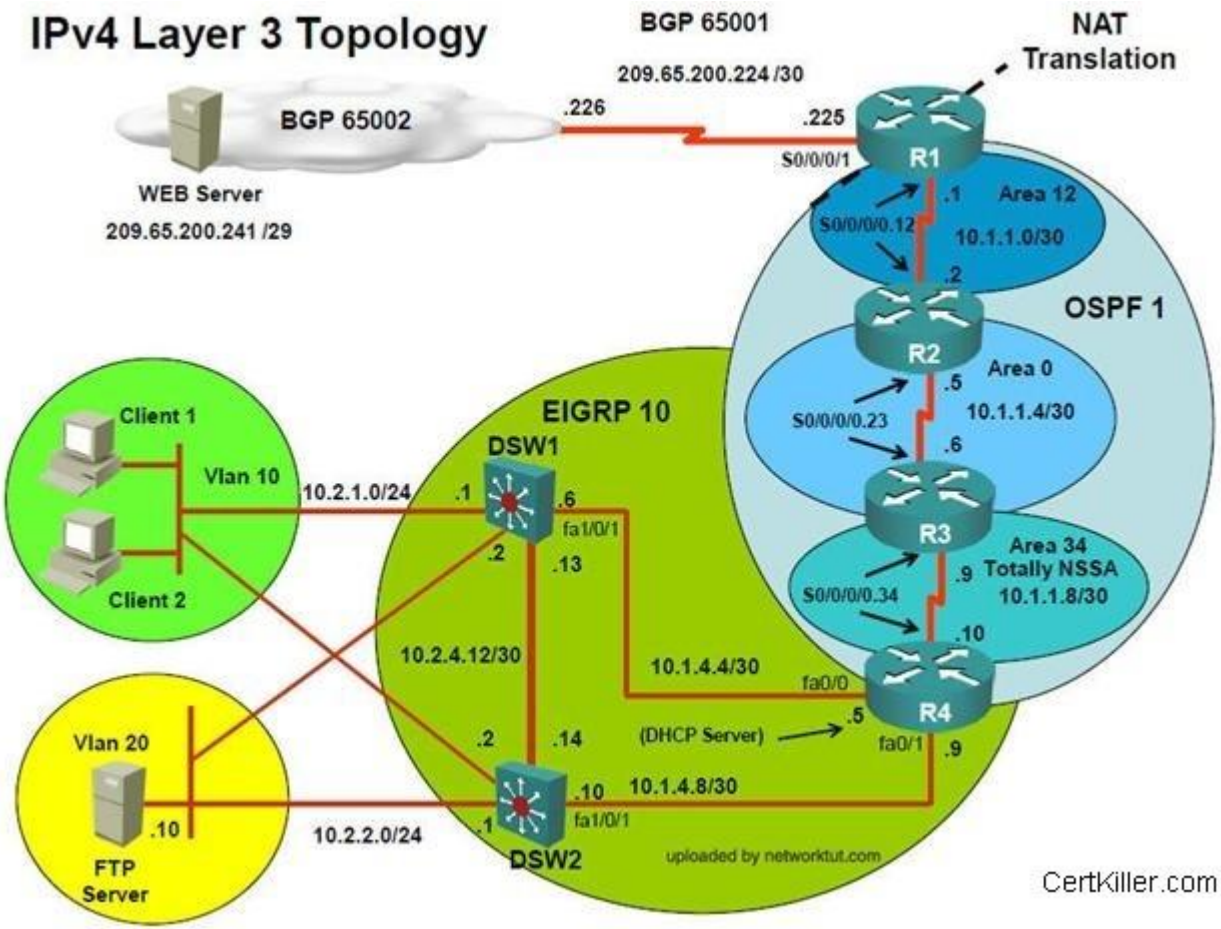


Figure 1

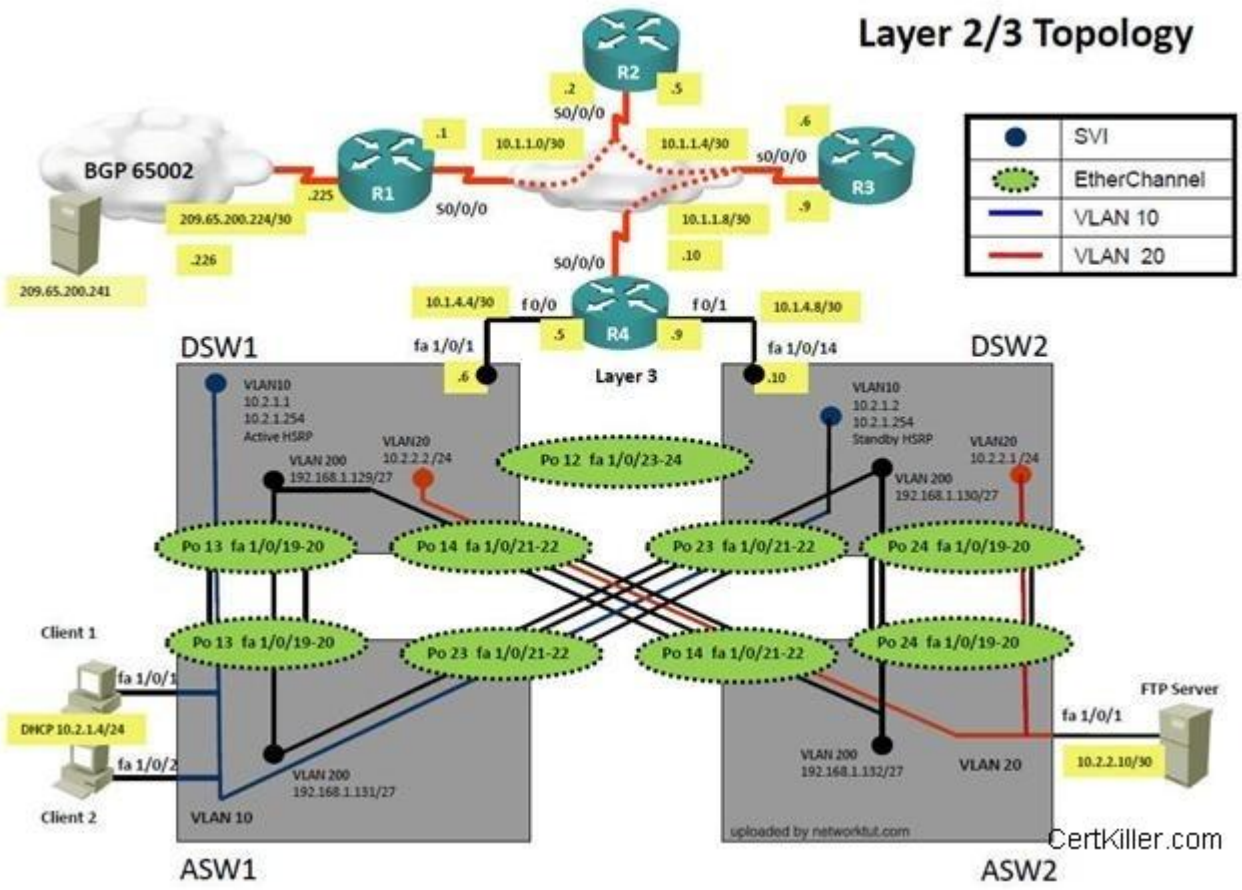


Figure 2

Trouble Ticket Statement

Client 1 and Client 2 are not able to reach the WebServer at 209.65.200.241. Initial troubleshooting shows that DSW1, DSW2 and all the routers are able to reach the WebServer

Configuration on R1

ip nat inside source list nat_pool interface Serial0/0/0/1 overload !
ip access-list standard nat_pool

permit 10.1.0.0
!
interface Serial0/0/0/1
ip address 209.65.200.224 255.255.255.252
ip nat outside
!
interfaceSerial0/0/0/0.12
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip ospf message-digest-key 1 md5 TSHOOT
ip ospd authentication message-digest

On Which device is the fault condition located?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: R1

QUESTION 2
(Ticket 5: NAT ACL)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

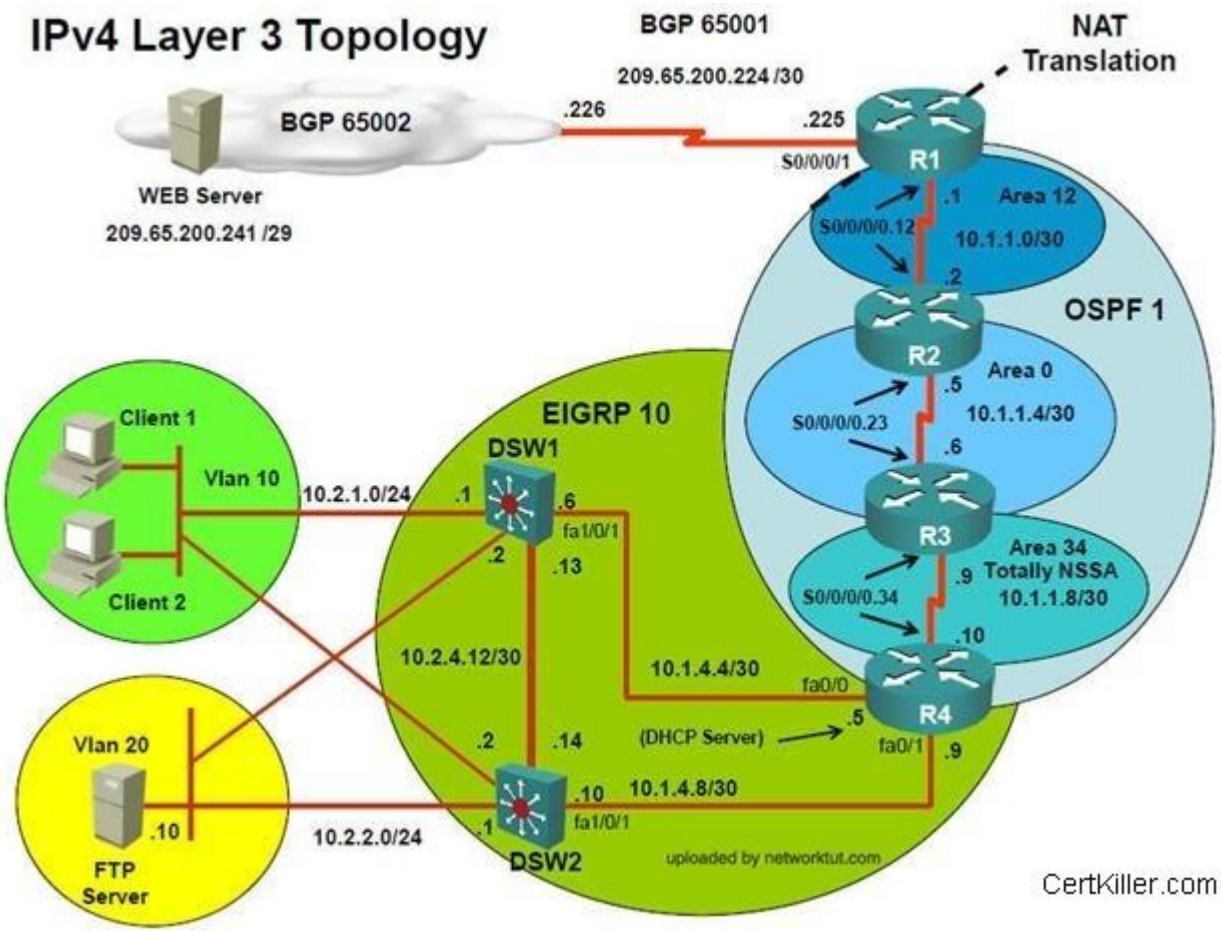

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

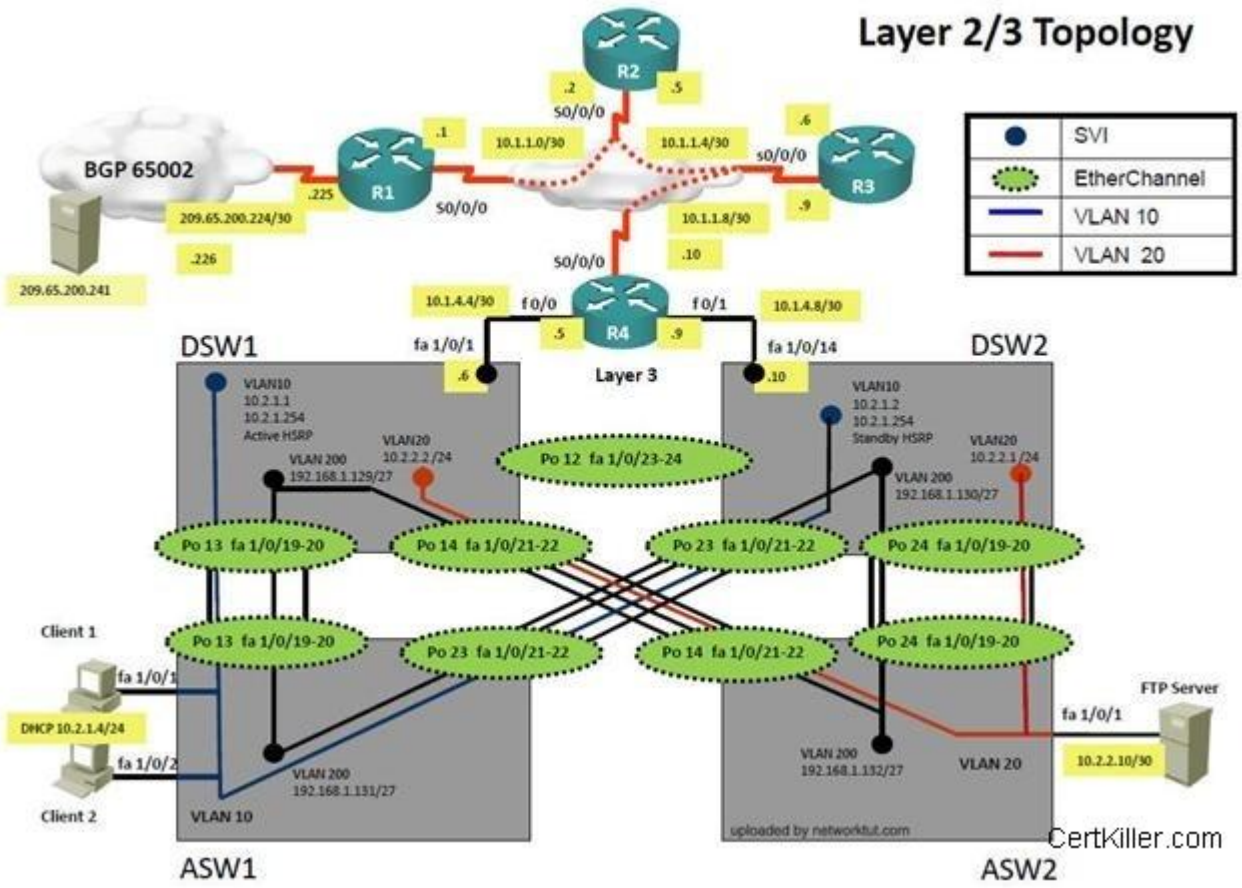


Figure 2

Trouble Ticket Statement

Client 1 and Client 2 are not able to reach the WebServer at 209.65.200.241. Initial troubleshooting shows that DSW1, DSW2 and all the routers are able to reach the WebServer

Configuration on R1

ip nat inside source list nat_pool interface Serial0/0/0/1 overload !
ip access-list standard nat_pool
permit 10.1.0.0

!
interface Serial0/0/0/1
ip address 209.65.200.224 255.255.255.252
ip nat outside
!
interfaceSerial0/0/0/0.12
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip ospf message-digest-key 1 md5 TSHOOT
ip ospd authentication message-digest

The Fault Condition is related to which technology?

A. EIGRP
B. HSRP
C. BGP
D. NAT
E. OSPF
F. OSPFv3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: NAT

QUESTION 3
(Ticket 5: NAT ACL)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

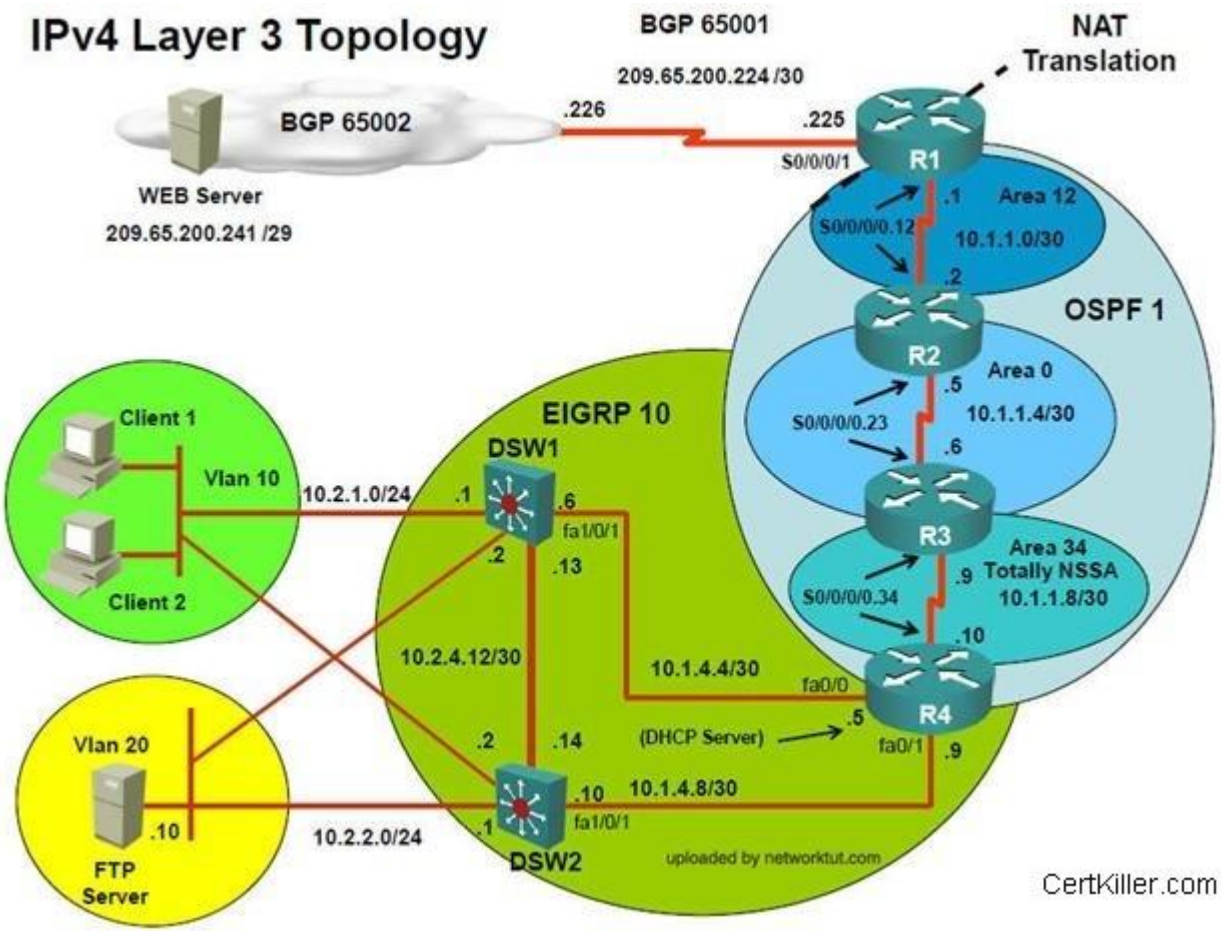


Figure 1

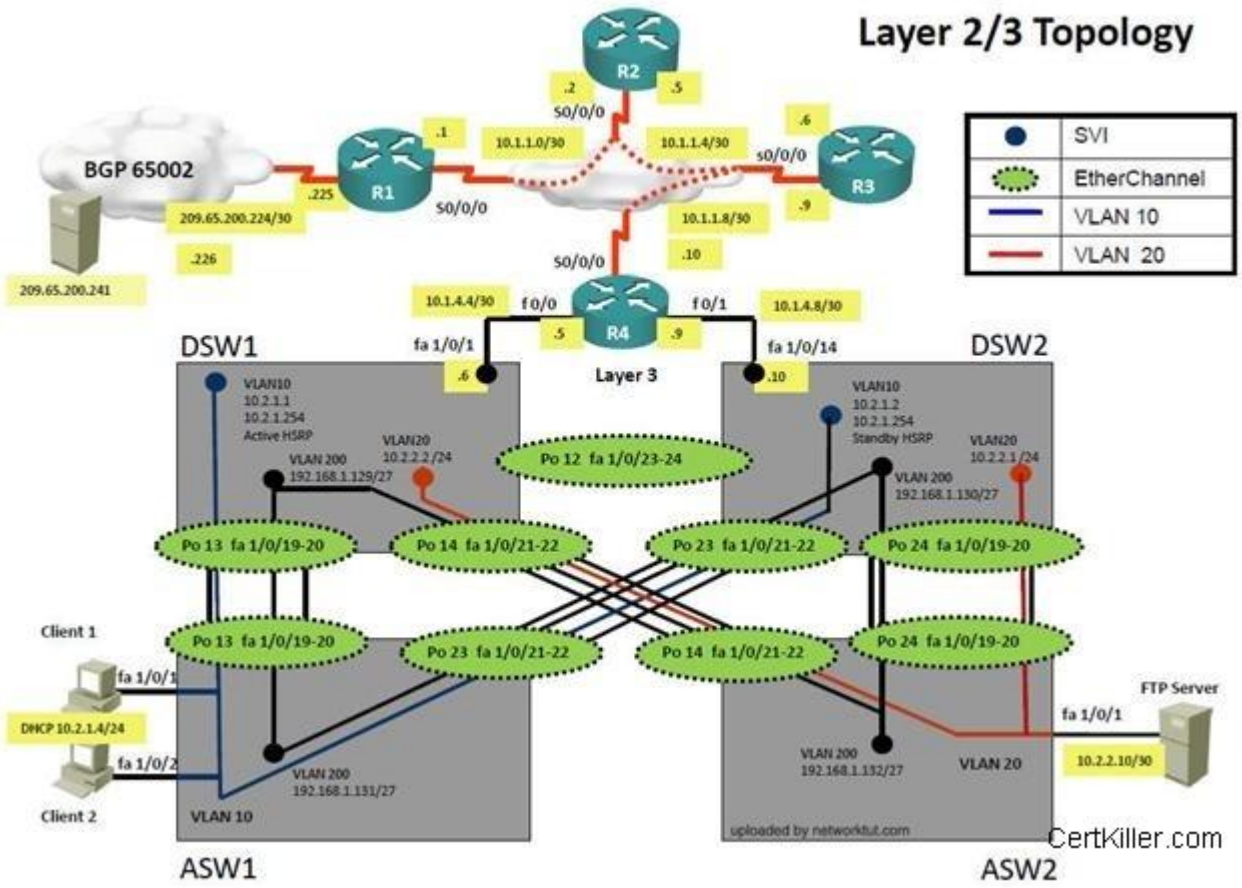


Figure 2

Trouble Ticket Statement

Client 1 and Client 2 are not able to reach the WebServer at 209.65.200.241. Initial troubleshooting shows that DSW1, DSW2 and all the routers are able to reach the WebServer

Configuration on R1

ip nat inside source list nat_pool interface Serial0/0/0/1 overload
!
ip access-list standard nat_pool

permit 10.1.0.0
!
interface Serial0/0/0/1
ip address 209.65.200.224 255.255.255.252
ip nat outside
!
interfaceSerial0/0/0/0.12
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip ospf message-digest-key 1 md5 TSHOOT
ip ospd authentication message-digest

What is the solution of the fault condition?

A. Add permit 10.2.0.0 statement in nat_pool access-list
B. Remove permit 10.1.0.0 statement from nat_pool access-list
C. Change ip nat inside source list nat_pool interface Serial0/0/0/1 overload to ip nat inside source list nat_pool interface Serial0/0/0/0.12 overload
D. Change ip nat outside statement under Serial0/0/0/1 configuration to ip nat inside

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: Add permit 10.2.0.0 statement in nat_pool access-list

Exam G

QUESTION 1
(Ticket 6: ACL)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

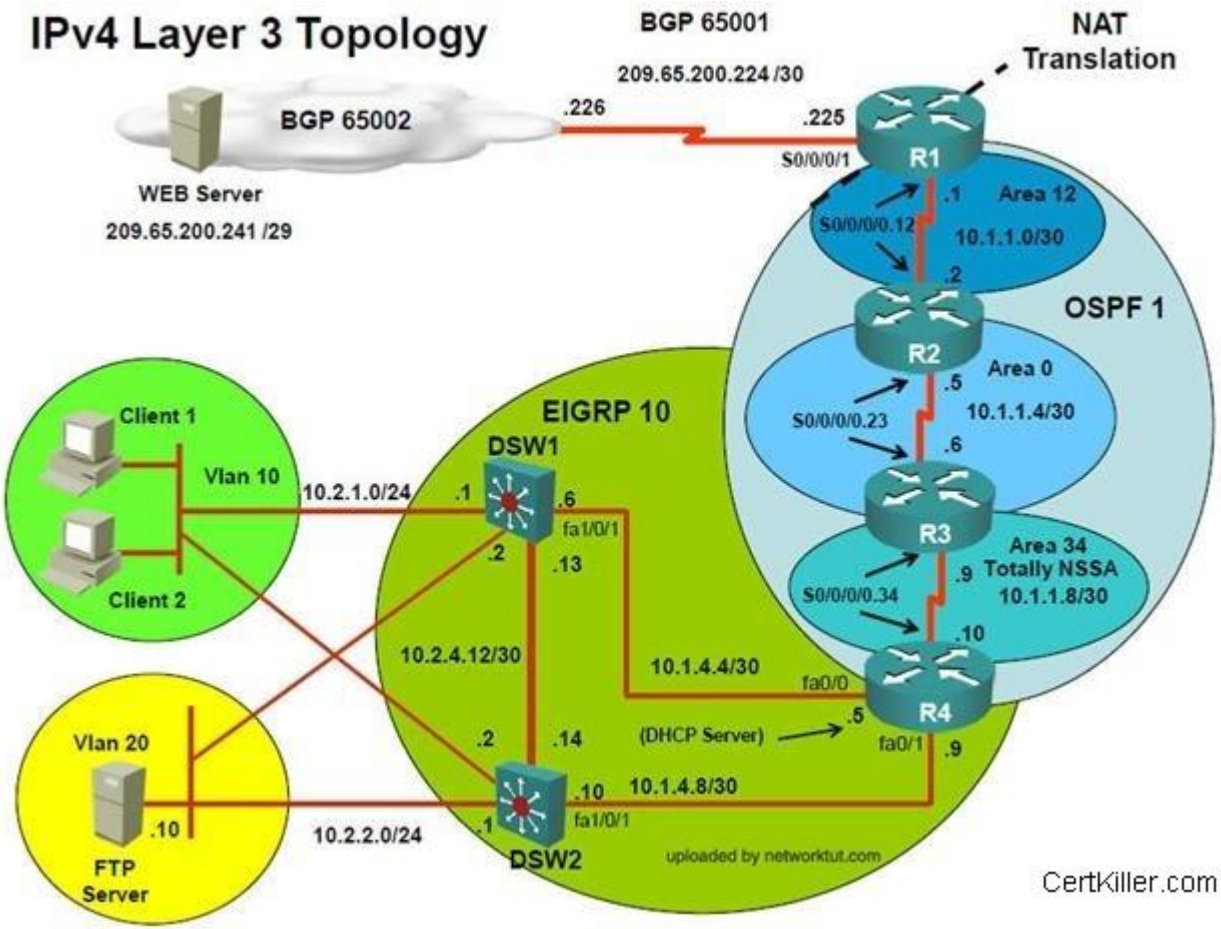


Figure 1

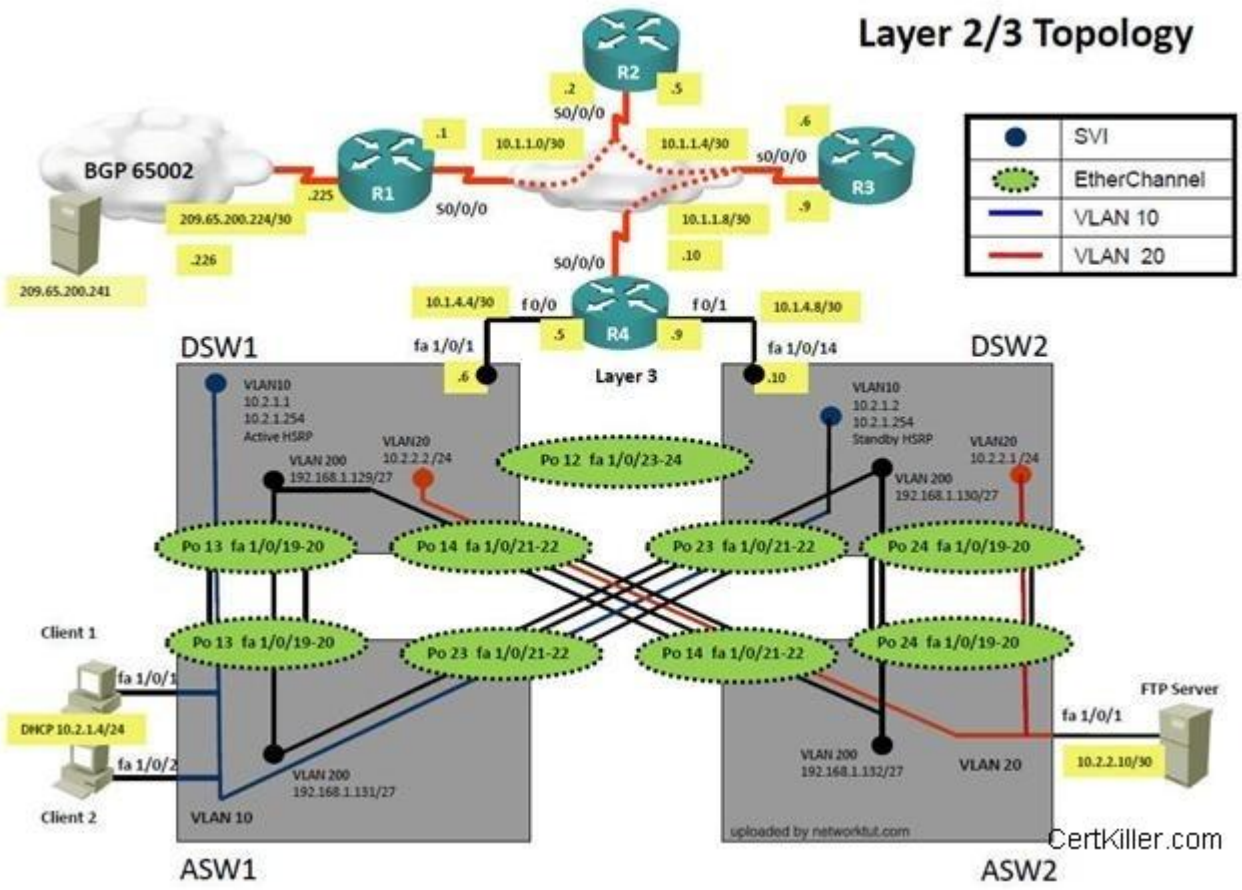
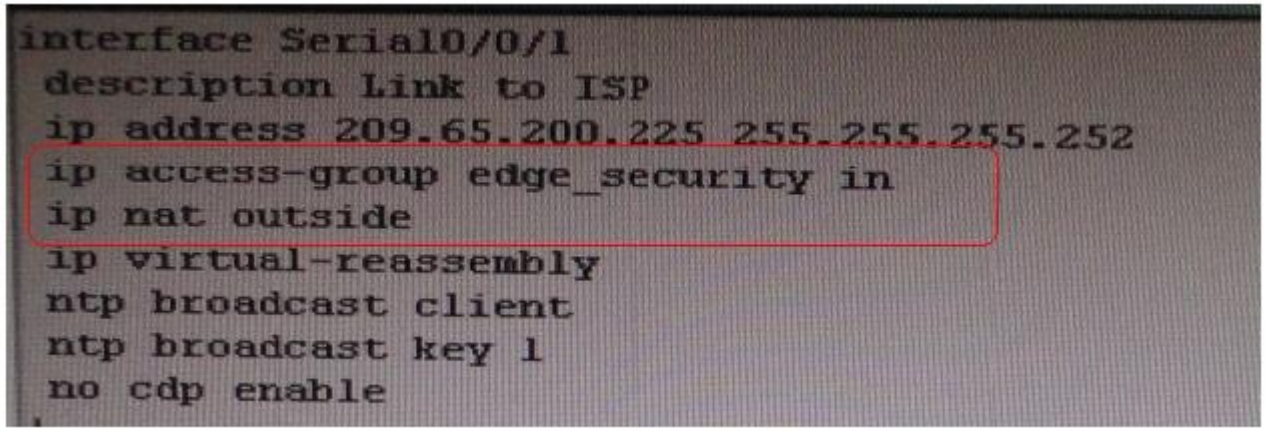
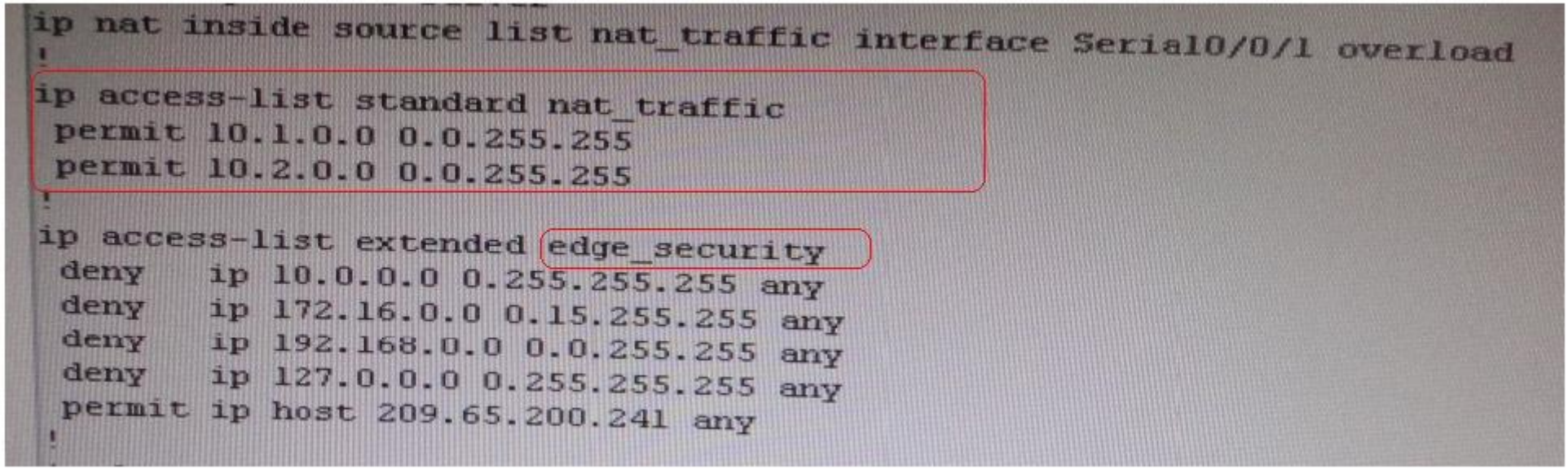


Figure 2

Trouble Ticket Statement

Configuration on R1





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: (none)
Explanation

Explanation/Reference:
Answer:
R1

QUESTION 2
(Ticket 6: ACL)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

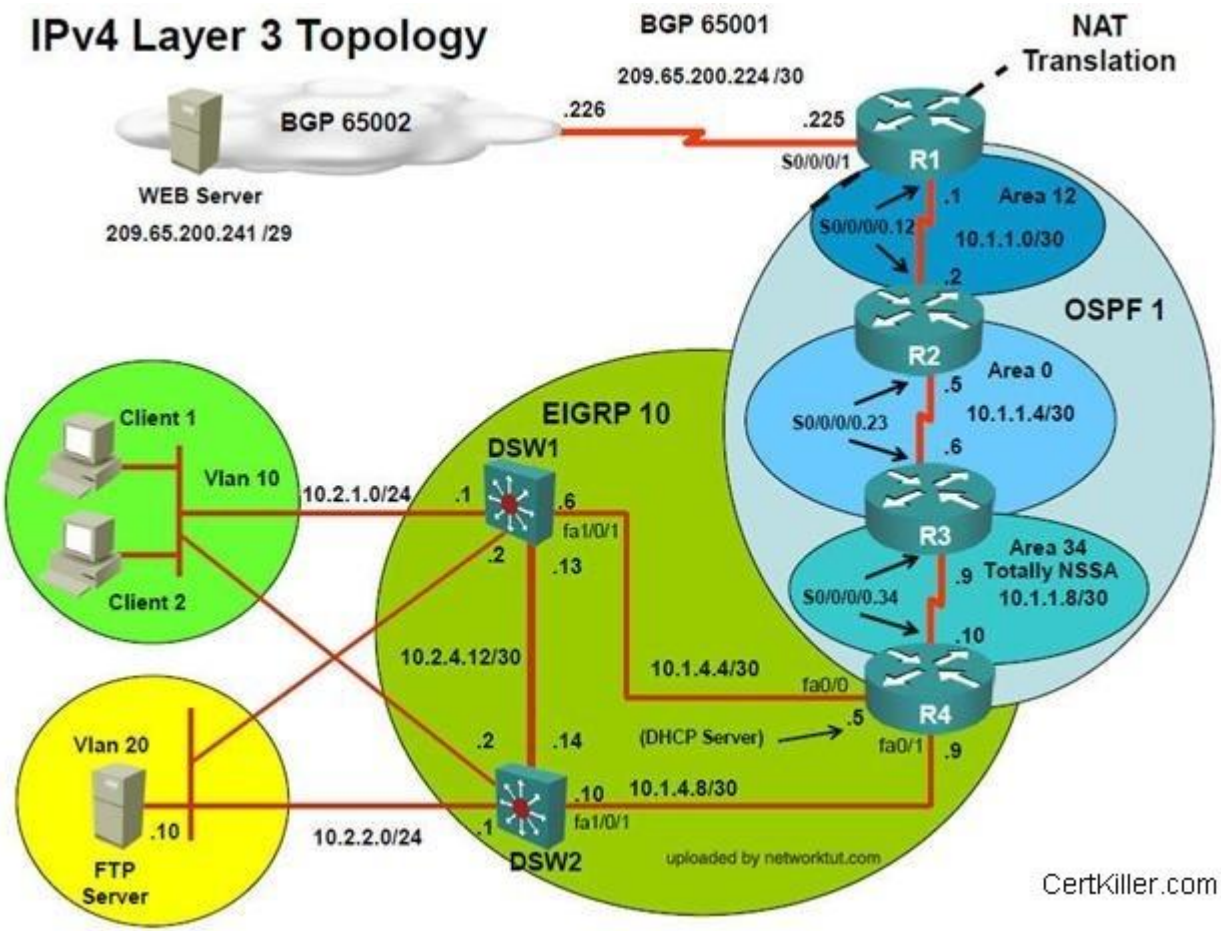

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.2
.13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

Figure 1

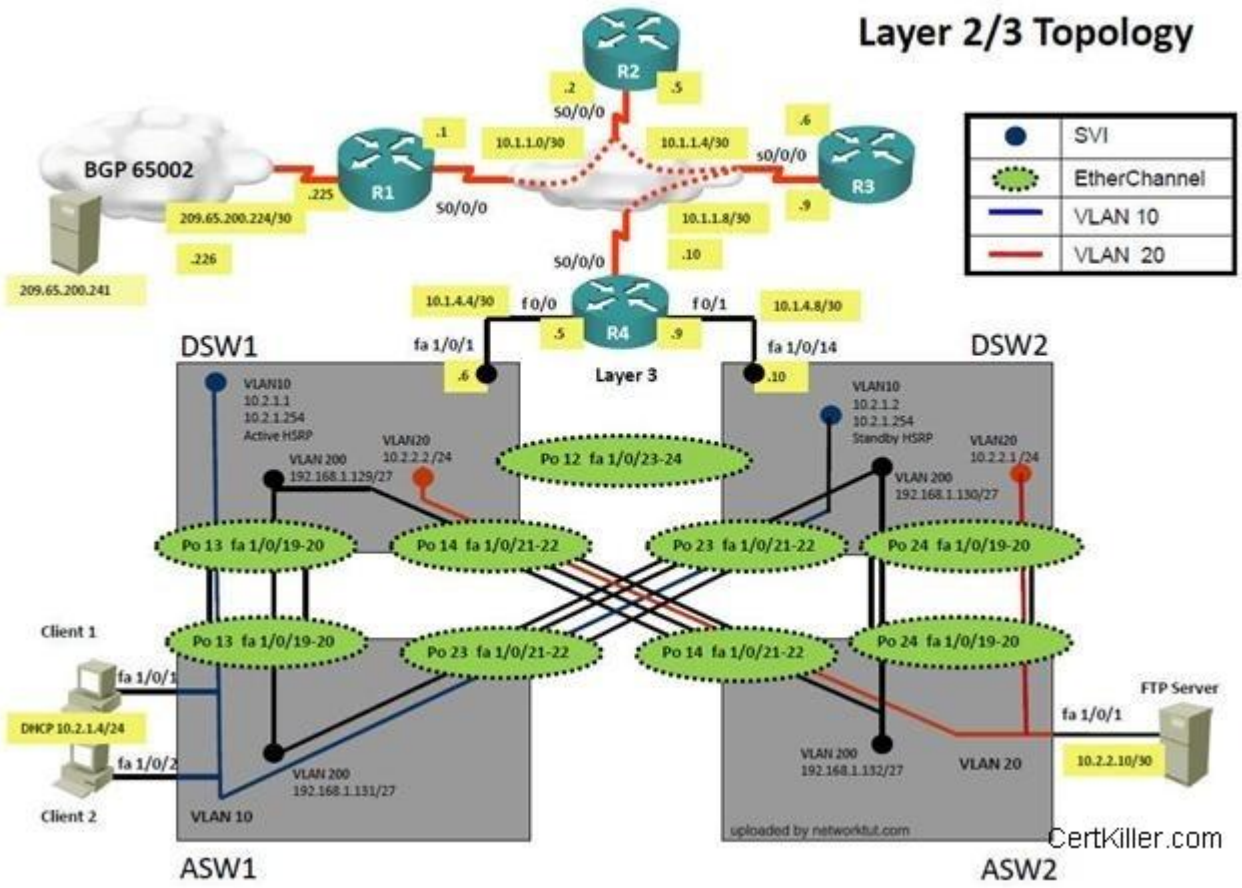


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer at 209.65.200.241. Initial troubleshooting shows that R1 is also not able to reach the WebServer. R1 also does not have any active BGP neighbor.

Config on R1

router bgp 65001
no synchronization
bgp log-neighbor-changes

```
network 209.65.200.224 mask 255.255.255.252
neighbor 209.65.200.226 remote-as 65002
no auto-summary
!
access-list 30 permit host 209.65.200.241
access-list 30 deny 10.1.0.0 0.0.255.255
access-list 30 deny 10.2.0.0 0.0.255.255
!
interface Serial0/0/0/1
ip address 209.65.200.224 255.255.255.252
ip nat outside
ip access-group 30 in
```

The Fault Condition is related to which technology?

A. IP Access
B. IP NAT
C. BGP
D. IP Access List
E. OSPF
F. Add permit statement for 209.65.200.224/30 network in access list 30

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: IP Access List

QUESTION 3
(Ticket 6: ACL)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

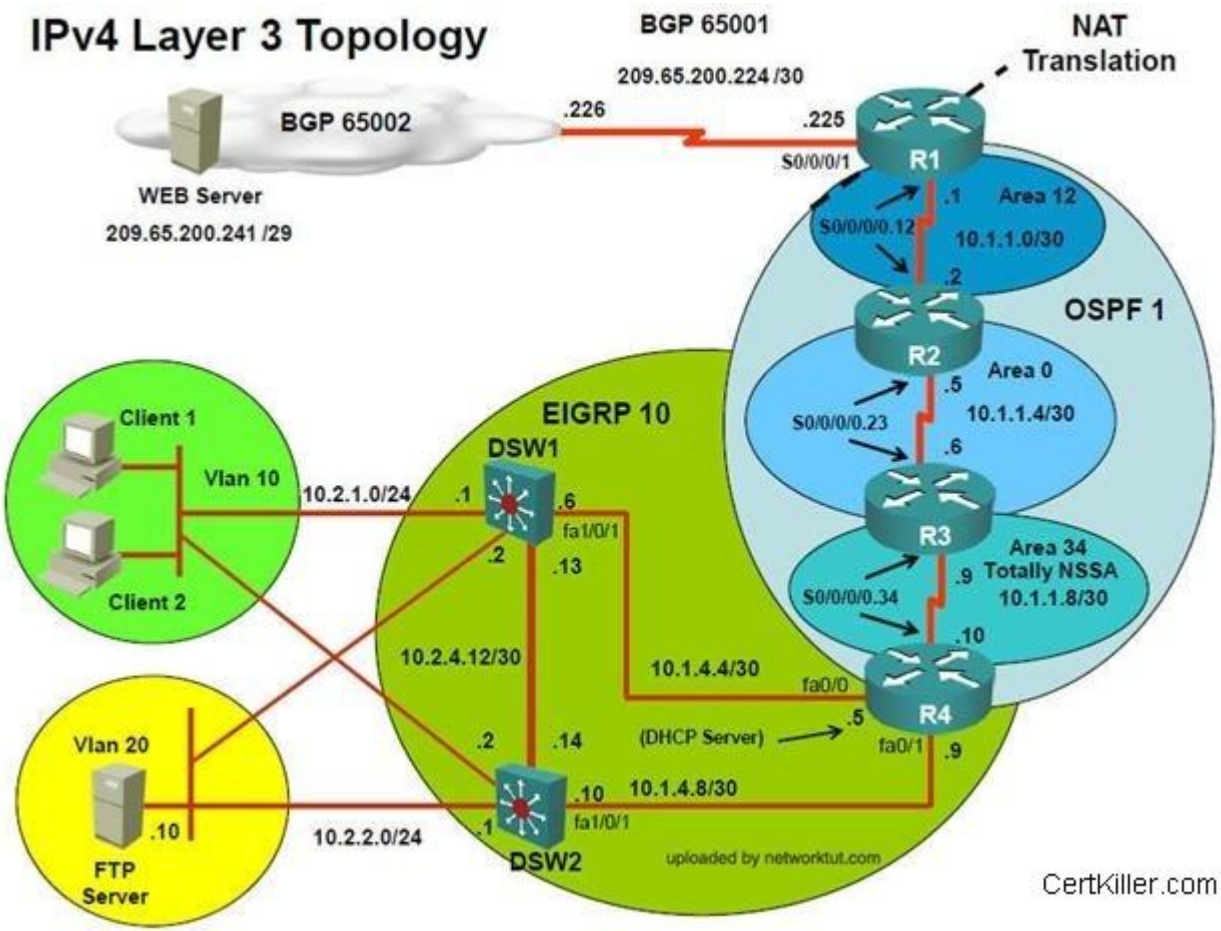


Figure 1

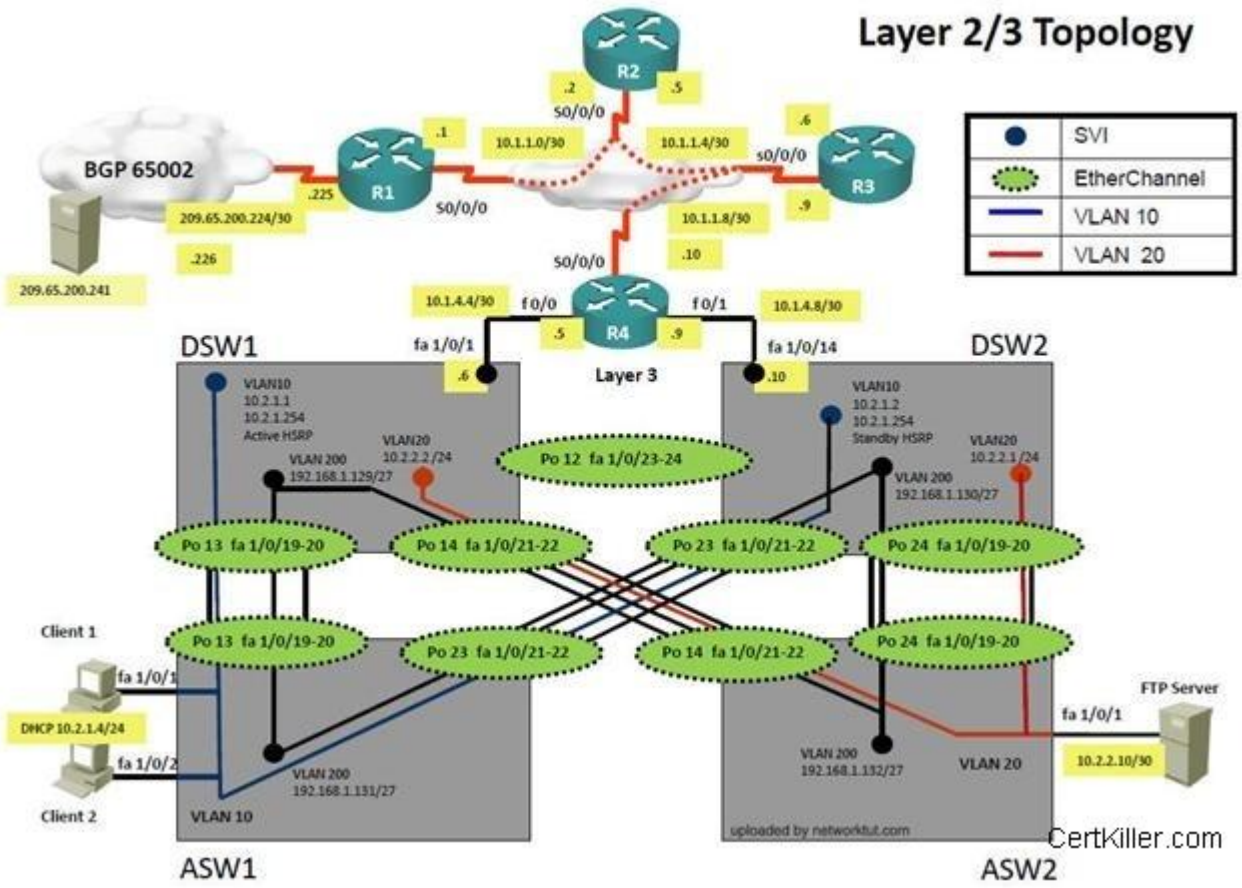


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer at 209.65.200.241. Initial troubleshooting shows that R1 is also not able to reach the WebServer. R1 also does not have any active BGP neighbor.

Config on R1

router bgp 65001
no synchronization
bgp log-neighbor-changes

```
network 209.65.200.224 mask 255.255.255.252
neighbor 209.65.200.226 remote-as 65002
no auto-summary
!
access-list 30 permit host 209.65.200.241
access-list 30 deny 10.1.0.0 0.0.255.255
access-list 30 deny 10.2.0.0 0.0.255.255
!
interface Serial0/0/0/1
ip address 209.65.200.224 255.255.255.252
ip nat outside
ip access-group 30 in
```

What is the solution of the fault condition?

A. Add permit statement for 209.65.200.224/30 network in access list 30
B. Remove Deny Statements from access-list 30
C. Change neighbor 209.65.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65001
D. Use extended access-list instead of standard access-list

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: Add permit statement for 209.65.200.224/30 network in access list 30

Exam H

QUESTION 1
(Ticket 7: Port Security)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

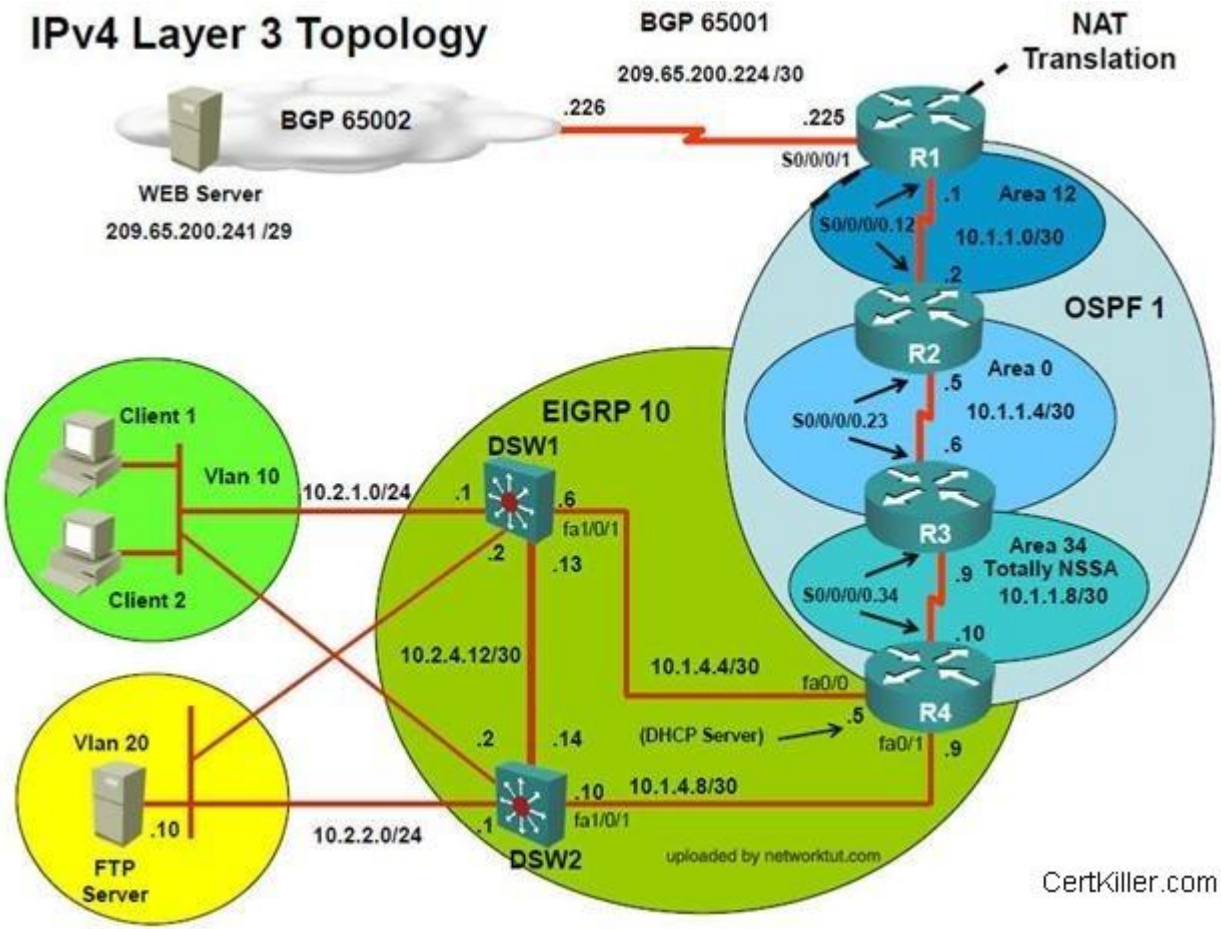


Figure 1

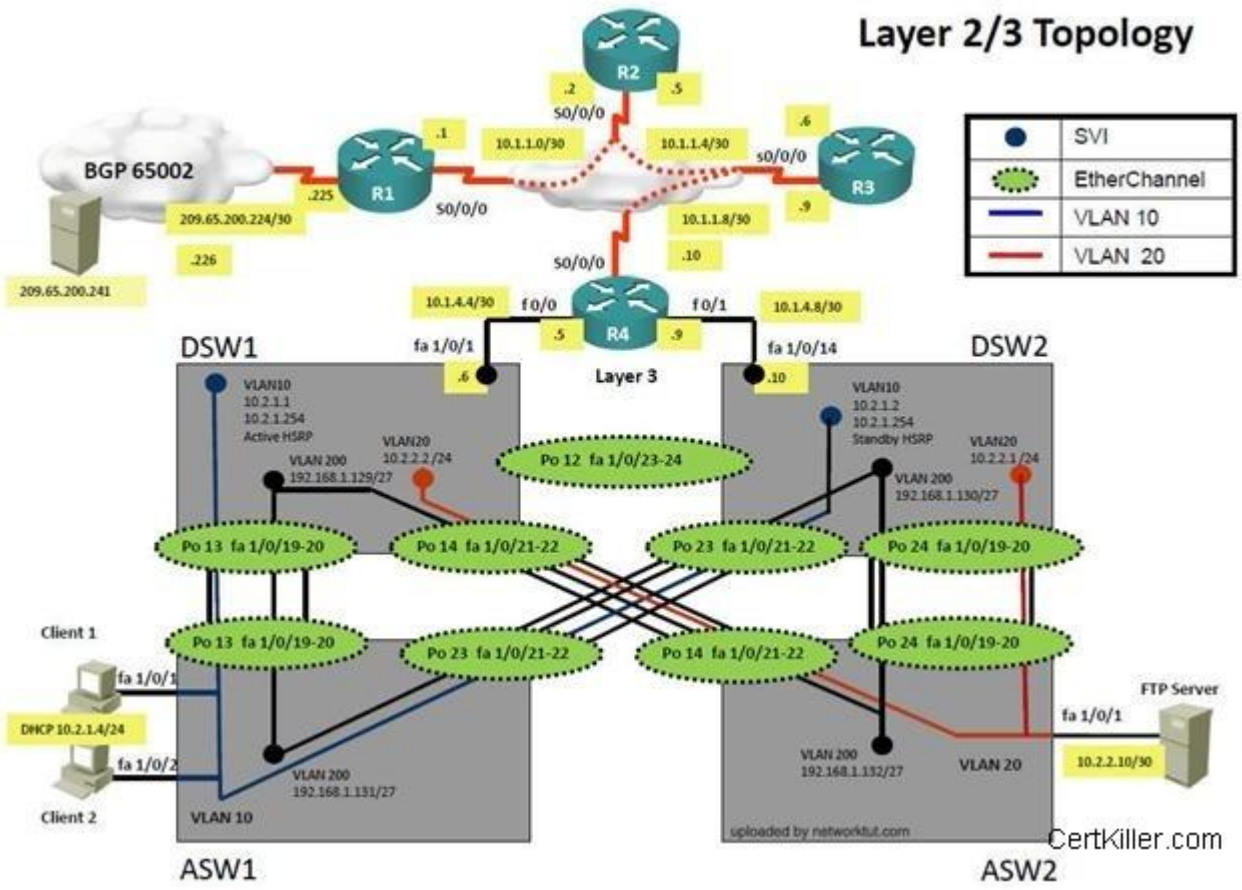


Figure 2

Trouble Ticket Statement

Client one is getting a 169.x.x.x IP address and is not able to ping Client 2 or DSW1. Inital troubleshooting shows that port Fa1/0/1 on ASW1 is in errdisable state.

Configuration on ASW1

Interface FastEthernet1/0/1

switchport mode access
switchport port-security
switchport port-security mac-address 0000.0000.0001

On which device is the fault condition located?

A. DSW1
B. ASW1
C. Client 1
D. FTP Server
E. ASW2
F. DSW2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: ASW1

QUESTION 2
(Ticket 7: Port Security)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

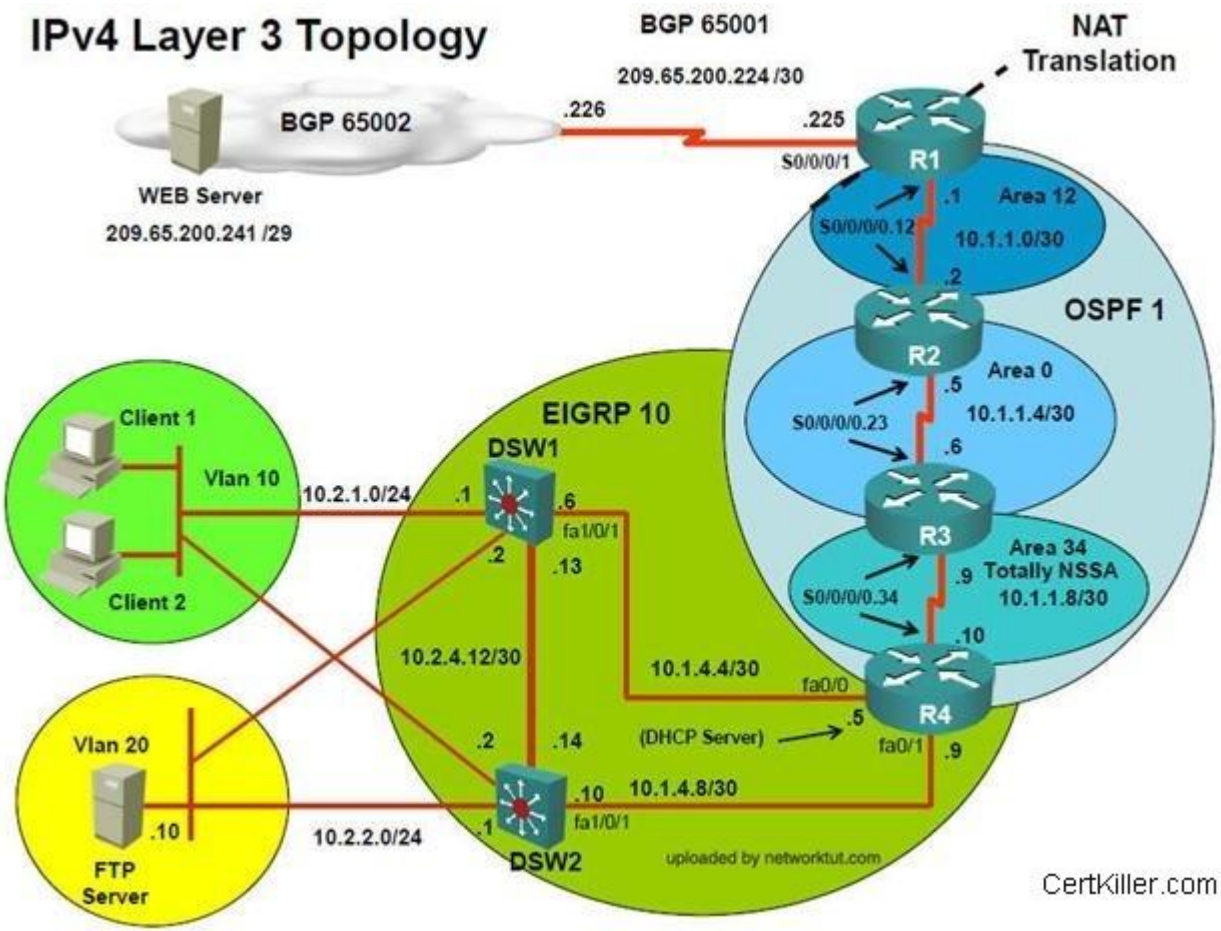


Figure 1

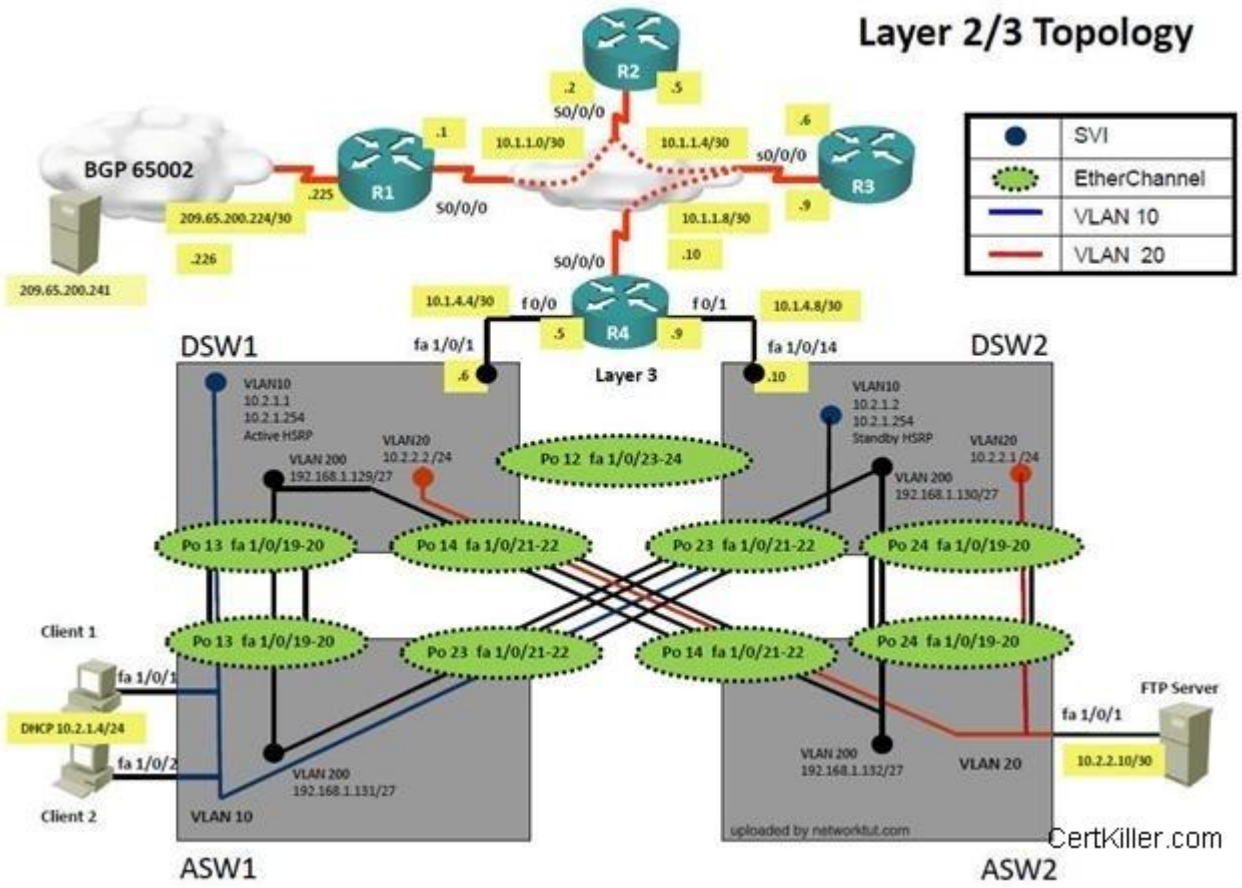


Figure 2

Trouble Ticket Statement

Client one is getting a 169.x.x.x IP address and is not able to ping Client 2 or DSW1. Inital troubleshooting shows that port Fa1/0/1 on ASW1 is in errdisable state.

Configuration on ASW1

Interface FastEthernet1/0/1
switchport mode access
CertKiller.com

switchport port-security
switchport port-security mac-address 0000.0000.0001

The Fault Condition is related to which technology?

A. VLAN Access Map
B. InterVLAN communication
C. DHCP
D. Port Security
E. ASW2
F. DSW1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: Port Security

QUESTION 3
(Ticket 7: Port Security)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

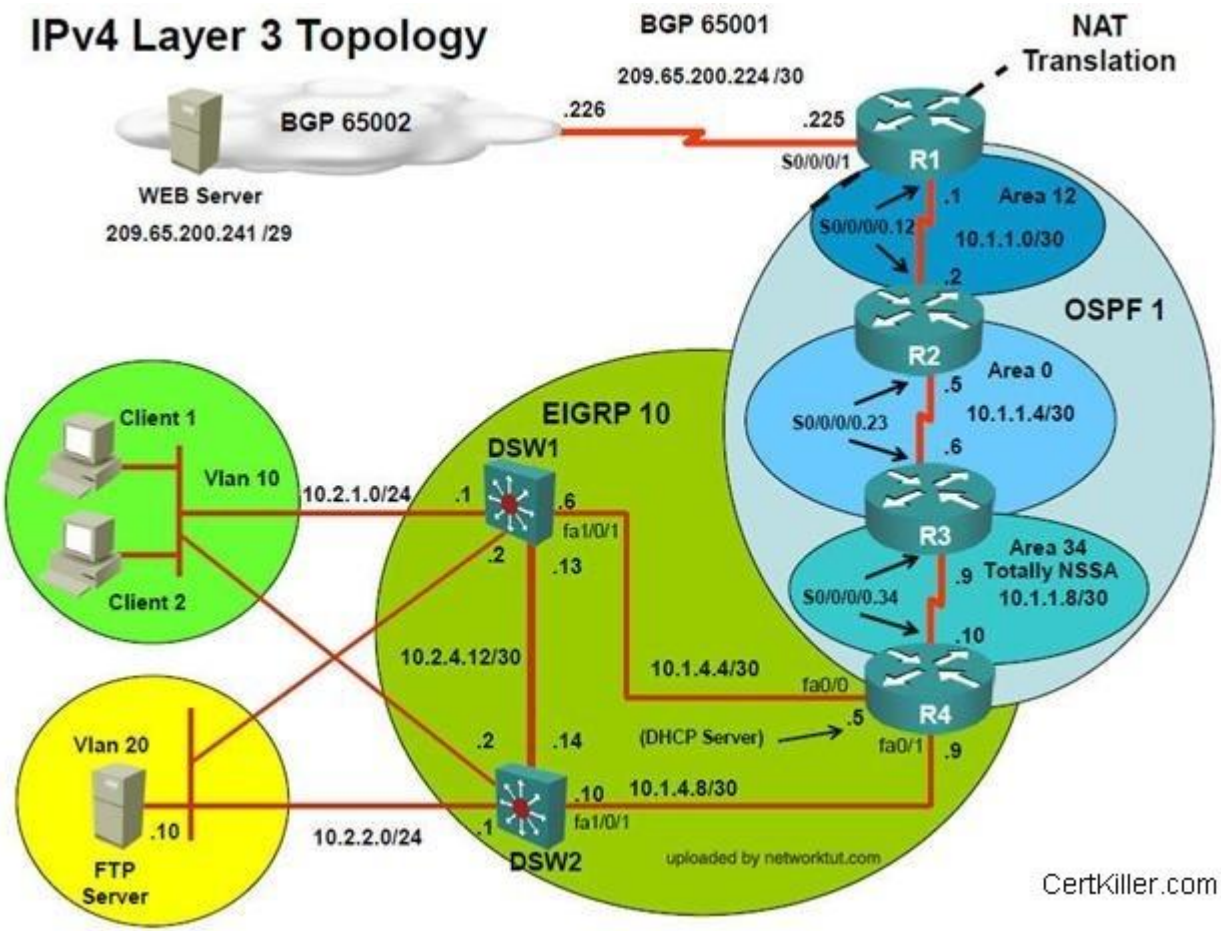


Figure 1

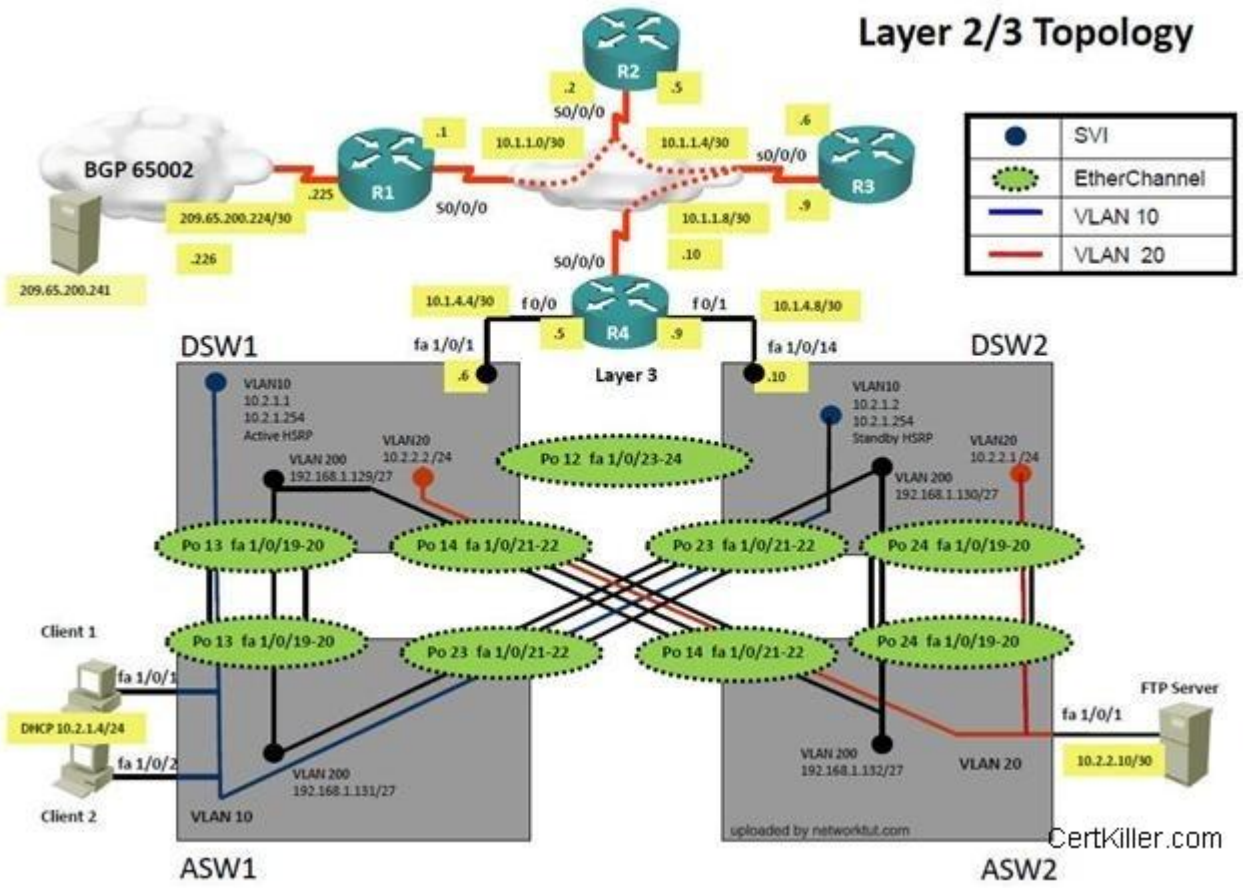


Figure 2

Trouble Ticket Statement

Client one is getting a 169.x.x.x IP address and is not able to ping Client 2 or DSW1. Inital troubleshooting shows that port Fa1/0/1 on ASW1 is in errdisable state.

Configuration on ASW1

Interface FastEthernet1/0/1
switchport mode access
switchport port-security

switchport port-security mac-address 0000.0000.0001

What is the solution of the fault condition?

A. Configurationure Static IP Address on Client 1
B. Change the IP Address of VLAN 10 on DSW1
C. Issue shutdown command followed by no shutdown command on port fa1/0/1 on ASW1
D. Issue no switchport port-security mac-address 0000.0000.0001 command followed by shutdown and no shutdown command on port fa1/0/1 on ASW1
E. Issue no switchport port-security mac-address 0000.0000.0001 command on port fa1/0/1 on ASW1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: Issue no switchport port-security mac-address 0000.0000.0001 command followed by shutdown and no shutdown command on port fa1/0/1 on ASW1

Exam I

QUESTION 1
(Ticket 8: Redistribution of EIGRP to OSPF)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

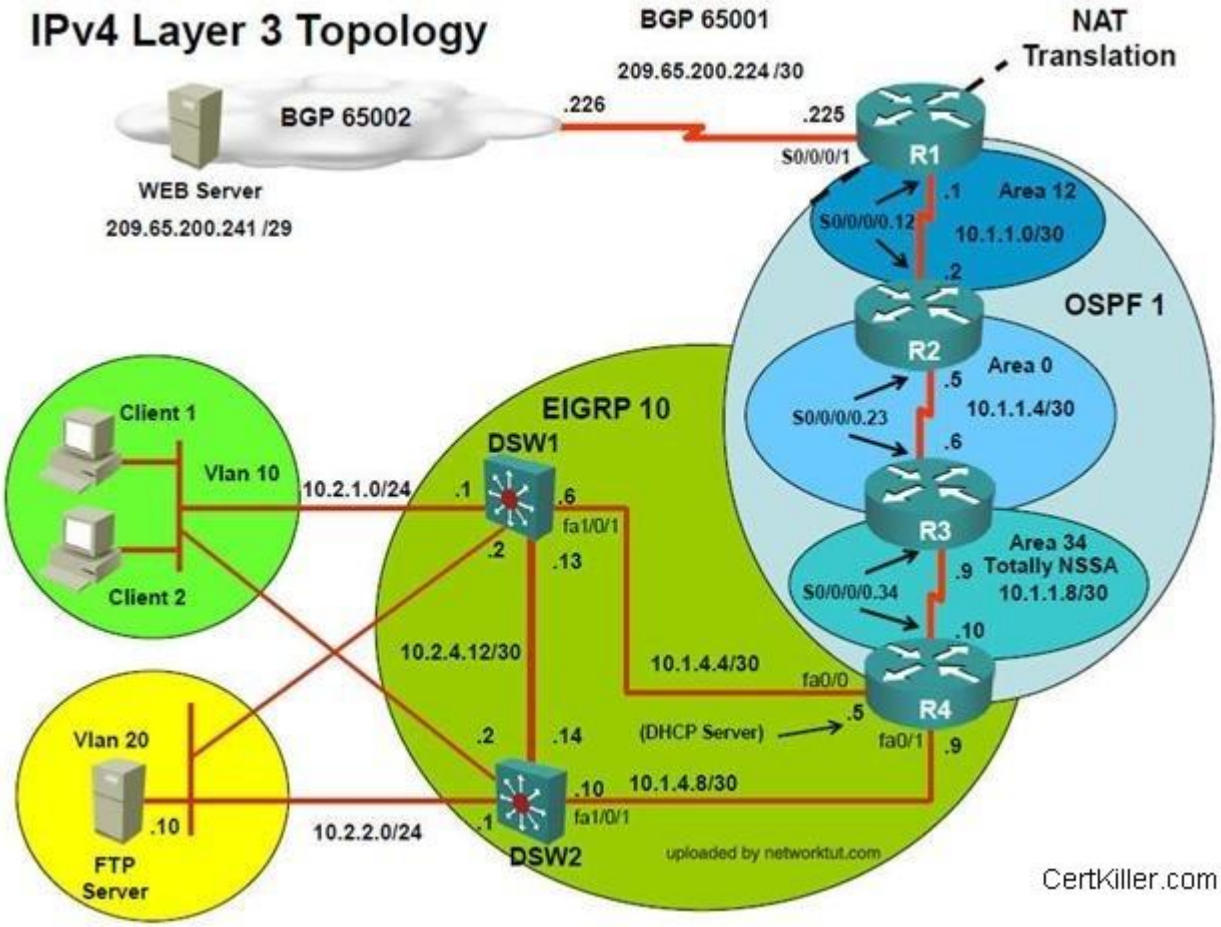


Figure 1

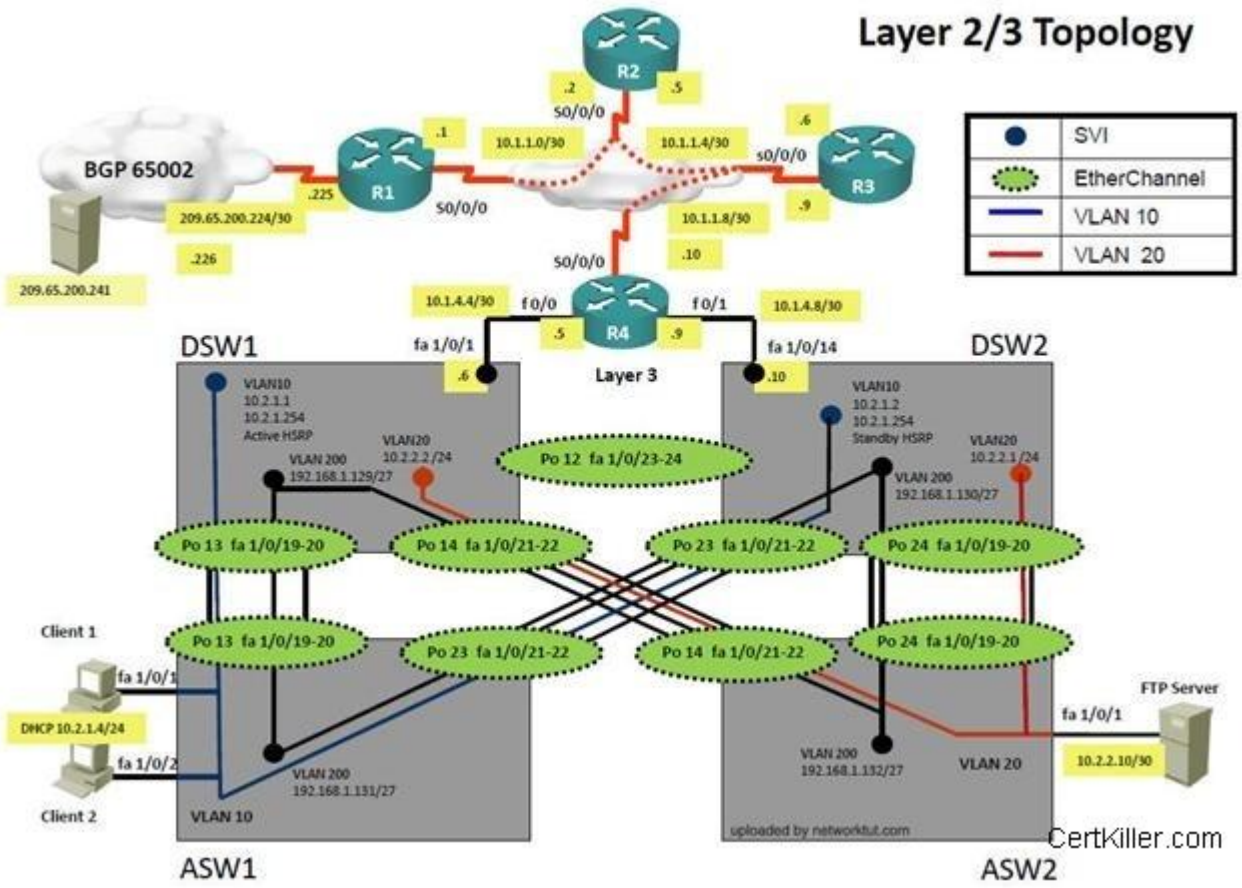


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer. Initial troubleshooting shows that DSW1 can ping the Fa0/1 interface of R4 but not the s0/0/0/0.34 interface.

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0

no auto-summary

Configuration on DSW2

router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary

Configuration on R4

router eigrp 10
network 10.1.4.5 0.0.0.0
no auto-summary
redistribute ospf 1 metric 100 10 255 1 1500 route-map OSPF_to_EIGRP
!
router ospf 1
network 10.1.1.8 0.0.0.0 area 34
redistribute eigrp 10 subnets
!
route-map OSPF->EIGRP
match ip address 1
!
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 1 permit 209.0.0.0 0.255.255.255

What is the solution of the fault condition?

A. DSW1
B. DSW2
C. Client 1
D. Client 2
E. R4

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Answer: R4

QUESTION 2
(Ticket 8: Redistribution of EIGRP to OSPF)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

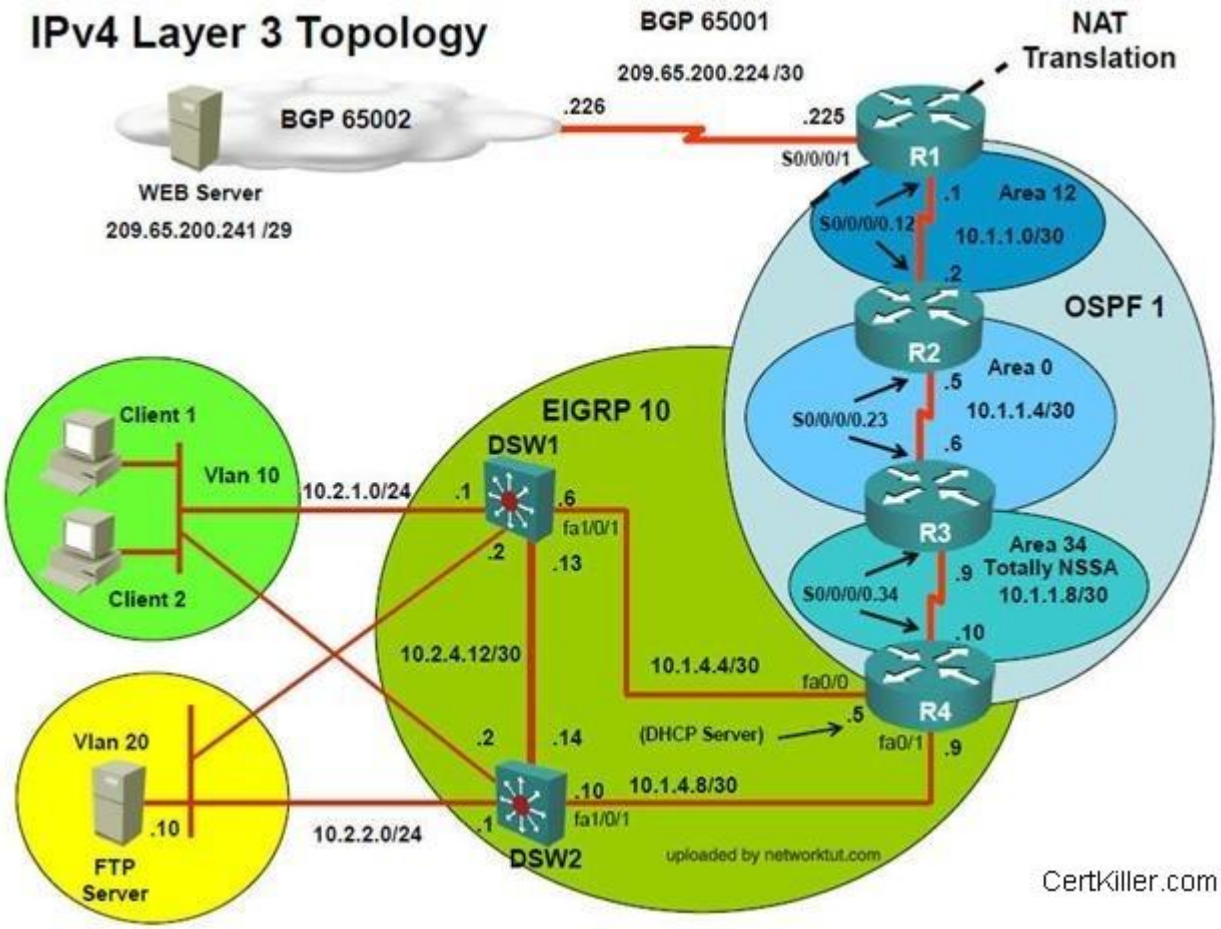


Figure 1

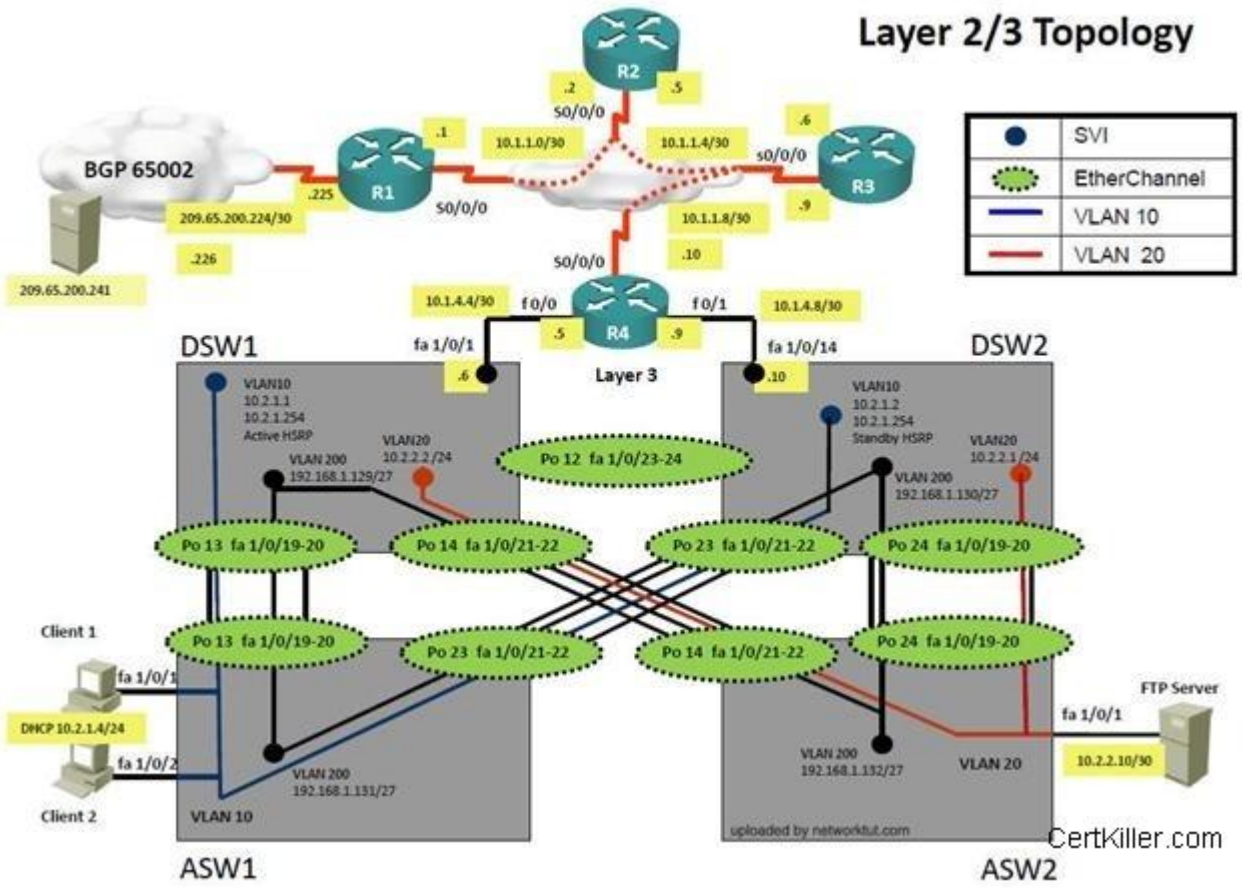


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer. Initial troubleshooting shows that DSW1 can ping the Fa0/1 interface of R4 but not the s0/0/0/0.34 interface.

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0

no auto-summary

Configuration on DSW2

router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary

Configuration on R4

router eigrp 10
network 10.1.4.5 0.0.0.0
no auto-summary
redistribute ospf 1 metric 100 10 255 1 1500 route-map OSPF_to_EIGRP
!
router ospf 1
network 10.1.1.8 0.0.0.0 area 34
redistribute eigrp 10 subnets
!
route-map OSPF->EIGRP
match ip address 1
!
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 1 permit 209.0.0.0 0.255.255.255

The Fault Condition is related to which technology?

A. EIGRP
B. Route Redistribution
C. OSPF
D. IP Addressing
E. HSRP
F. BGP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: Route Redistribution

QUESTION 3
(Ticket 8: Redistribution of EIGRP to OSPF)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

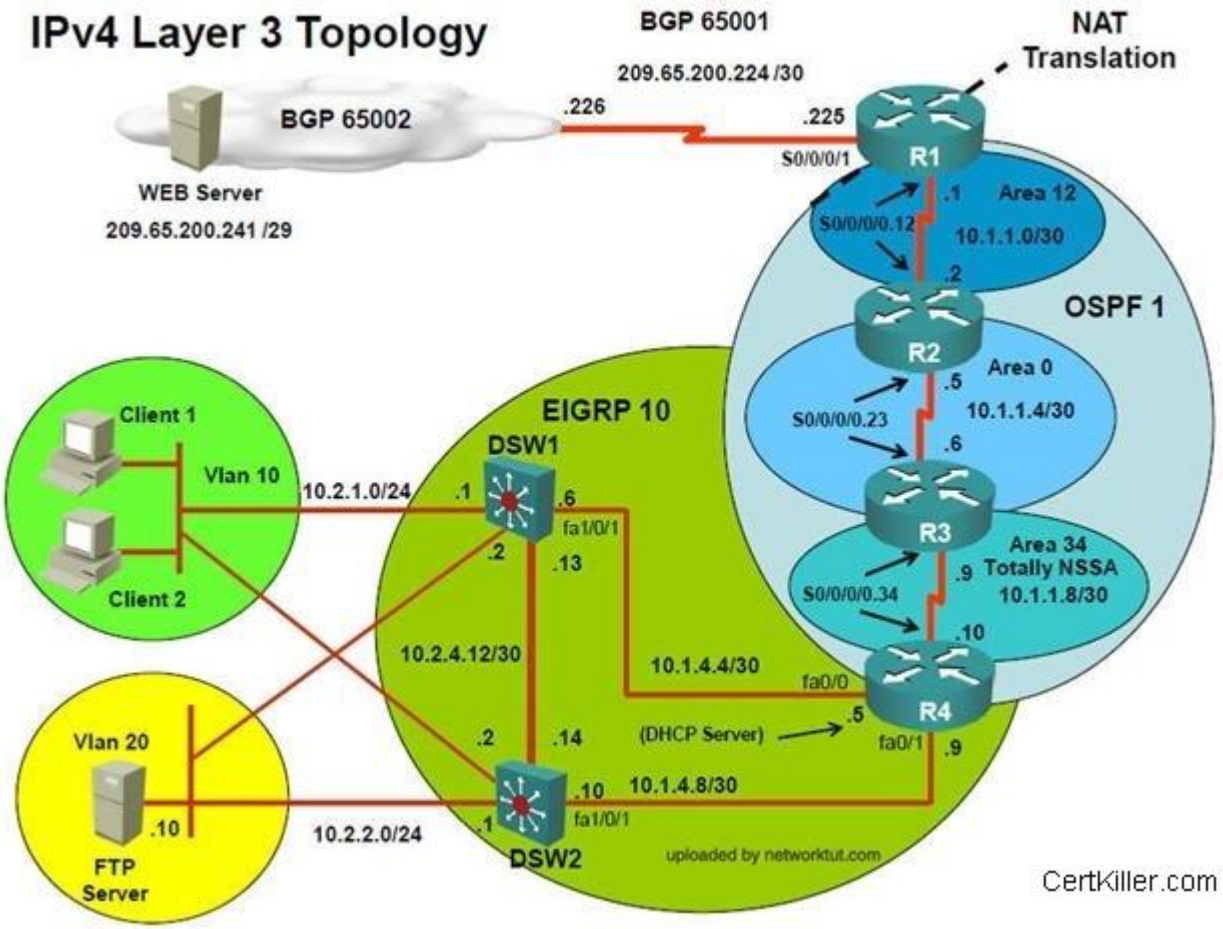


Figure 1

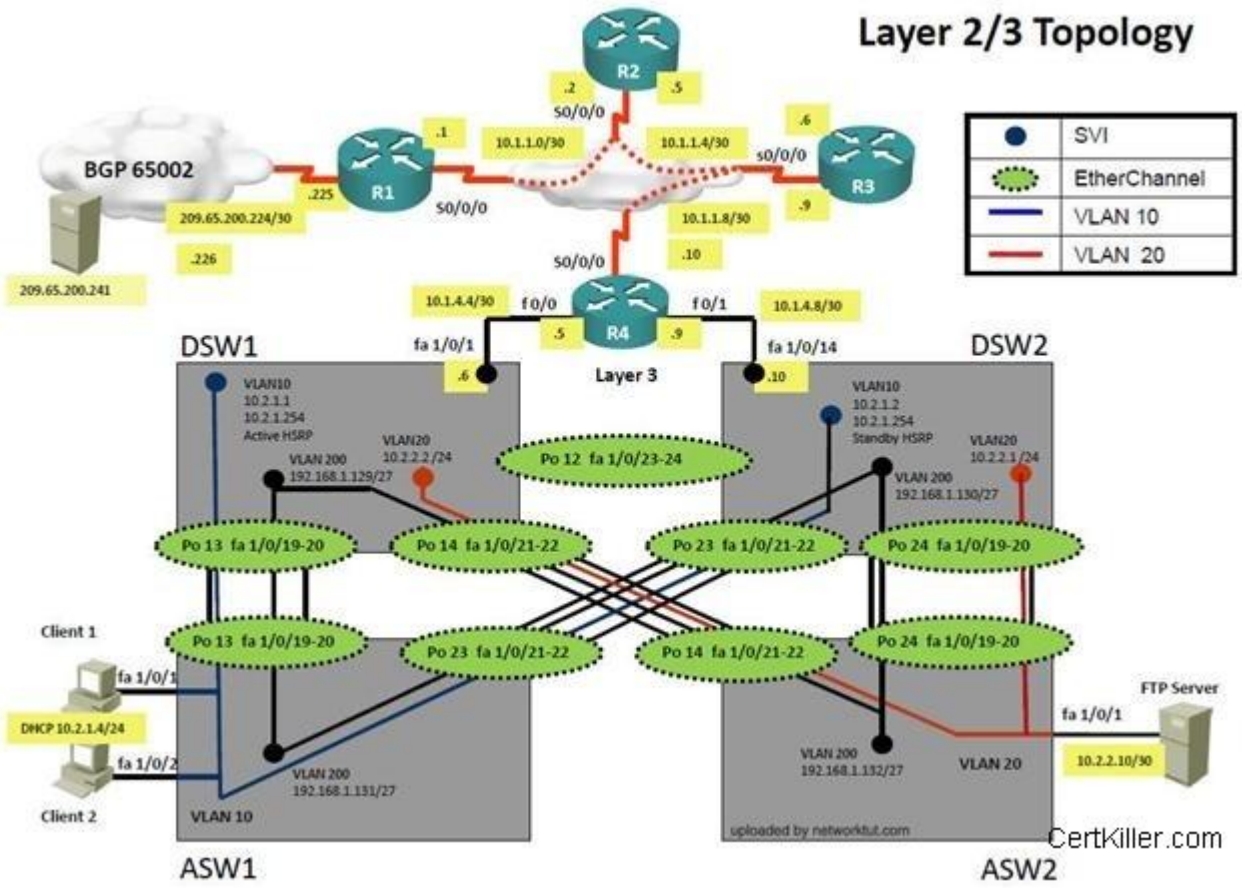
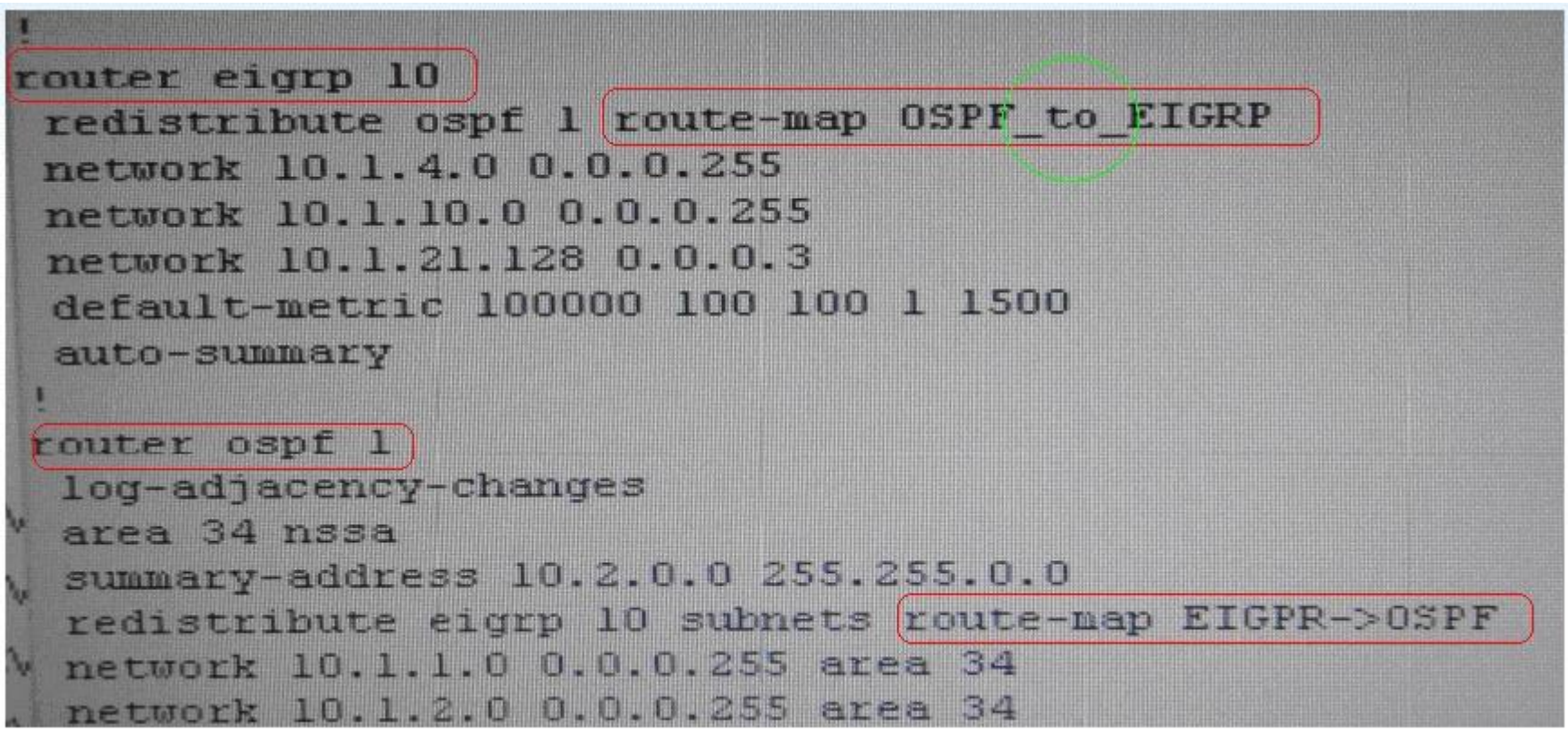
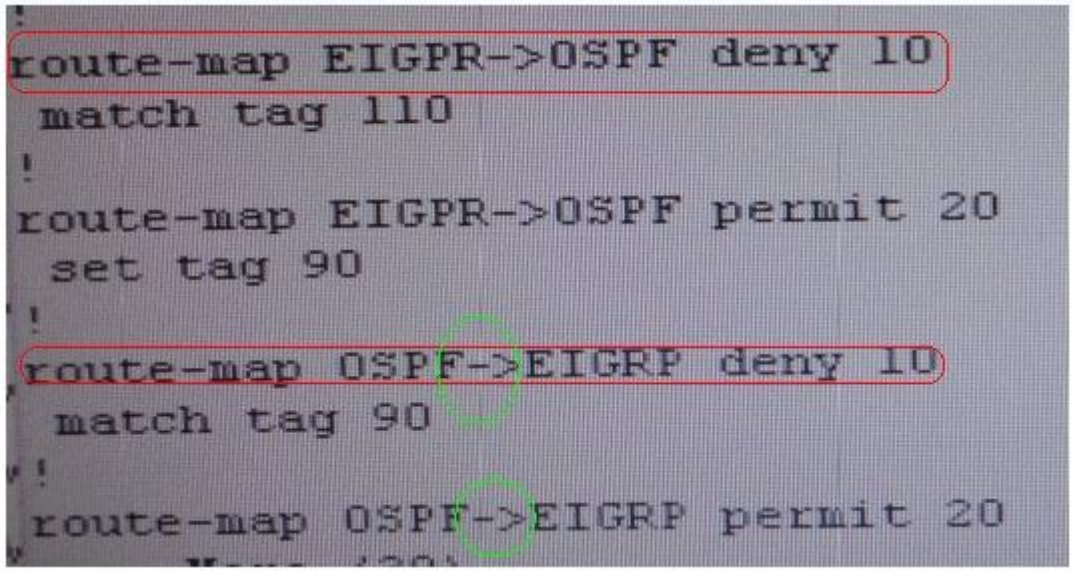


Figure 2

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

Configuration on R4


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



What 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 EIGRP process, delete the redistribute EIGRP 10 subnets route-map EIGRP->OSPF command and enter the redistribute eigrp 10 subnets route-map OSPF->EIGRP command.
D. Under the EIGRP process, delete the redistribute EIGRP 10 subnets route-map EIGRP->OSPF command and enter the redistribute eigrp 10 subnets route-map EIGRP->OSPF command.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer:
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.

Exam J

QUESTION 1
(Ticket 9: VLAN Access Map)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

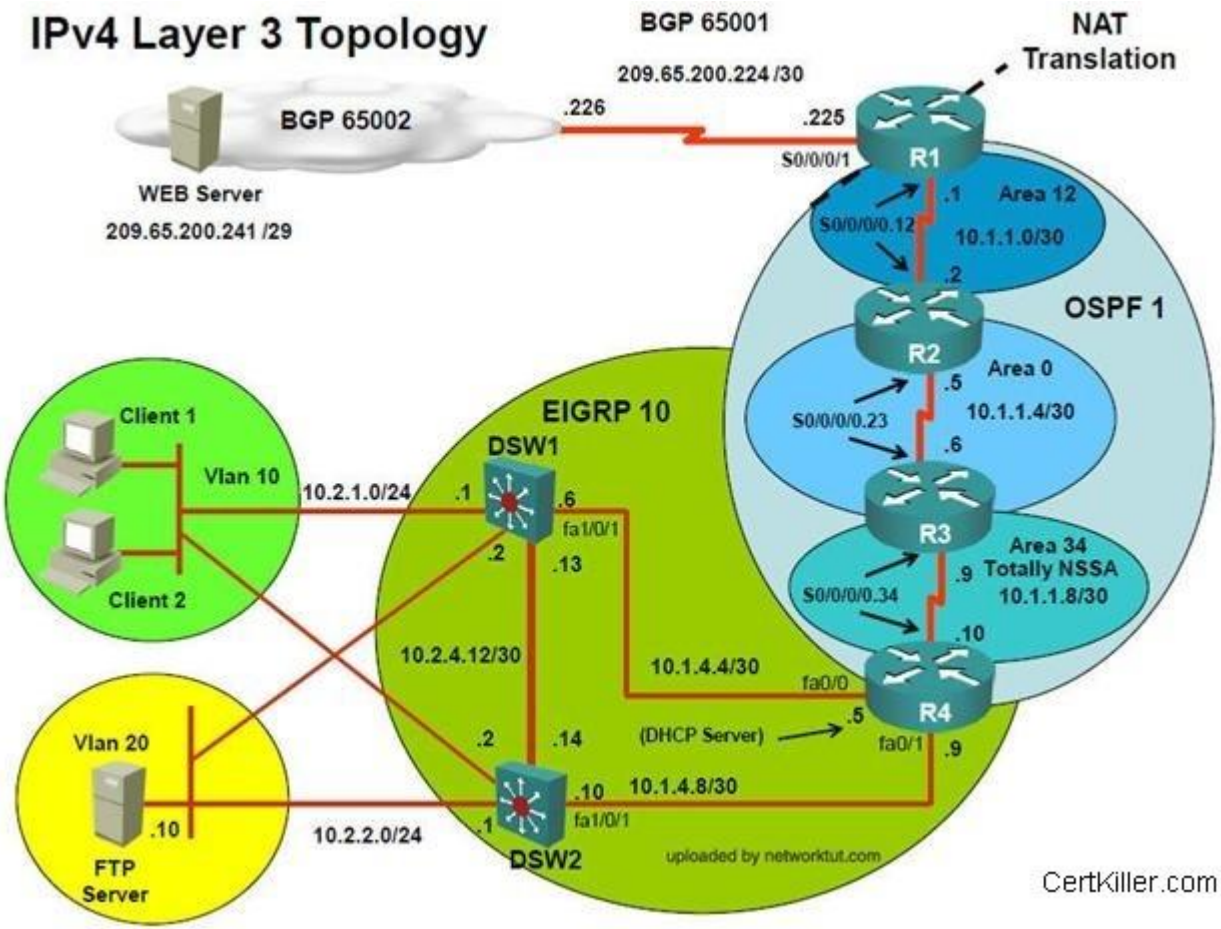


Figure 1

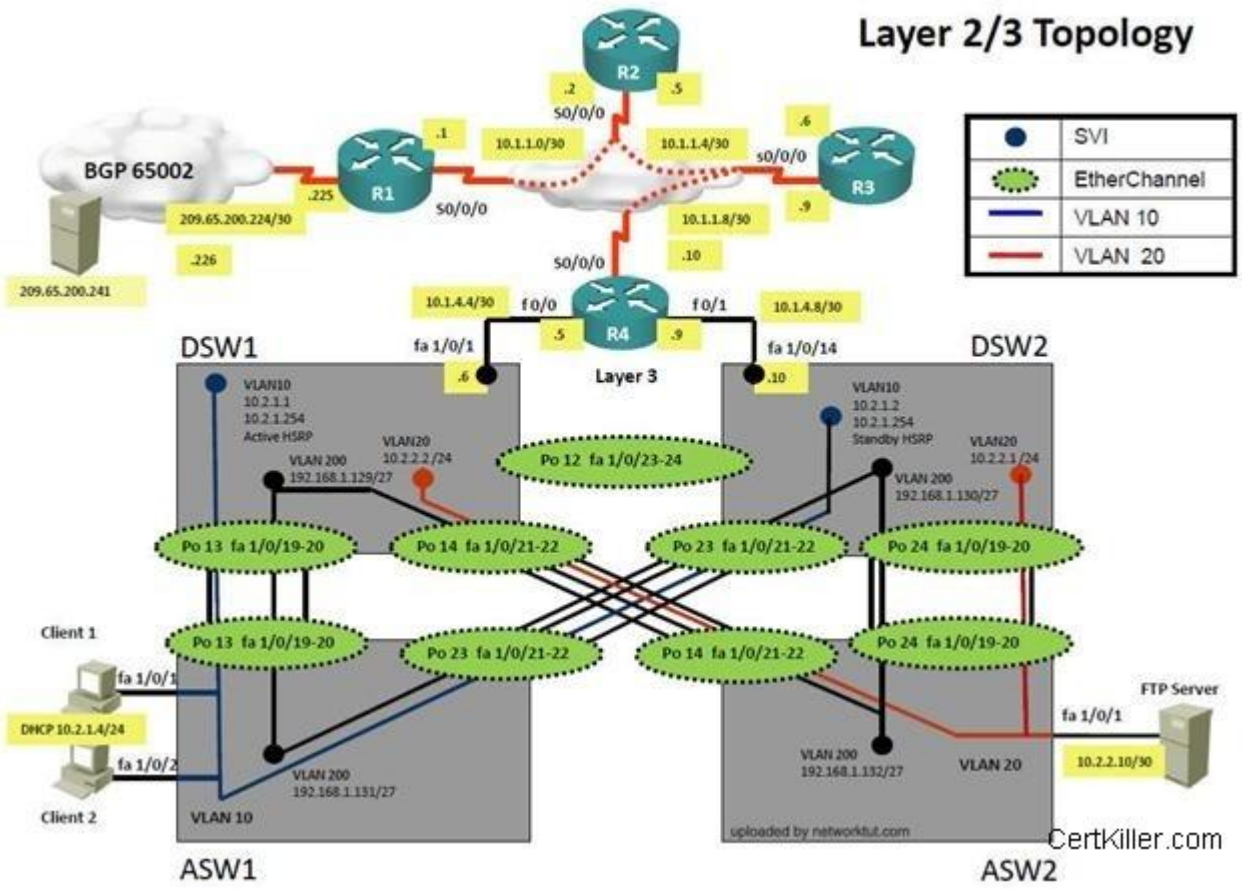


Figure 2

Trouble Ticket Statement

Client 1 is getting an IP address from the DHCP server but is not able to ping DSW1 or the FTP

Server

Configuration on DSW1

vlan access-map test1 10

```
drop
match ip address 10
!
vlan filter test1 vlan-list 10
!
ip access-list standard 10
permit 10.2.0.0 0.0.255.255
!
Interface VLAN10
ip address 10.2.1.1 255.255.255.0
!
```

On which device is the fault condition located?

A. R4
B. DSW1
C. Client 1
D. FTP Server
E. DSW2
F. R1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer: DSW1

QUESTION 2
(Ticket 10: VLAN Access Map)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

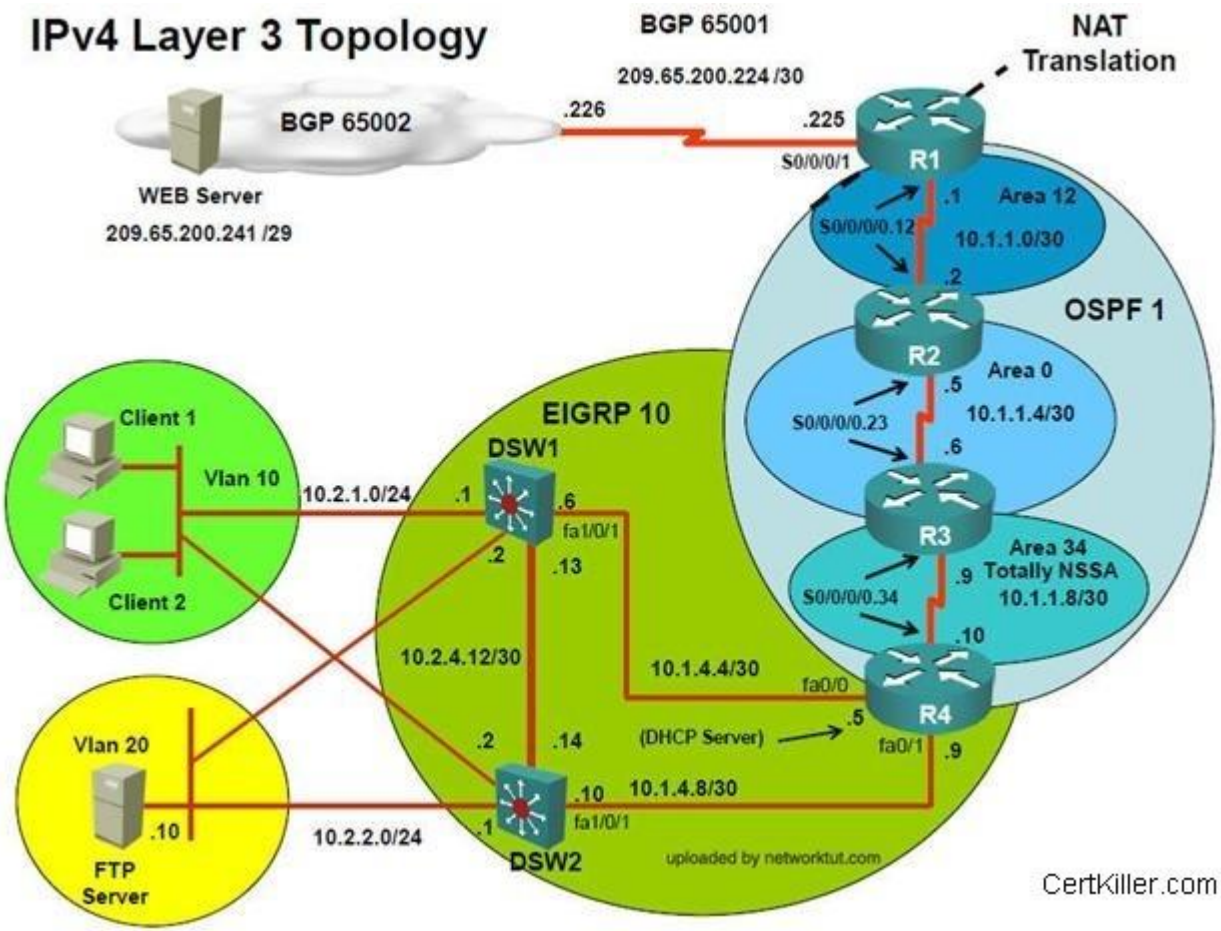

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

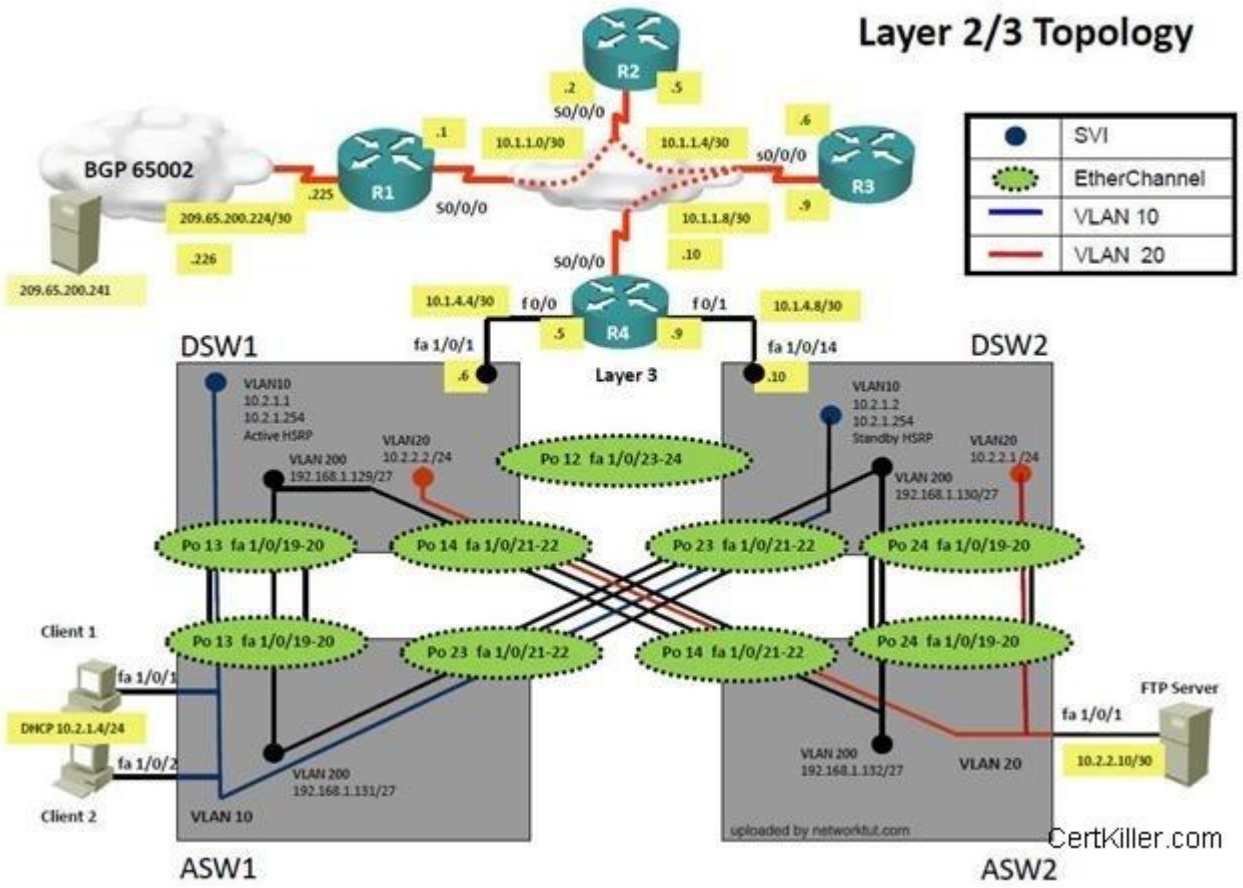


Figure 2

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

Configuration on DSW1

DSW1
vlan access-map test1 10
 action drop
 match ip address 10
vlan access-map test1 20
 action drop

```
 match ip address 20
vlan access-map test1 30
 action foward
 match ip address 30
vlan access-map test1 40
 action foward
!
vlan filter test1 vlan-list 10
vlan internal allocation policy asdending
!
access-list 10 permit 10.2.1.3
access-list 20 permit 10.2.1.4
access-list 30 permit 10.2.1.0 0.0.0.255
```

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: (none)
Explanation

Explanation/Reference:
Notice: After choosing DSW1 for Ans1, next page (for Ans2) you have to scroll down to find the VLAN ACL/Port ACL option. The scroll bar only appears in this ticket and is very difficult to be seen.

QUESTION 3
(Ticket 10: VLAN Access Map)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

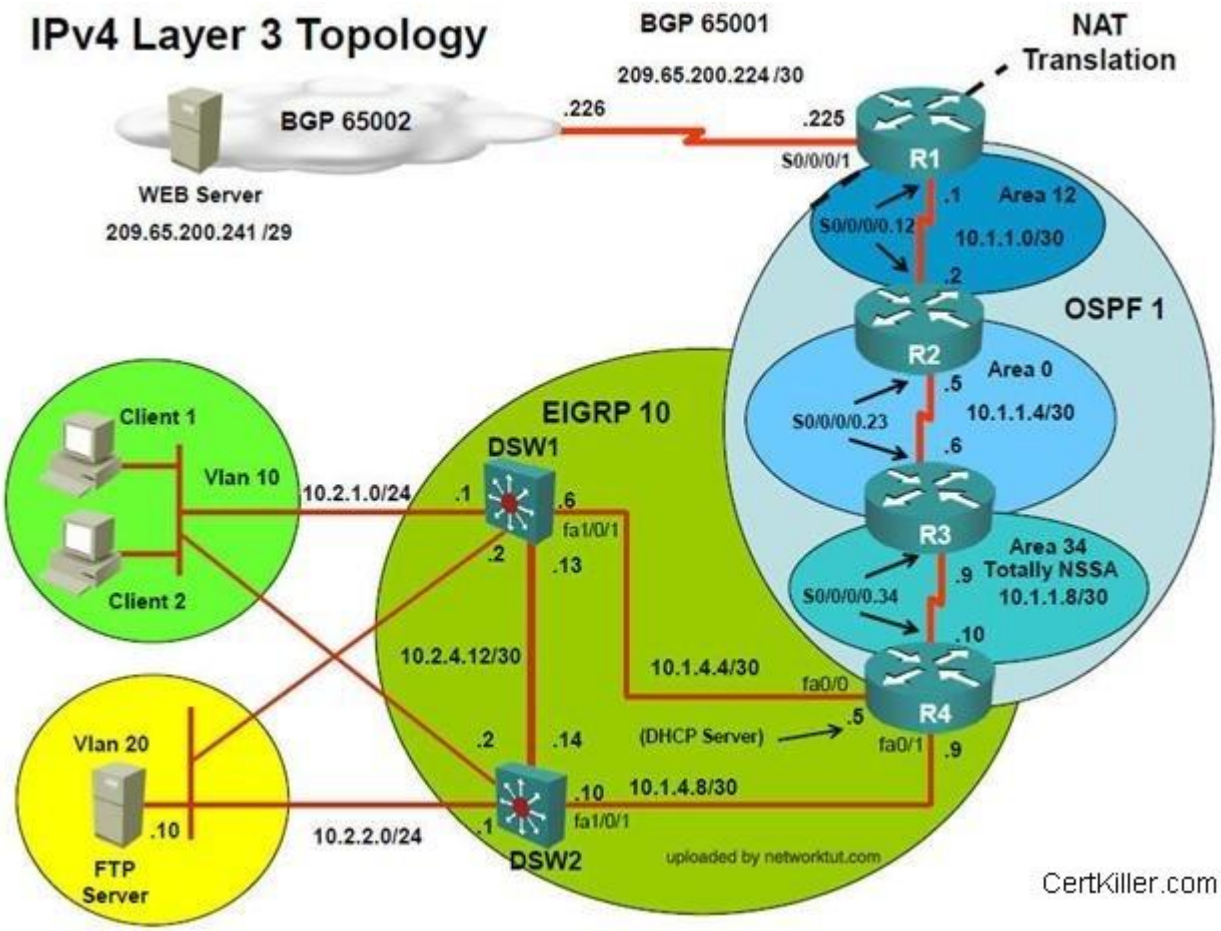


Figure 1

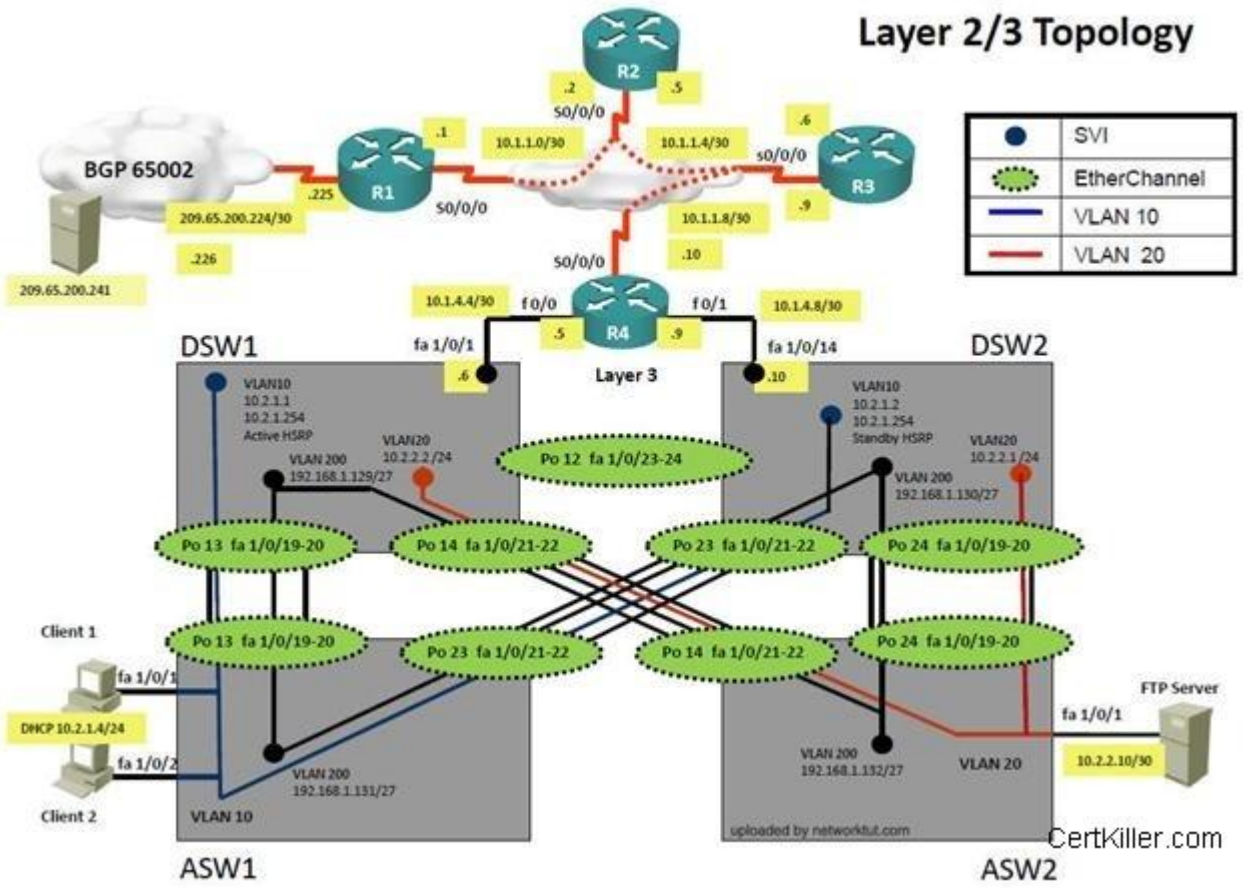


Figure 2

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

Configuration on DSW1

DSW1
vlan access-map test1 10
 action drop
 match ip address 10
vlan access-map test1 20
 action drop

```
 match ip address 20
vlan access-map test1 30
 action foward
 match ip address 30
vlan access-map test1 40
 action foward
!
vlan filter test1 vlan-list 10
vlan internal allocation policy asdending
!
access-list 10 permit 10.2.1.3
access-list 20 permit 10.2.1.4
access-list 30 permit 10.2.1.0 0.0.0.255
```

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: D
Section: (none)
Explanation

Explanation/Reference:
“that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241″: Though the Ticket was placed for Client 1, eliminating just “vlan access-map test1 10″ but client2 still cannot access the WEB Server because IP of client2 present in “vlan access-map test1 20″ so should be select this choice for answer

Exam K

QUESTION 1
(Ticket 10: EIGRP AS number)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

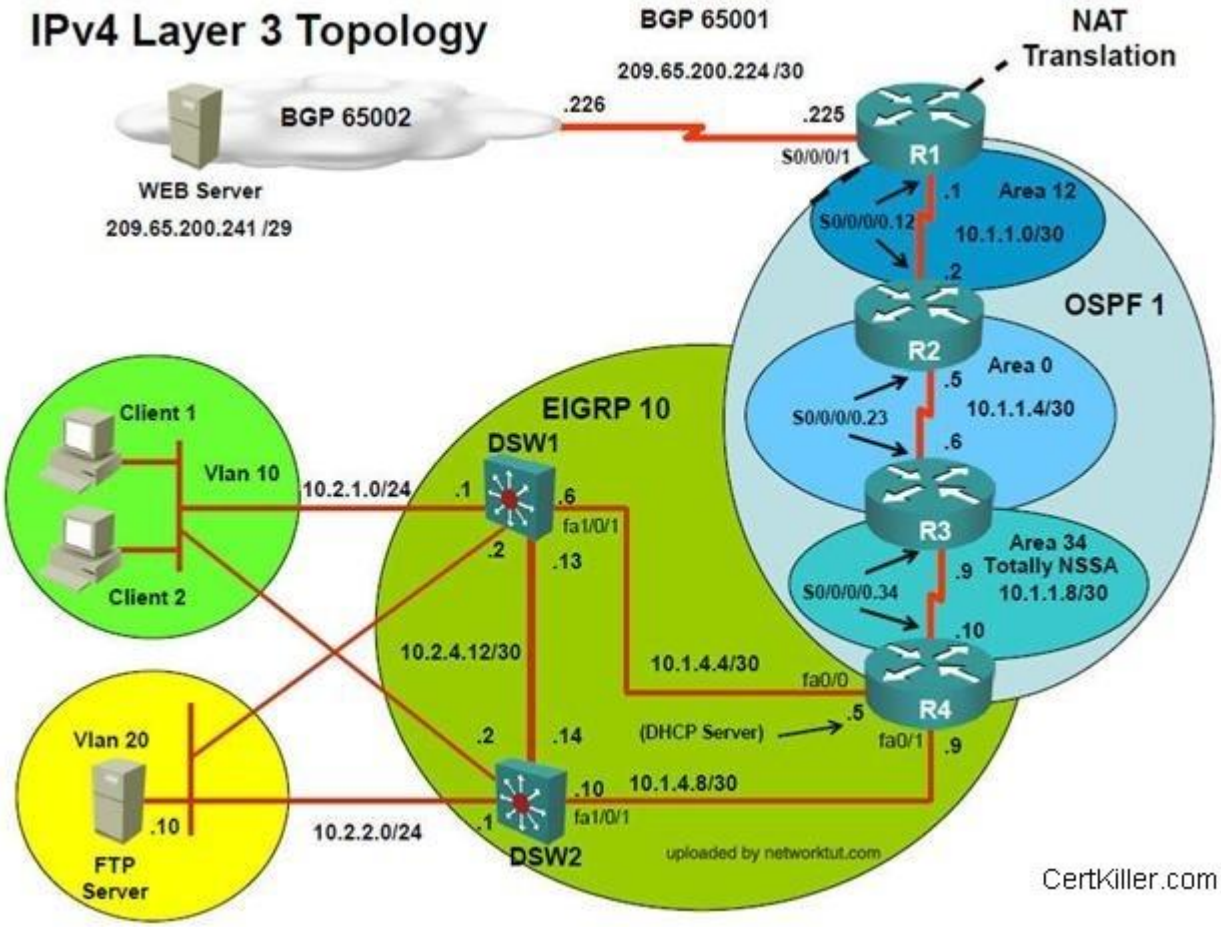


Figure 1

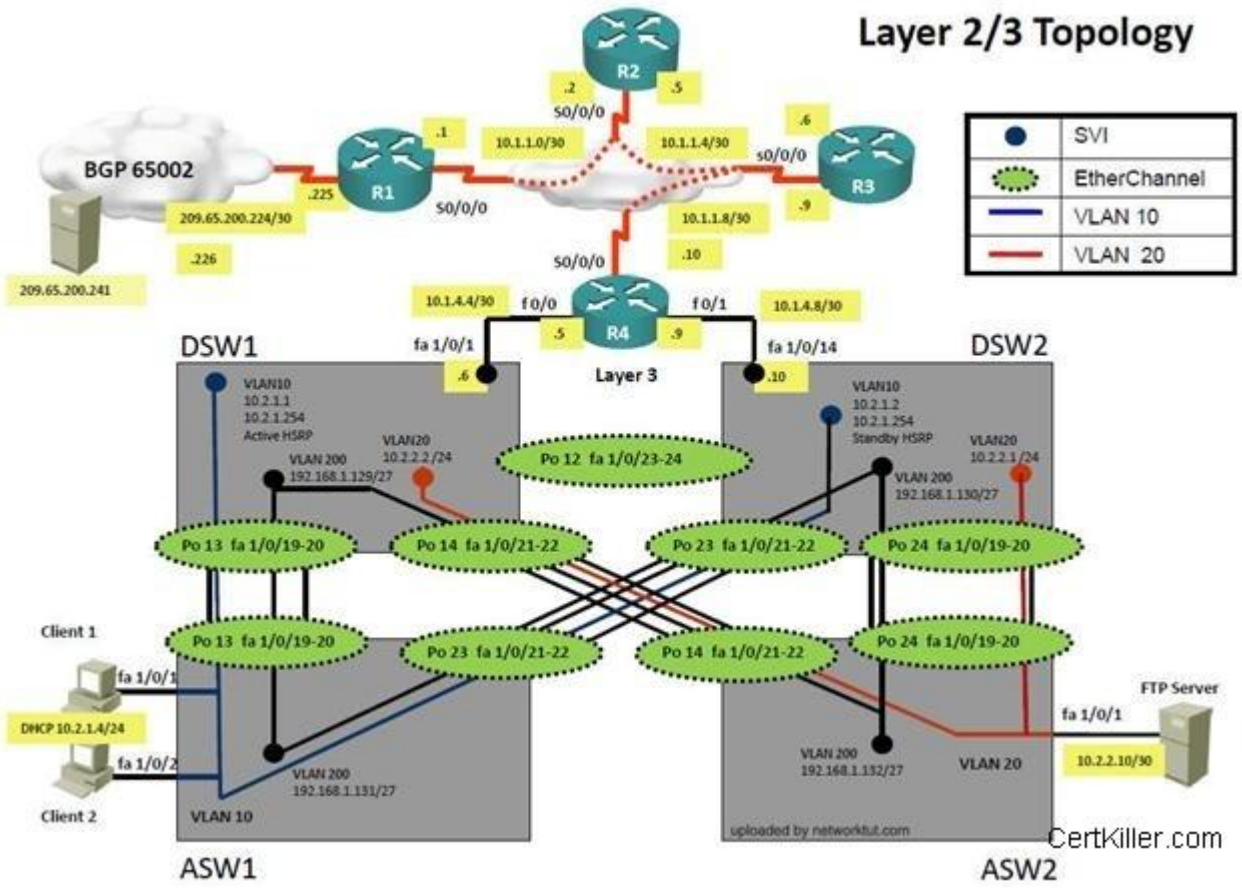


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer. Initial troubleshooting shows that DSW1 can ping the Fa0/1 interface of R4 but not the s0/0/0/0.34 interface.

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0
no auto-summary

Configuration on DSW2

```
router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary
```

Configuration on R4

```
router eigrp 1
network 10.1.4.5 0.0.0.0
no auto-summary
redistribute ospf 1
```

On which device is the fault condition located?

A. DSW1
B. DSW2
C. Client 1
D. R4
E. R2
F. R1
G. R3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Answer: R4

QUESTION 2
(Ticket 9: EIGRP AS number)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

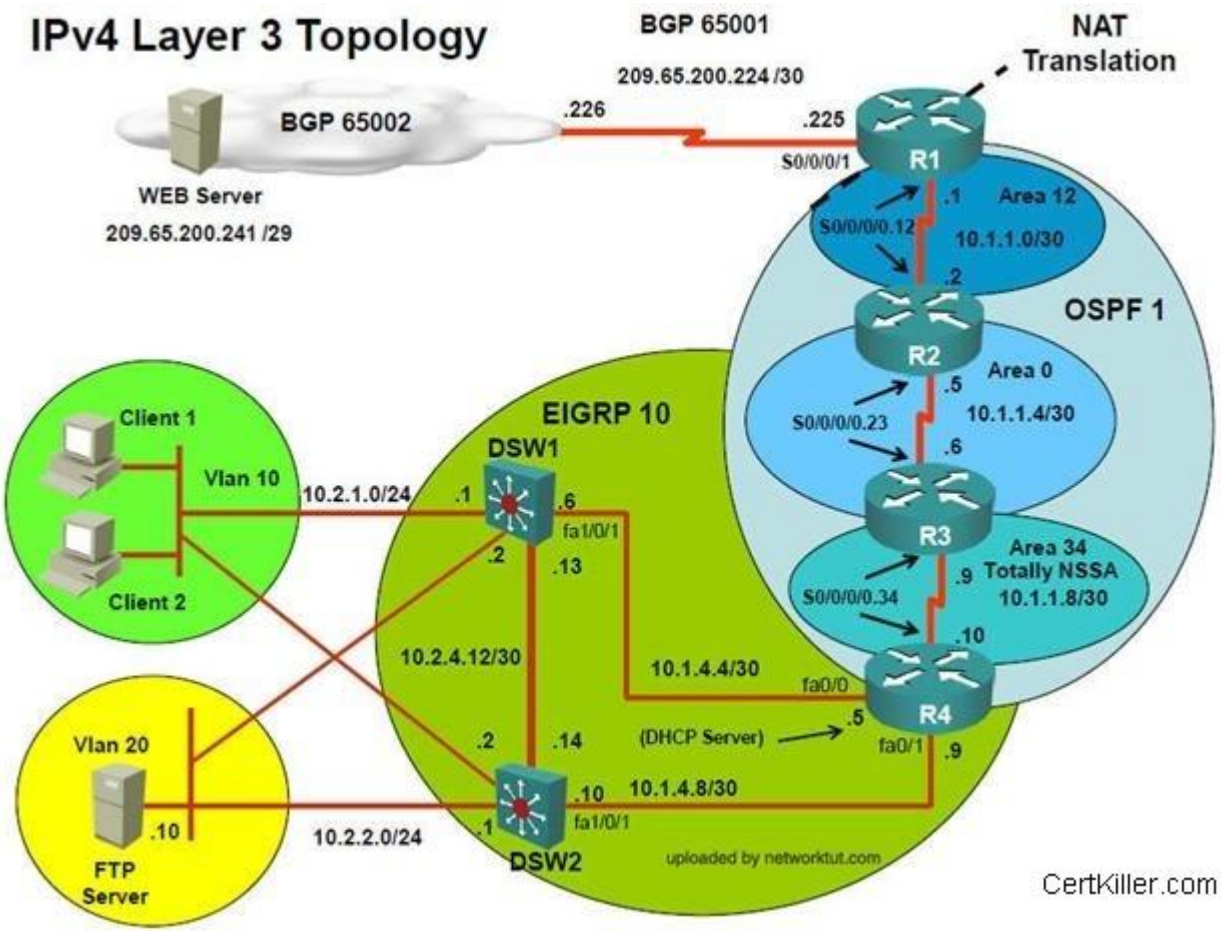

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.10
R4
EIGRP 10
DSW1
Client 1
Vlan 10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

Figure 1

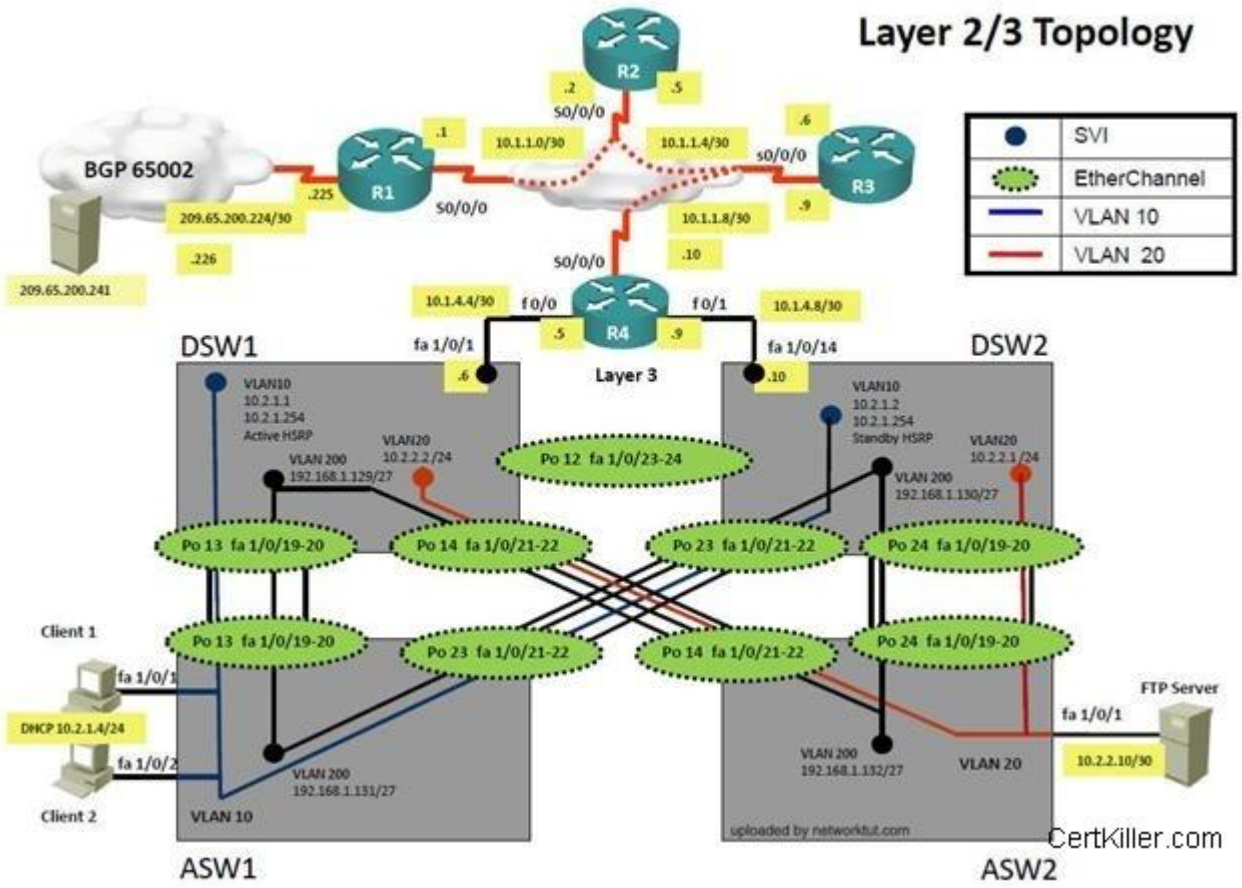


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer. Initial troubleshooting shows that DSW1 can ping the Fa0/1 interface of R4 but not the s0/0/0/0.34 interface.

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0

no auto-summary

Configuration on DSW2

router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary

Configuration on R4

router eigrp 1
network 10.1.4.5 0.0.0.0
no auto-summary
redistribute ospf 1

The Fault Condition is related to which technology?

A. EIGRP
B. InterVLAN communication
C. OSPF
D. Switch to Switch Connectivity
E. BGP
F. HSRP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: EIGRP

QUESTION 3
(Ticket 9: EIGRP AS number)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

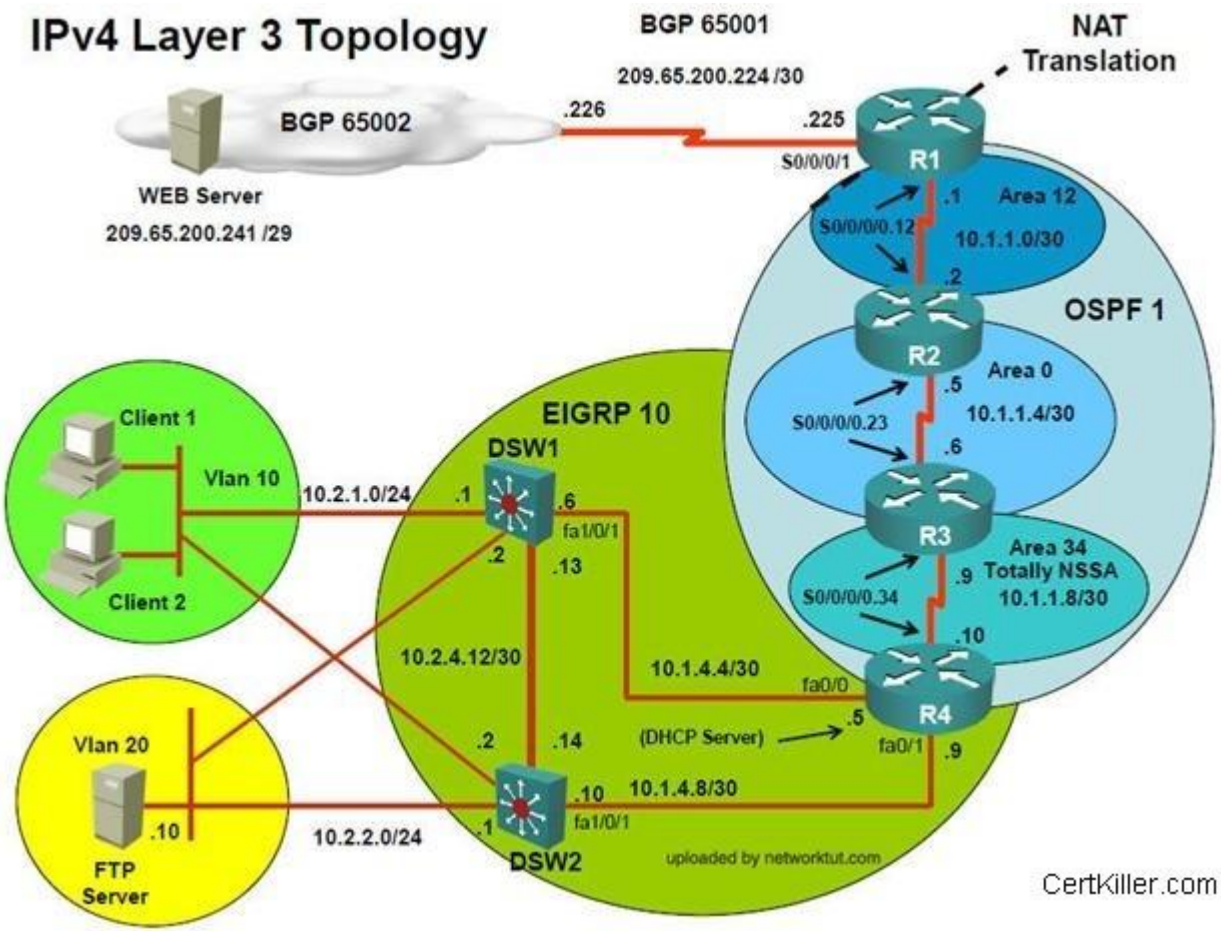

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

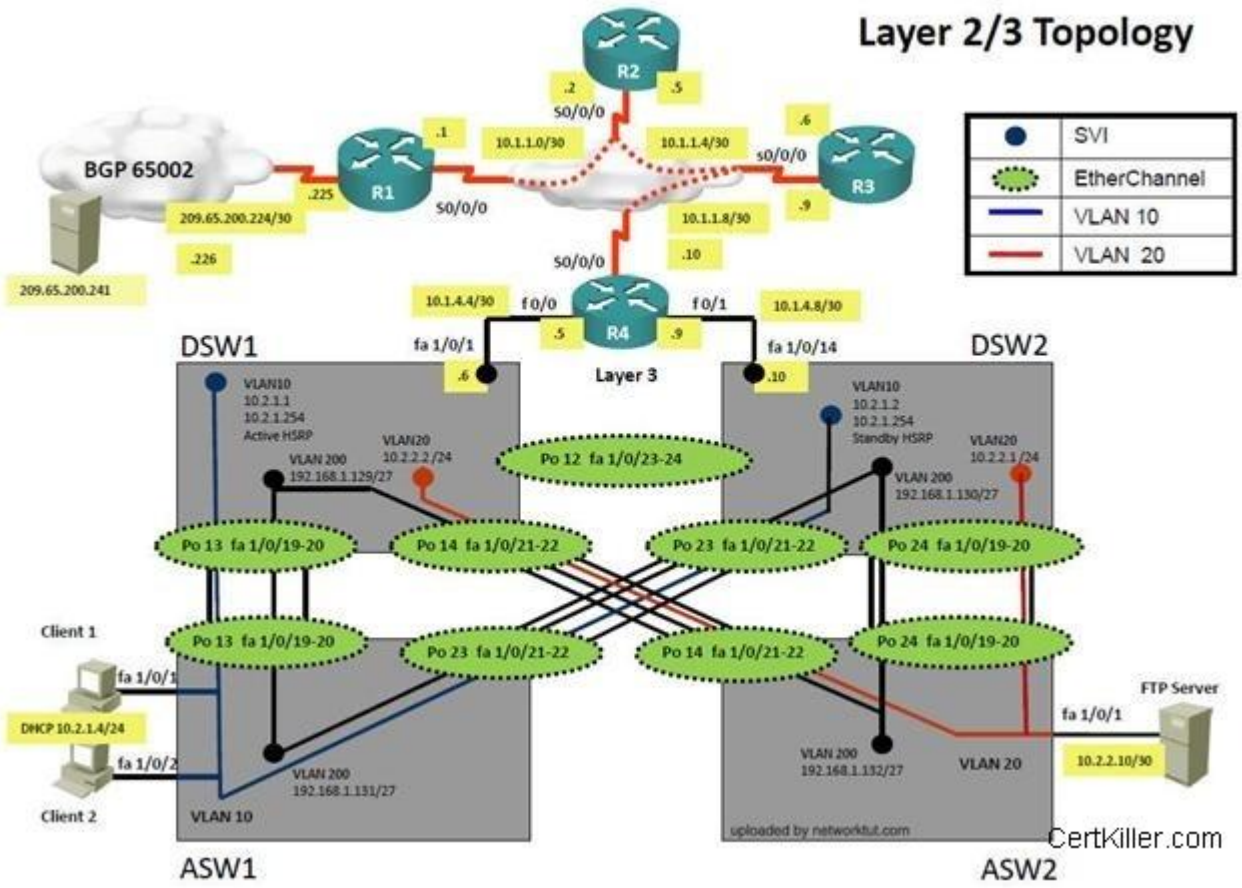
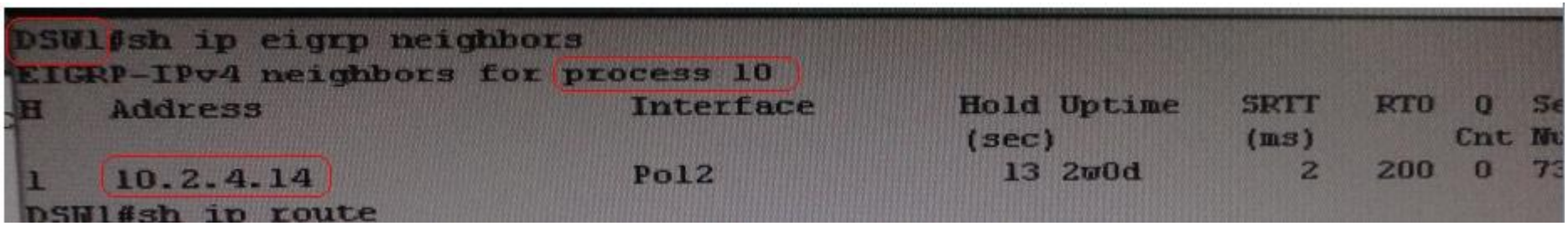


Figure 2

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

Configuration on R4



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: (none)
Explanation

Explanation/Reference:
Answer: Change the AS number on the EIGRP routing process from 1 to 10 to much the AS number used on DSW1 and DSW2.

Exam L

QUESTION 1
(Ticket 11: HSRP Issue)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

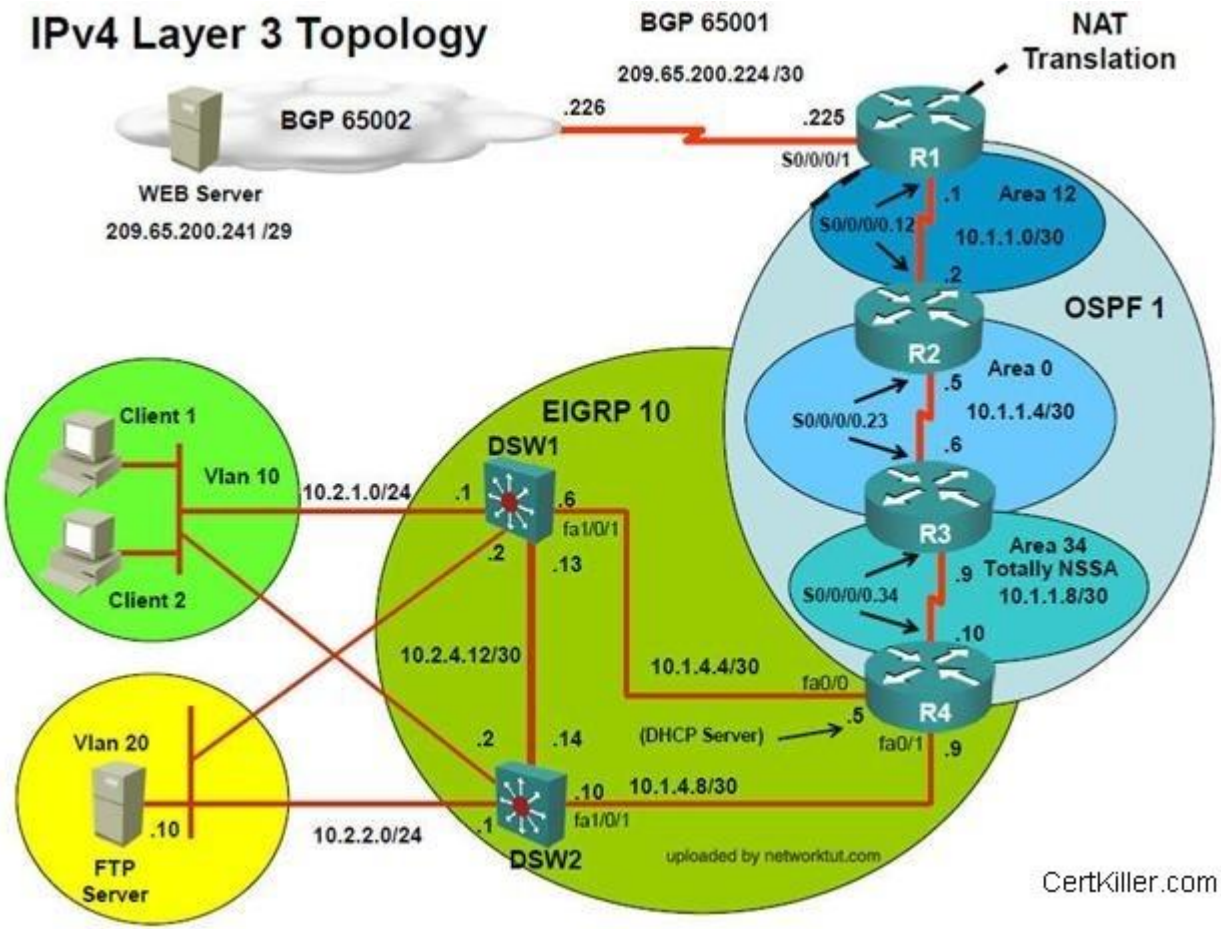


Figure 1

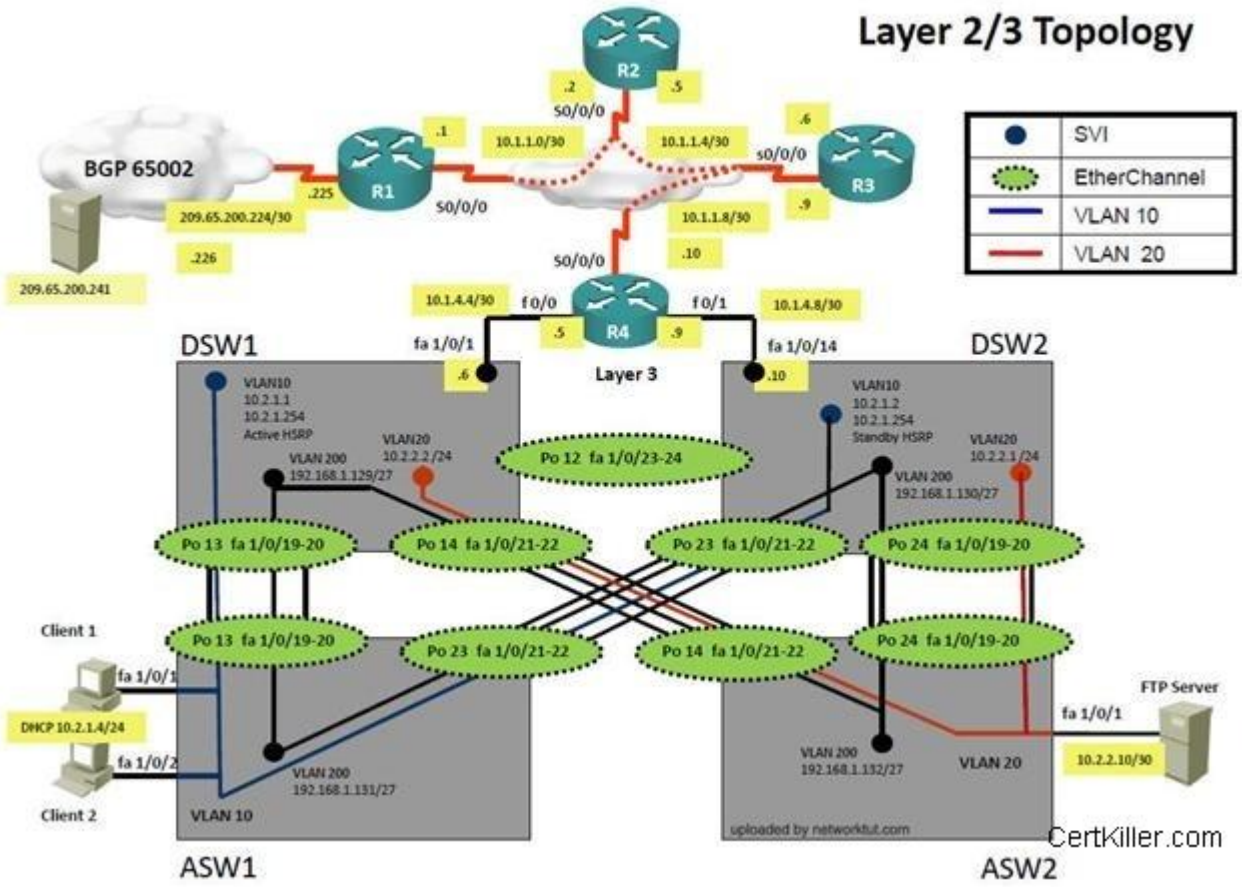


Figure 2

Trouble Ticket Statement

HSRP has been configurationured between DSW1 and DSW2. DSW1 is configurationured to be active router but it never becomes active even though the HSRP communication between DSW1 and DSW2 is working.

Configuration on DSW1

track 1 ip route 10.1.21.128 255.255.0.0 metric threshold threshold metric up 1 down 2

```
!
track 10 ip route 10.2.21.128 255.255.255.0 metric threshold threshold metric up 63 down 64
!
interface Vlan10
ip address 10.2.1.1 255.255.255.0
standby 10 ip 10.2.1.254
standby 10 priority 200
standby 10 preempt
standby 10 track 1 decrement 60
```

Configuration on R4

```
interface loopback0
ip address 10.2.21.128 255.255.255.0
```

On which device is the fault condition located?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer:
DSW1

QUESTION 2
(Ticket 12: HSRP Issue)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

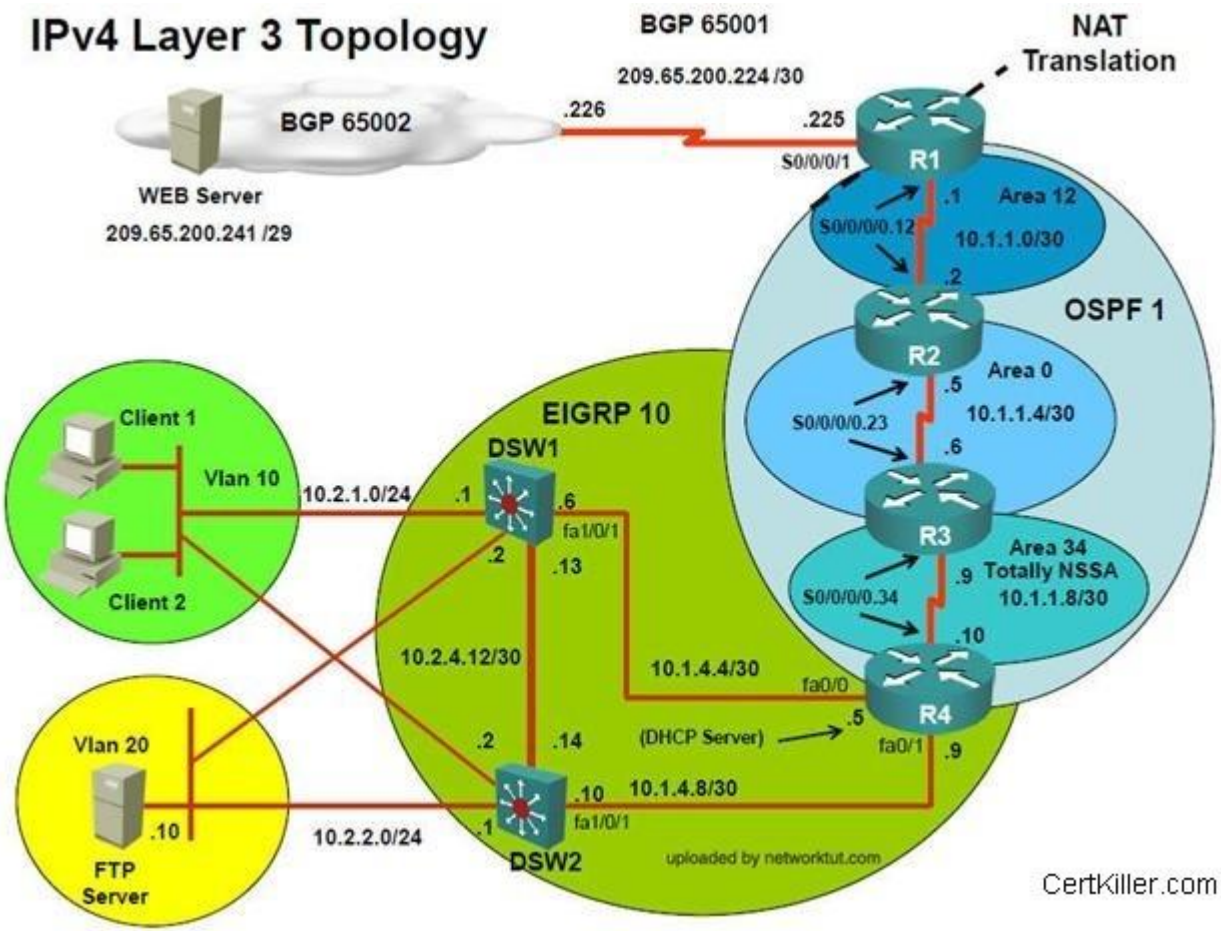

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.10
R4
EIGRP 10
DSW1
Client 1
Vlan 10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

Figure 1

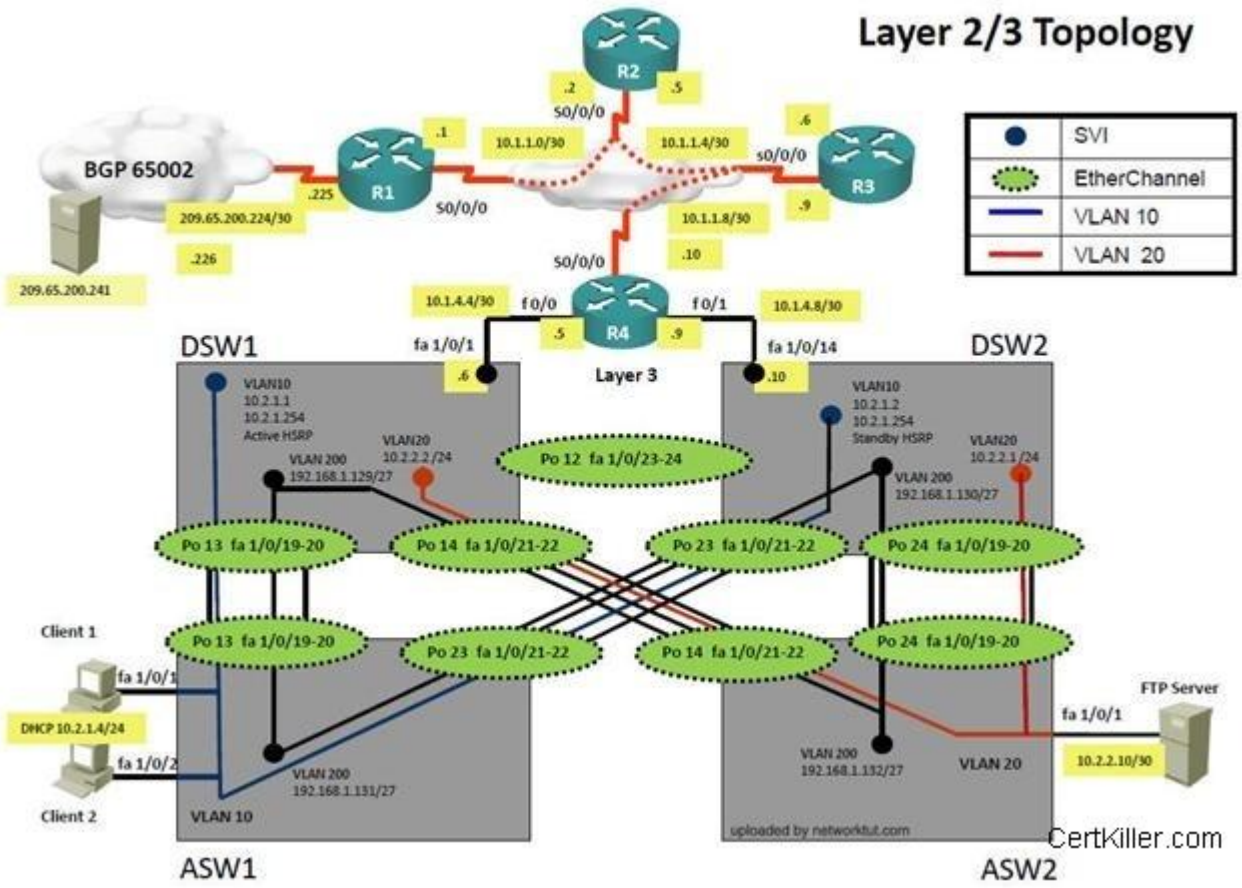


Figure 2

Trouble Ticket Statement

HSRP has been configurationured between DSW1 and DSW2. DSW1 is configurationured to be active router but it never becomes active even though the HSRP communication between DSW1 and DSW2 is working.

Configuration on DSW1

track 1 ip route 10.1.21.128 255.255.0.0 metric threshold threshold metric up 1 down 2
!
track 10 ip route 10.2.21.128 255.255.255.0 metric threshold threshold metric up 63 down 64

!
interface Vlan10
ip address 10.2.1.1 255.255.255.0
standby 10 ip 10.2.1.254
standby 10 priority 200
standby 10 preempt
standby 10 track 1 decrement 60

Configuration on R4

interface loopback0
ip address 10.2.21.128 255.255.255.0

Fault Condition is related to which technology?

A. GLBP
B. HSRP
C. OSPF
D. Switch to Switch Connectivity
E. VRRP
F. EIGRP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Answer:
HSRP

QUESTION 3
(Ticket 12: HSRP Issue)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

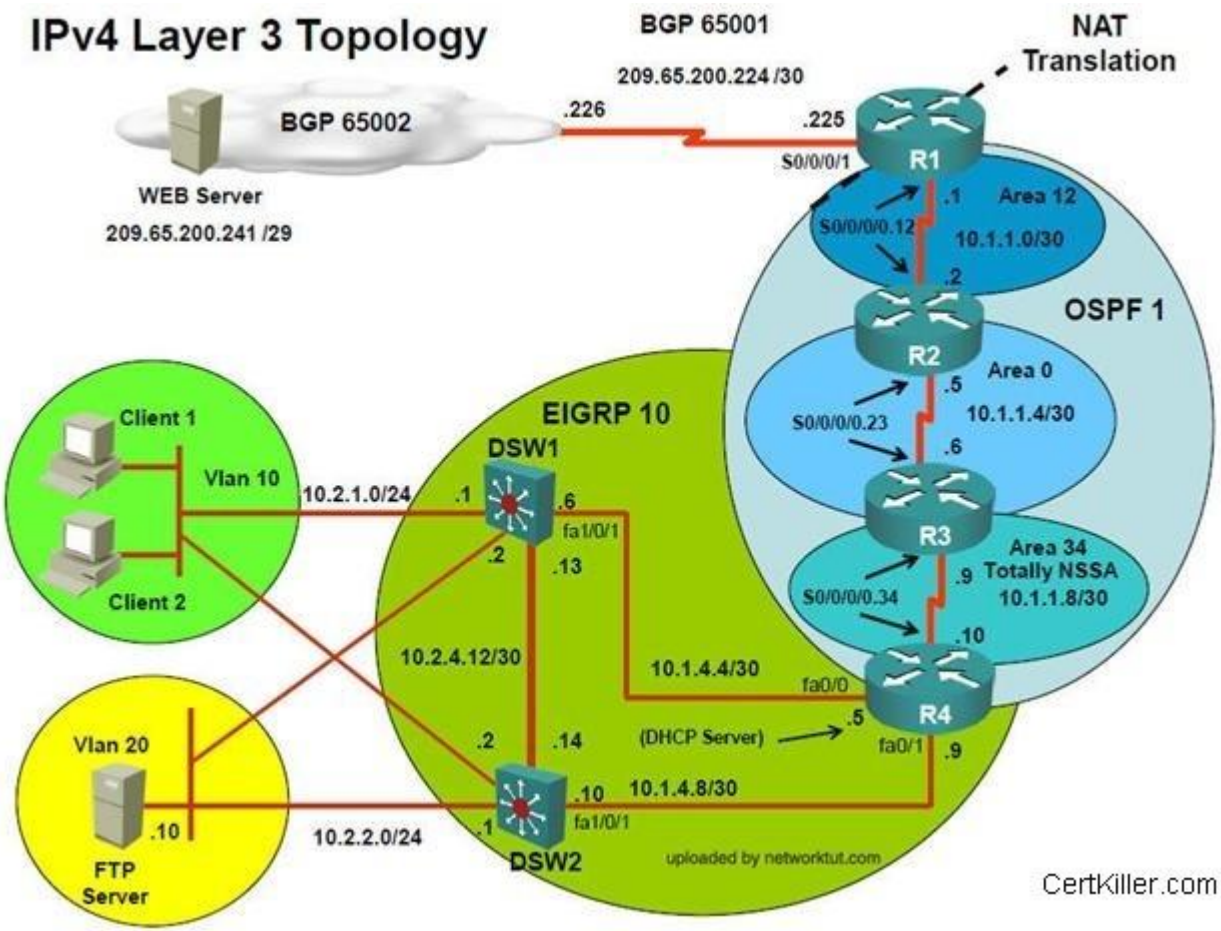

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.10
R4
EIGRP 10
DSW1
Client 1
Vlan 10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

Figure 1

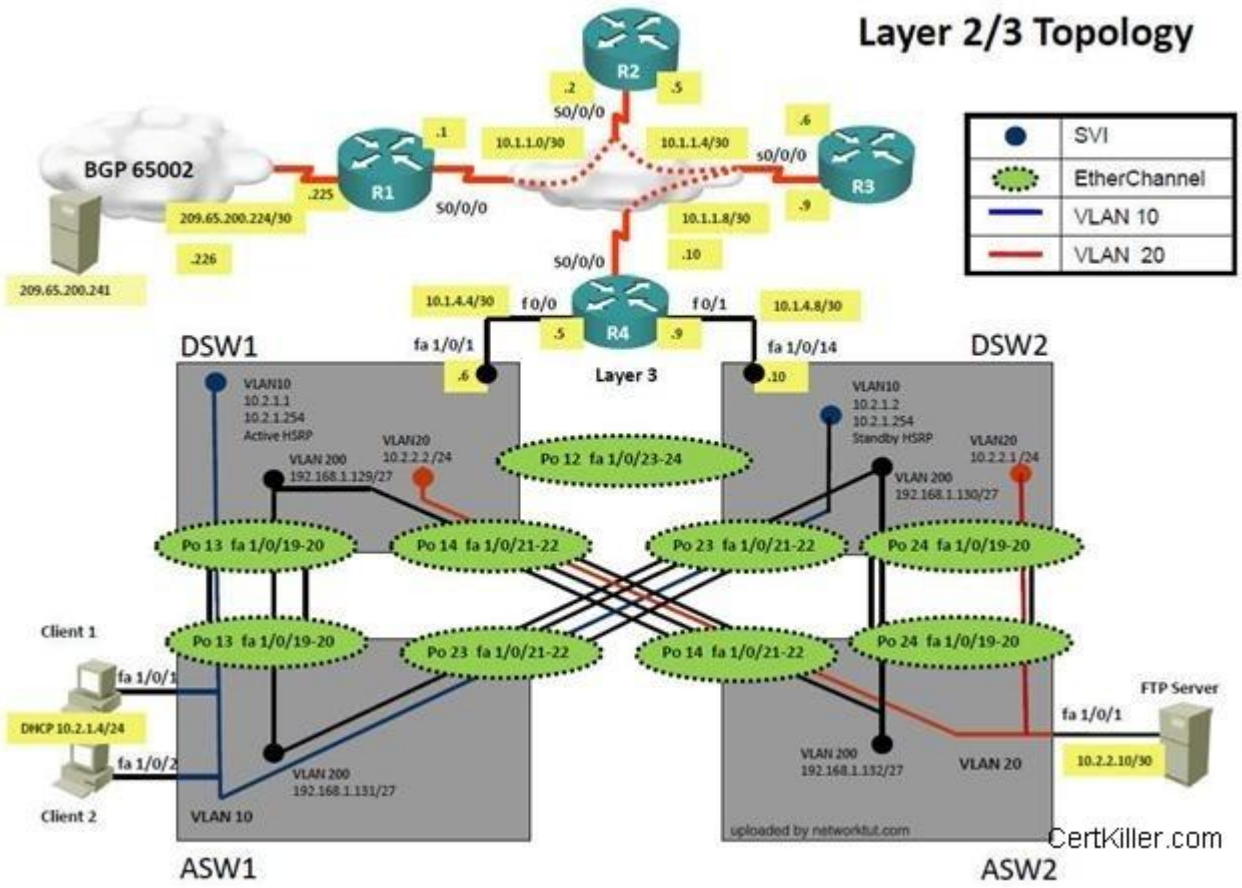


Figure 2

Trouble Ticket Statement

HSRP has been configurationured between DSW1 and DSW2. DSW1 is configurationured to be active router but it never becomes active even though the HSRP communication between DSW1 and DSW2 is working.

Configuration on DSW1

track 1 ip route 10.1.21.128 255.255.0.0 metric threshold threshold metric up 1 down 2
!
track 10 ip route 10.2.21.128 255.255.255.0 metric threshold threshold metric up 63 down 64

!
interface Vlan10
ip address 10.2.1.1 255.255.255.0
standby 10 ip 10.2.1.254
standby 10 priority 200
standby 10 preempt
standby 10 track 1 decrement 60

Configuration on R4

interface loopback0
ip address 10.2.21.128 255.255.255.0

What is the solution of fault condition?

A. Change standby priority to 140
B. Change standby priority to 260
C. Change standby 10 track 1 decrement 60 to standby 10 track 10 decrement 60
D. Change standby 10 track 1 decrement 60 to standby 10 track 1 decrement 100
E. Change standby 10 track 1 decrement 60 to standby 10 track 10 decrement 100
F. Change standby 10 track 1 decrement 60 to standby 10 track 1 decrement 60

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer:
Change standby 10 track 1 decrement 60 to standby 10 track 10 decrement 60

Exam M

QUESTION 1
(Ticket 12: DHCP Issue Topology Overview)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

- 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

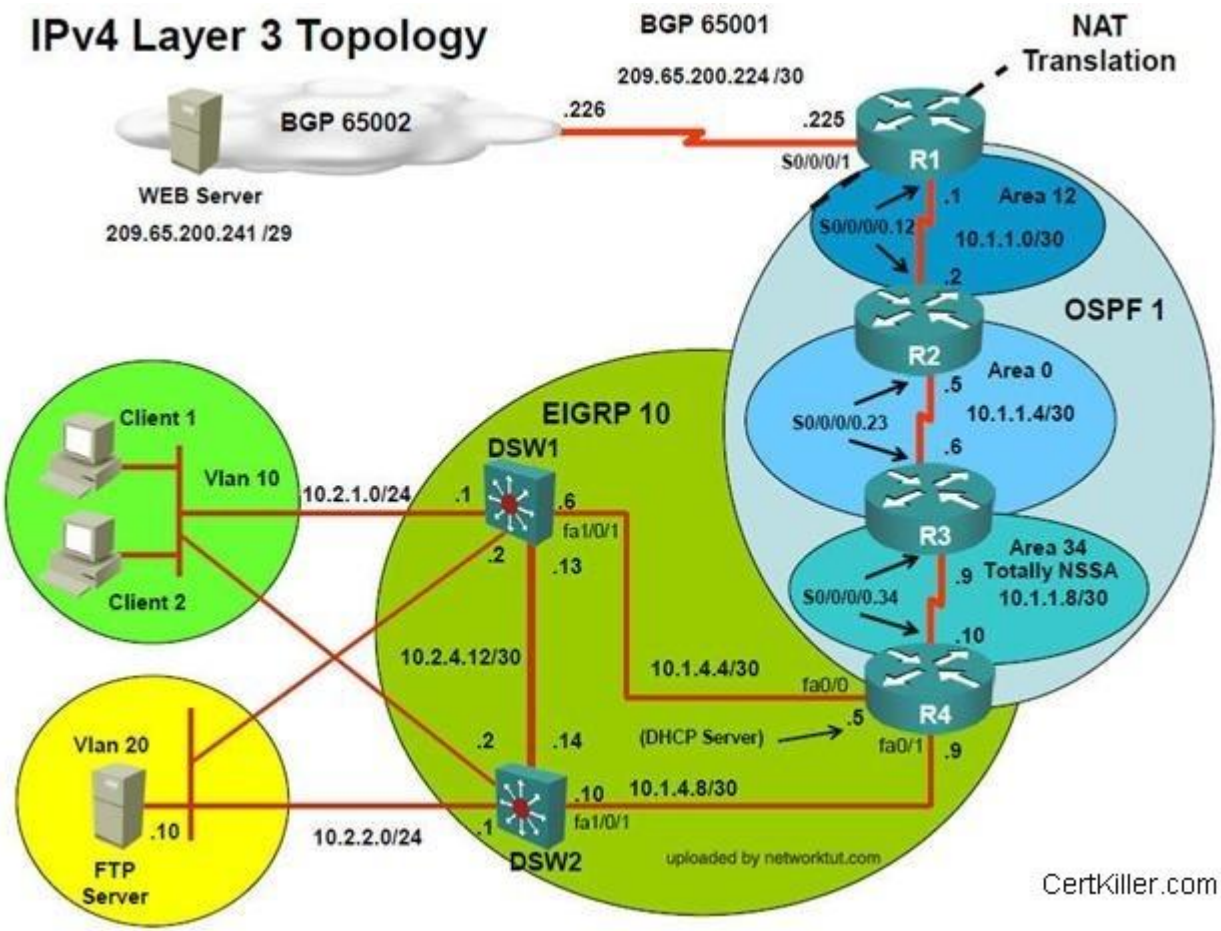

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

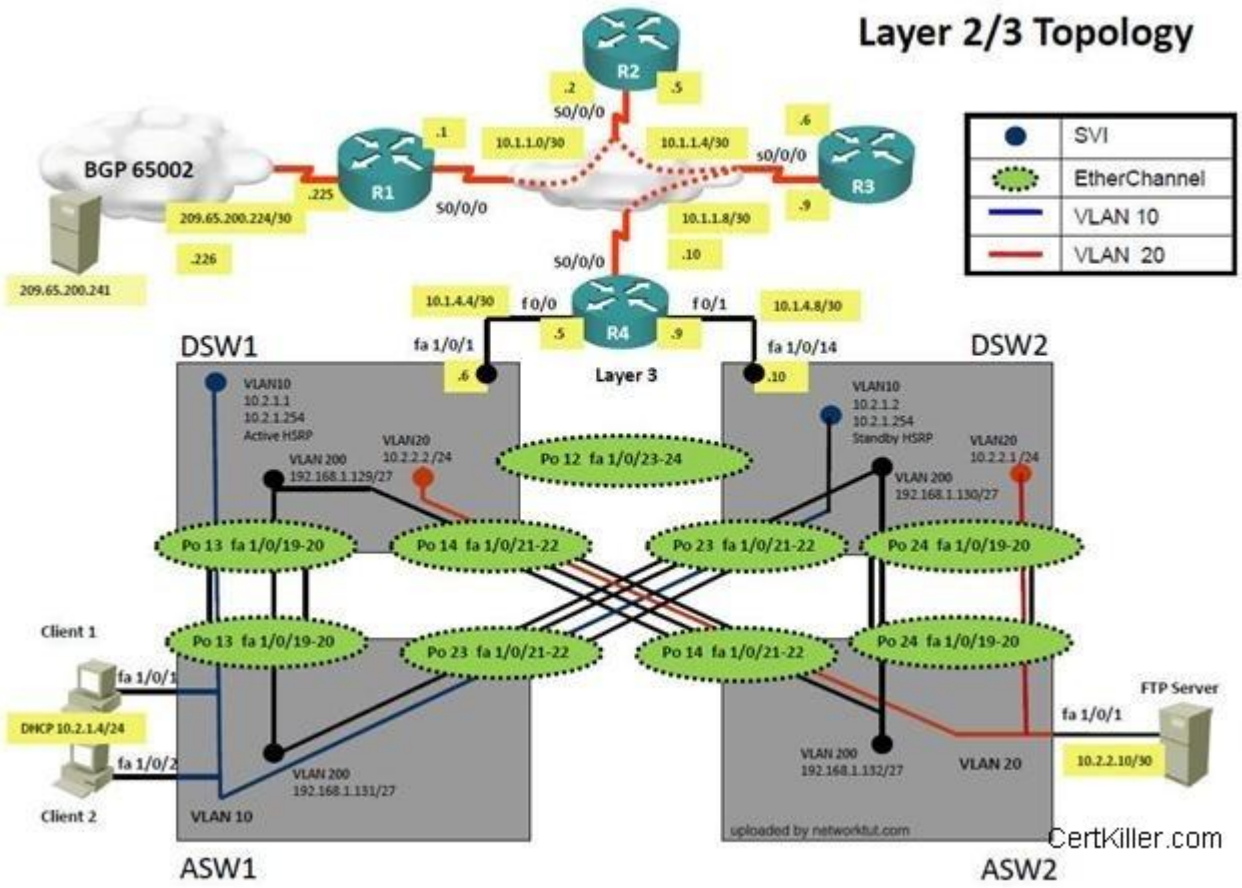


Figure 2

Question:

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

Solution
Steps need to follow as below:-

- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4

ipconfig ----- Client will be receiving Private IP address 169.254.X.X

- From ASW1 we can ping 10.2.1.254….

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

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

Configuration on R4 was:

!
ip dhcp exclude 10.2.1.1-10.2.1.253
!

The fault condition is related to which theconology?

A. R4
B. DSW1
C. DSW2
D. ASW1
E. ASW2
F. Client 1
G. Client 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: R4

QUESTION 2

(Ticket 13: DHCP Issue Topology Overview)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

- 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

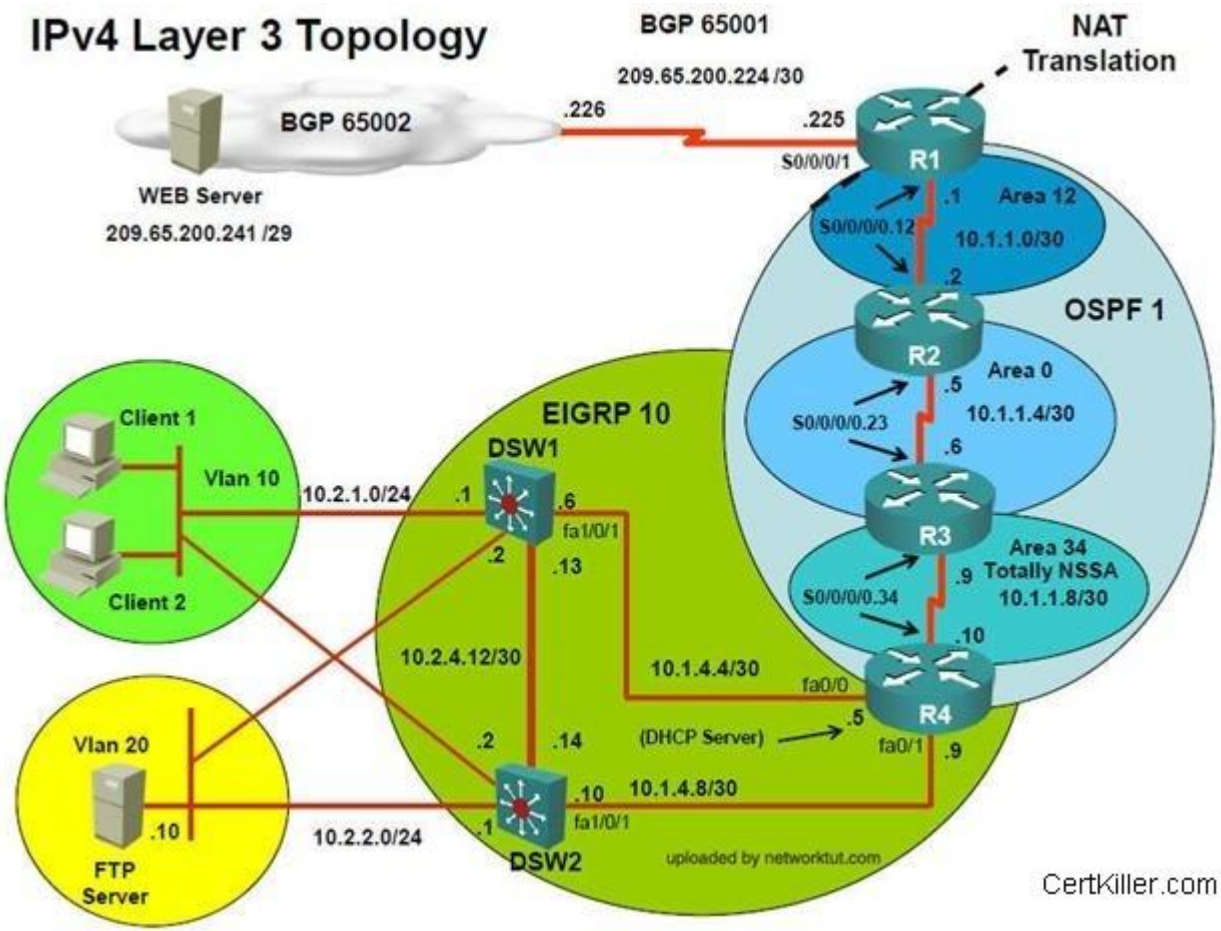

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

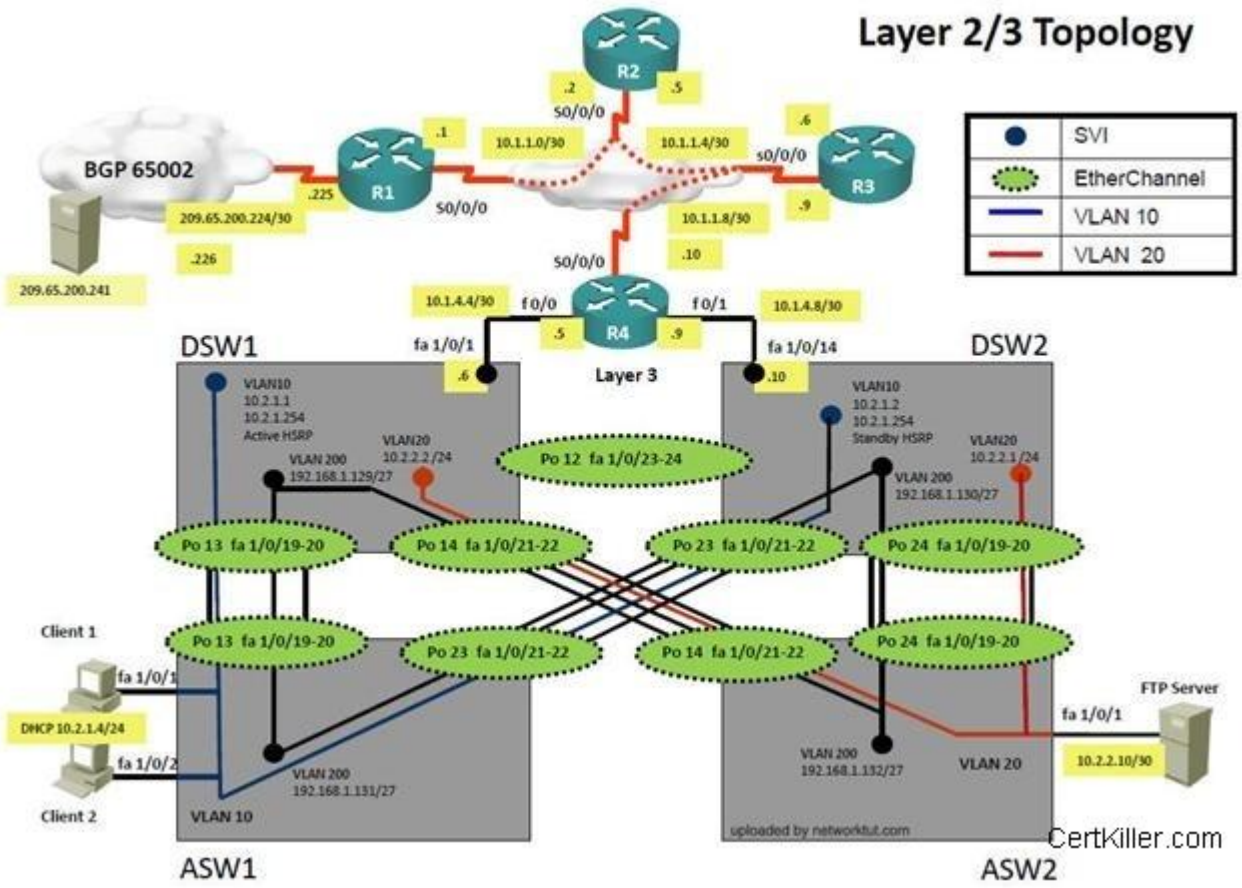


Figure 2

Question:

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

Solution
Steps need to follow as below:-

- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4

ipconfig ----- Client will be receiving Private IP address 169.254.X.X

- From ASW1 we can ping 10.2.1.254….

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

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

Configuration on R4 was:

!
ip dhcp exclude 10.2.1.1-10.2.1.253
!

The fault condition is related to which technology?

A. NTP
B. IP DHCP Server
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: B
Section: (none)
Explanation

Explanation/Reference:
Answer:
IP DHCP Server

QUESTION 3
(Ticket 13: DHCP Issue Topology Overview)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

- 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

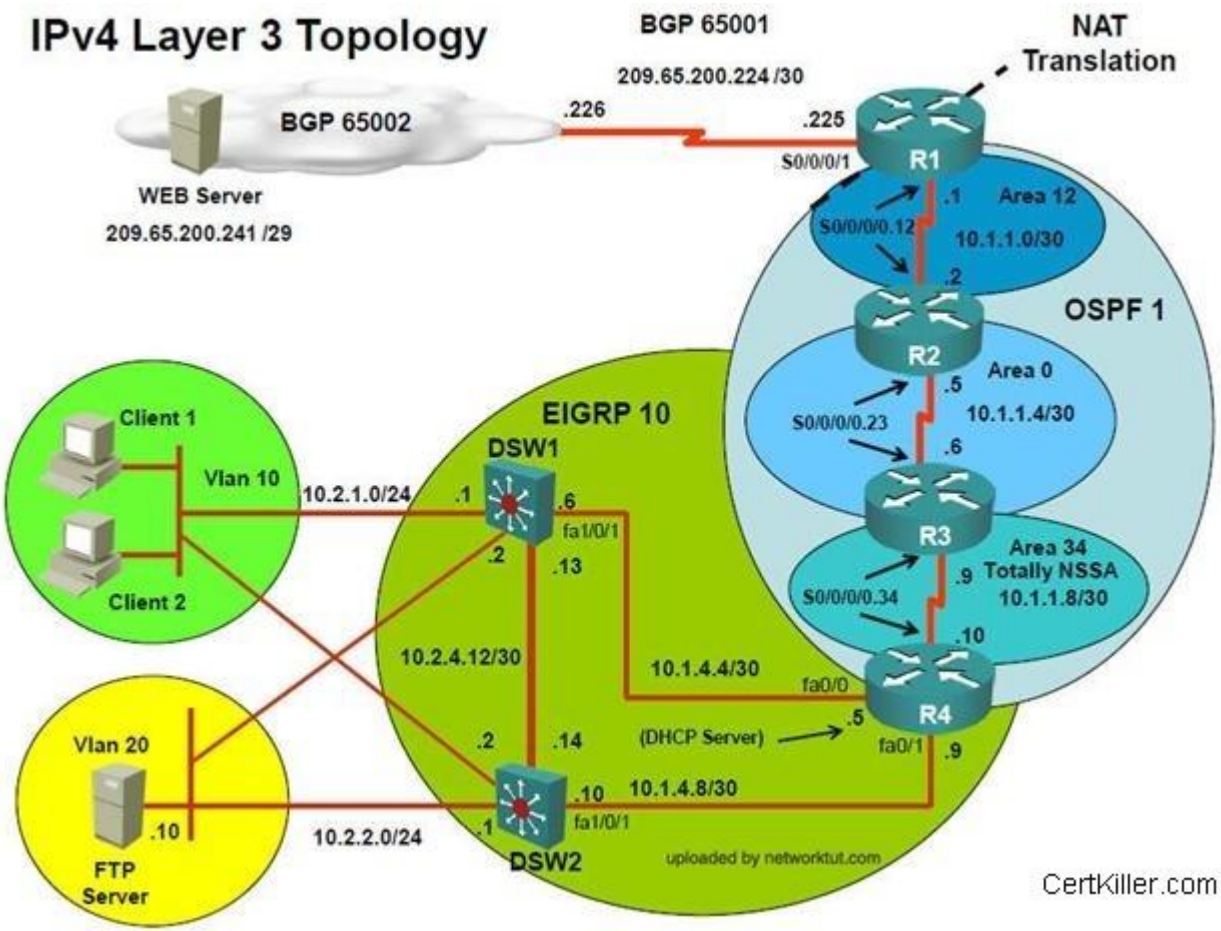

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.2
.13
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
CertKiller.com

Figure 1

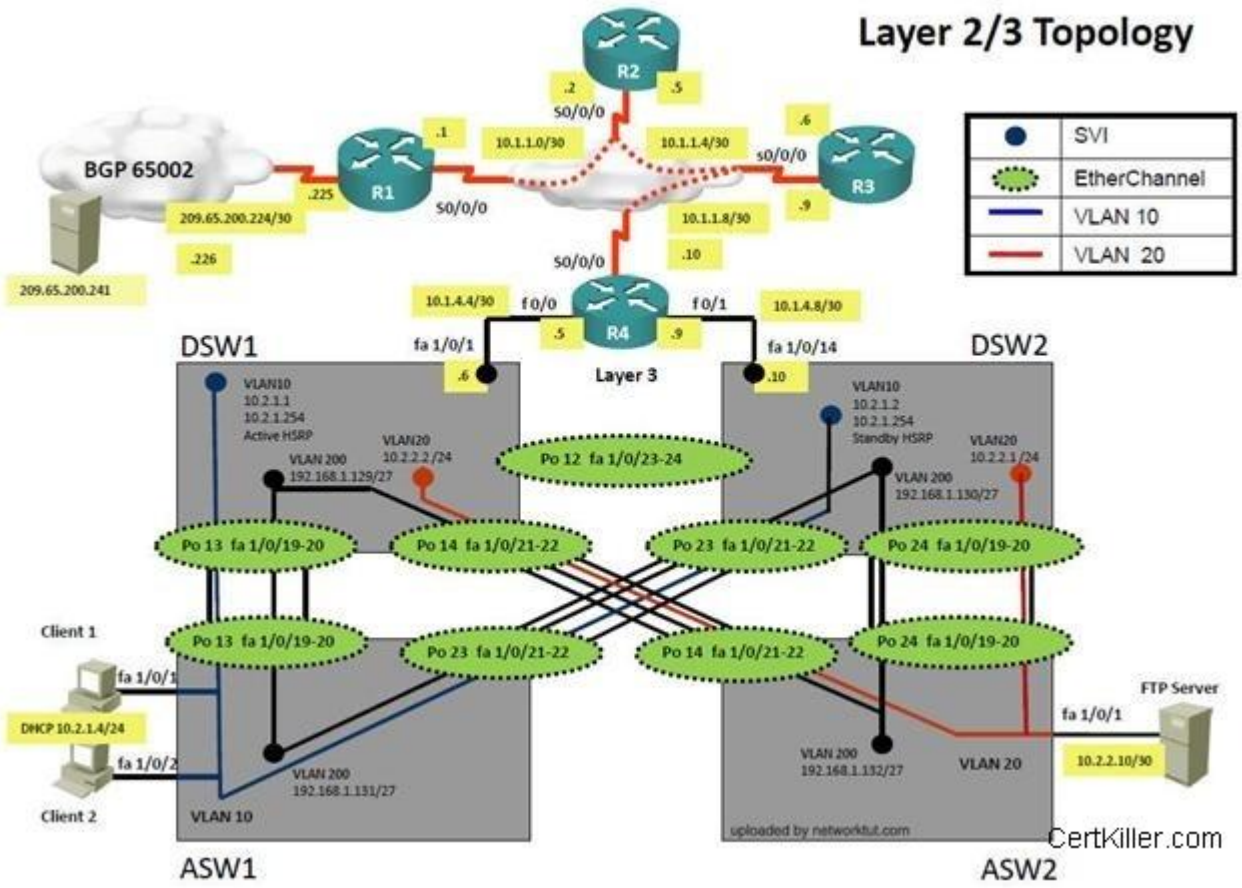


Figure 2

Question:

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

Solution
Steps need to follow as below:-

- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4

ipconfig ----- Client will be receiving Private IP address 169.254.X.X

- From ASW1 we can ping 10.2.1.254….

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

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

Configuration on R4 was:

!
ip dhcp exclude 10.2.1.1-10.2.1.253
!

What is the solution of the fault condition?

A. on DSW1 delete ip dhcp exclude 10.2.1.1-10.2.1.253 and apply ip dhcp-excluded 10.2.1.1-10.2.1.2
B. on DSW2 delete ip dhcp exclude 10.2.1.1-10.2.1.253 and apply ip dhcp-excluded 10.2.1.1-10.2.1.2
C. on R4 delete ip dhcp exclude 10.2.1.1-10.2.1.253 and apply ip dhcp-excluded 10.2.1.1-10.2.1.2
D. on R4 delete ip dhcp exclude 10.2.1.1-10.2.1.253 and apply ip dhcp-excluded 10.2.1.1-10.2.1.10

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer:
IP DHCP Server

Exam N

QUESTION 1
(Ticket 13: EIGRP Passive Interface)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

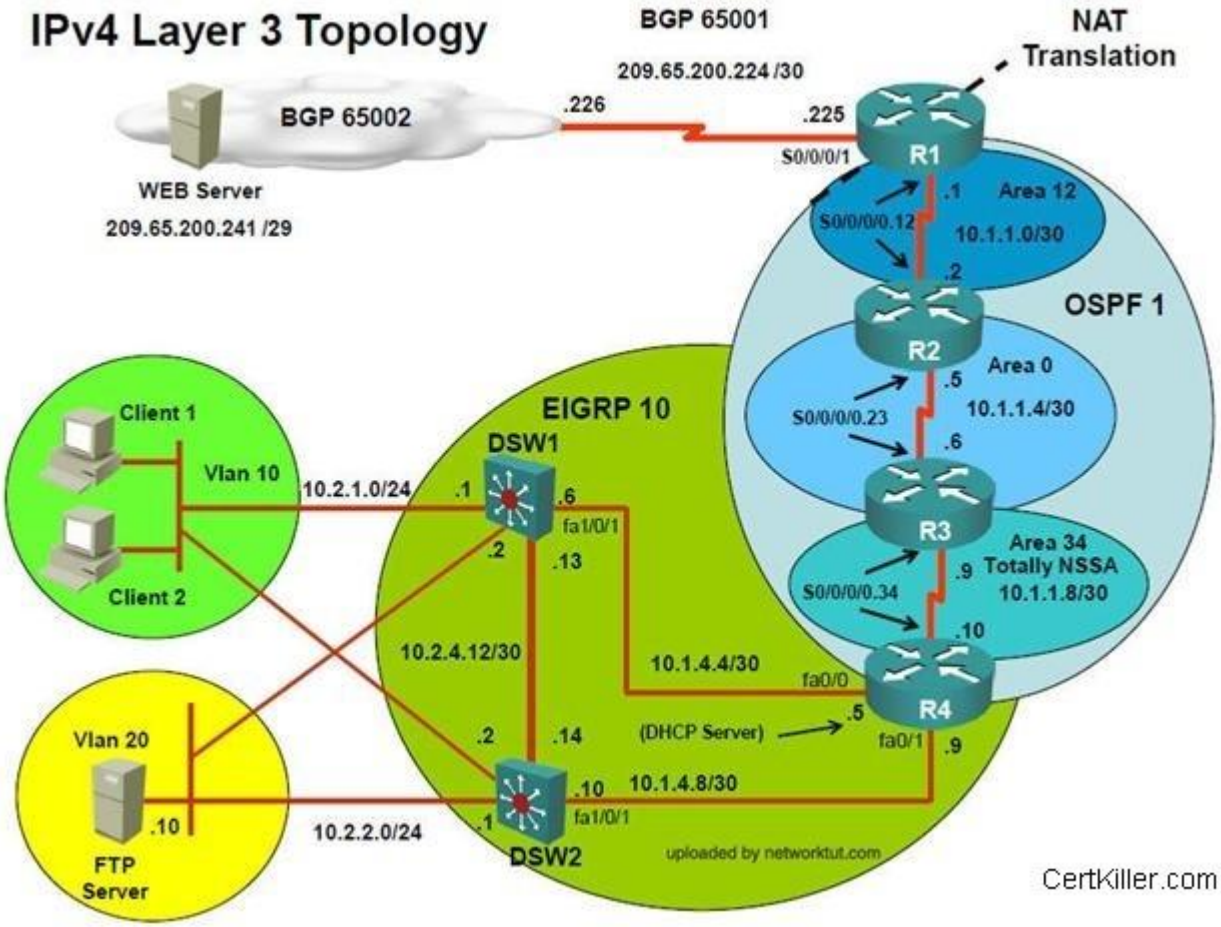


Figure 1

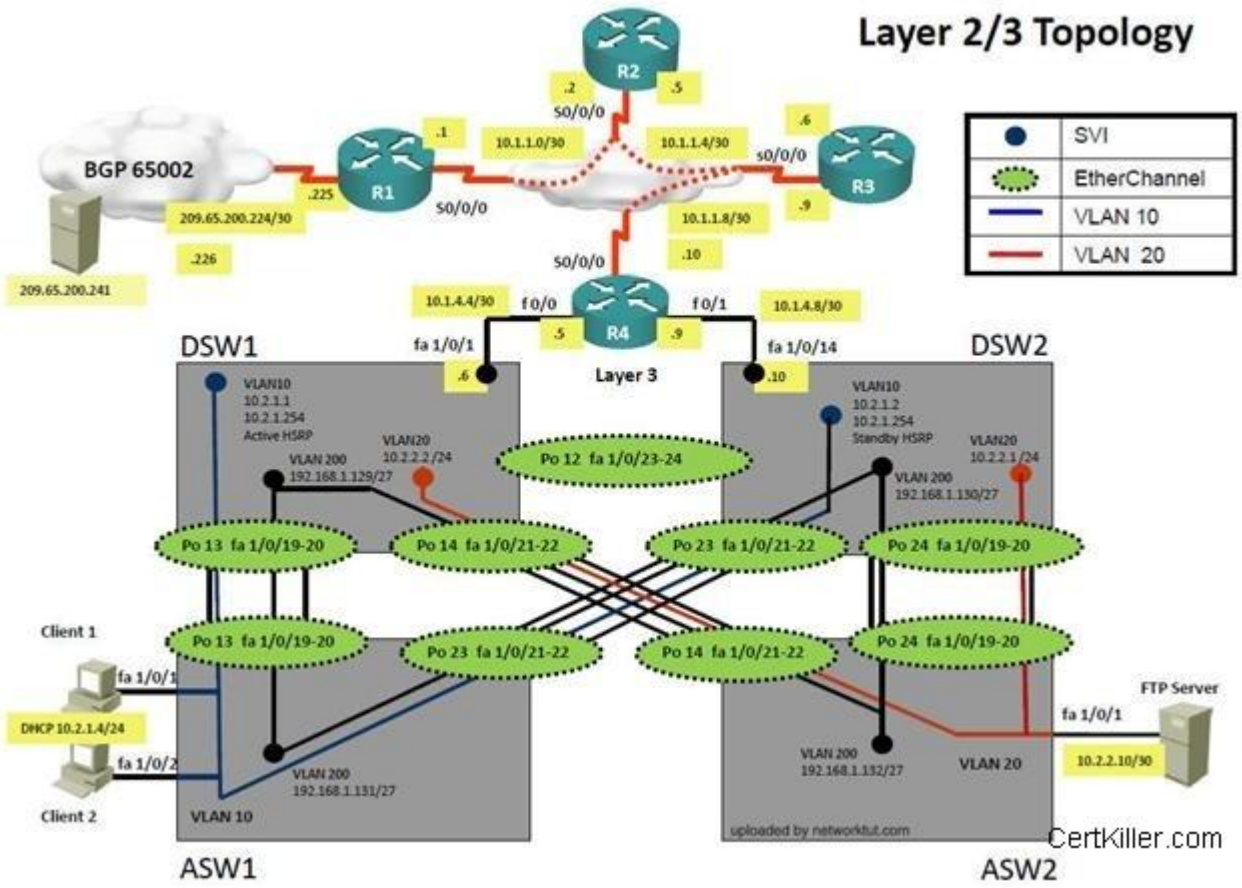


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer. Initial troubleshooting shows that DSW1 can ping the Fa0/1 interface of R4 but not the s0/0/0/0.34 interface.

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0
no auto-summary

Configuration on DSW2

```
router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary
```

Configuration on R4

```
router eigrp 10
passive-interface default
redistribute ospf 1 route-map OSPF->EIGRP
network 10.1.4.4 0.0.0.3
network 10.1.4.8 0.0.0.3
default-metric 10000 100 255 1 10000
no auto-summary
```

On which device is the fault condition located?

A. DSW1
B. DSW2
C. Client 1
D. R1
E. R2
F. R3
G. R4

Correct Answer: G
Section: (none)
Explanation

Explanation/Reference:
Answer: R4

QUESTION 2
(Ticket 14: EIGRP Passive Interface)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

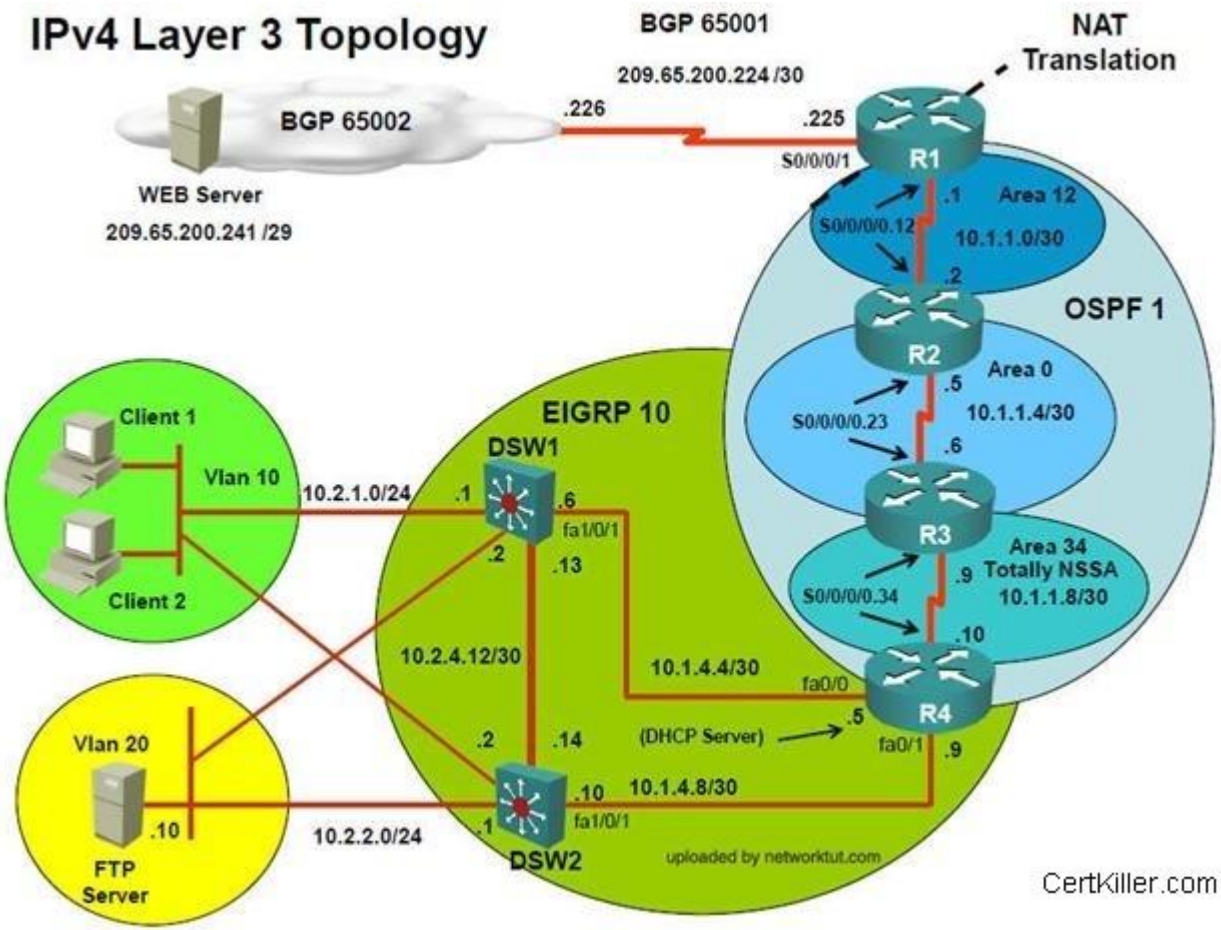

IPv4 Layer 3 Topology
BGP 65001
NAT
Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.9
S0/0/0/0.34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

Figure 1

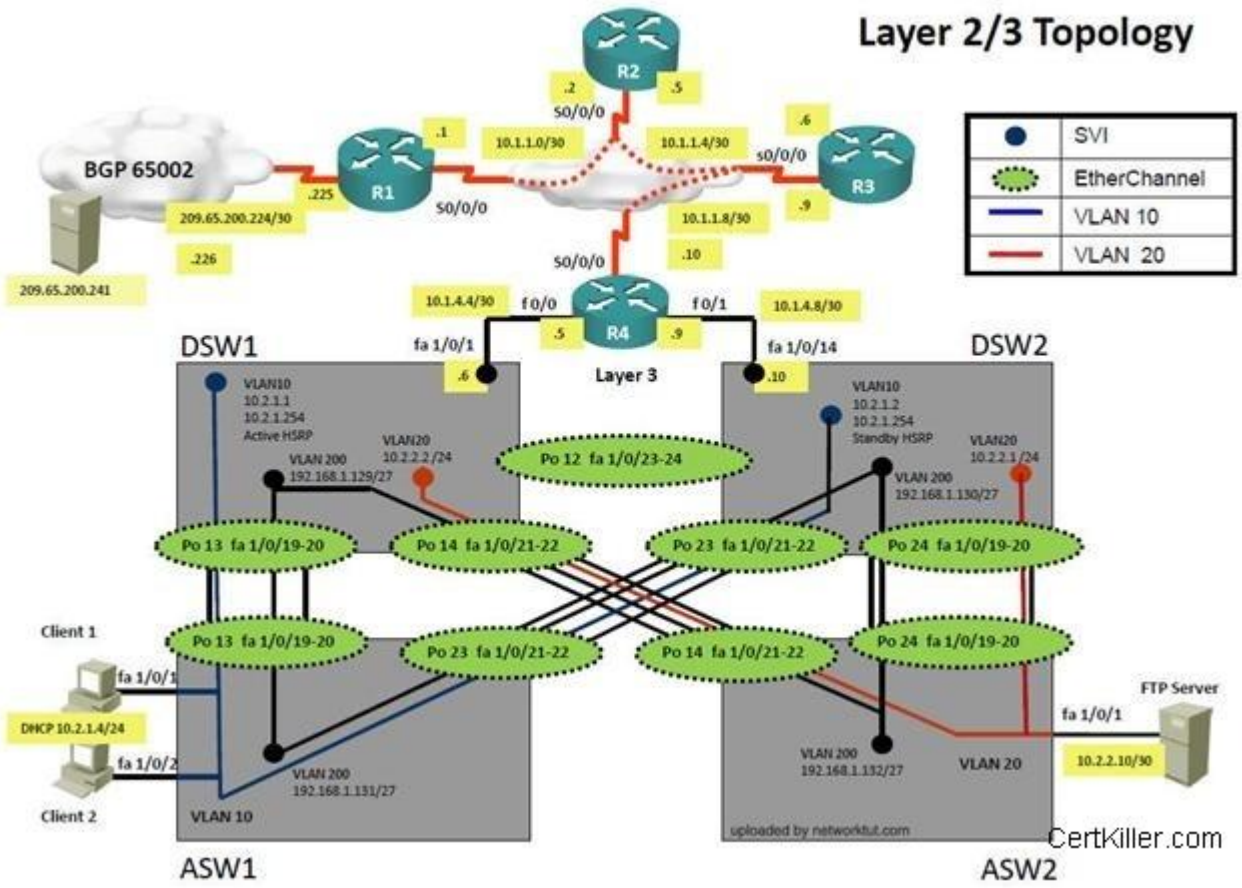


Figure 2

Trouble Ticket Statement

Client 1 is not able to reach the WebServer. Initial troubleshooting shows that DSW1 can ping the Fa0/1 interface of R4 but not the s0/0/0/0.34 interface.

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0

no auto-summary

Configuration on DSW2

router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary

Configuration on R4

router eigrp 10
passive-interface default
redistribute ospf 1 route-map OSPF->EIGRP
network 10.1.4.4 0.0.0.3
network 10.1.4.8 0.0.0.3
default-metric 10000 100 255 1 10000
no auto-summary

The Fault Condition is related to which technology?

A. Route Redistribution
B. IPv4 OSPF Routing
C. IPv4 EIGRP Routing
D. Static Route
E. BGP
F. RIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: IPv4 EIGRP Routing

QUESTION 3
(Ticket 14: EIGRP Passive Interface)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

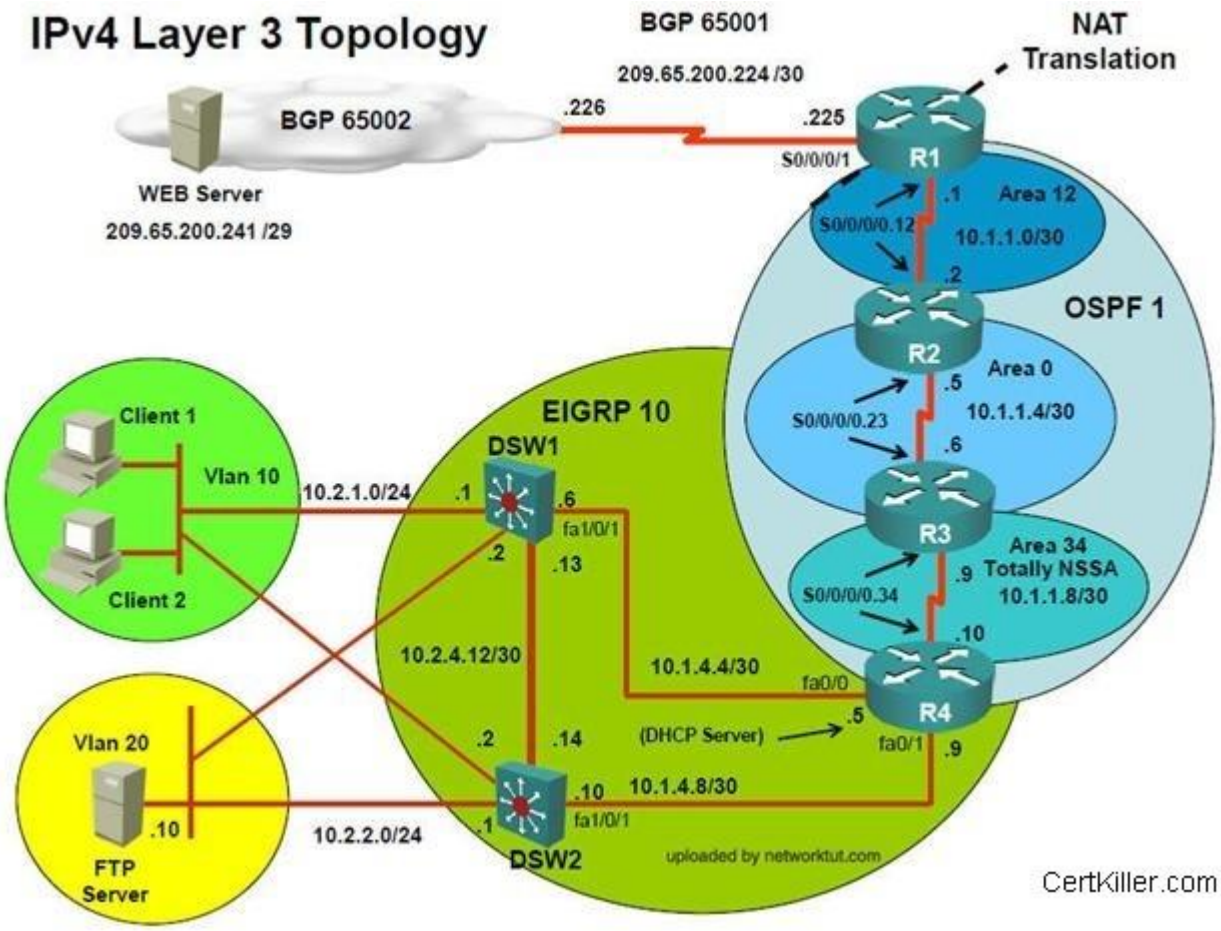

IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT
Translation
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
EIGRP 10
Client 1
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
R3
Area 34
Totally NSSA
.2
.13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

Figure 1

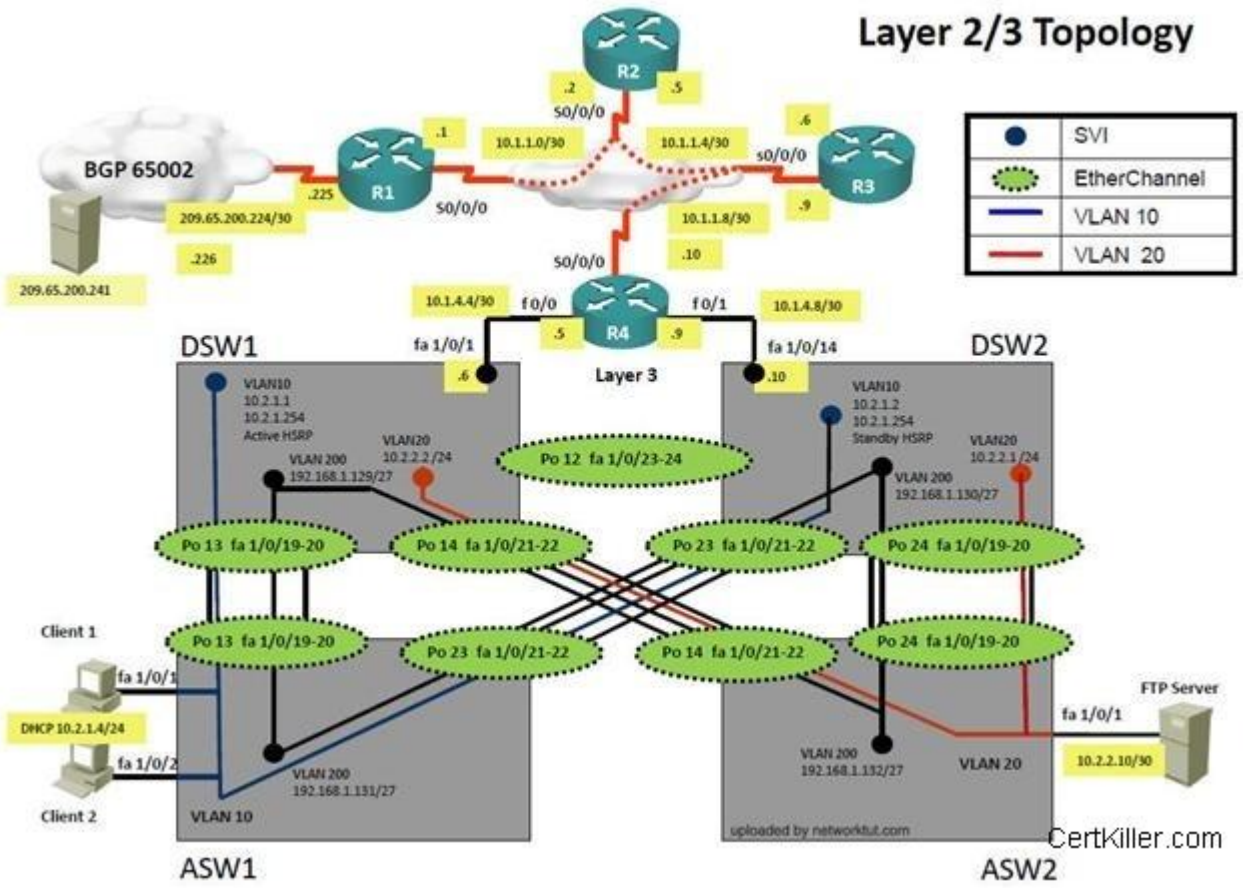


Figure 2

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

Configuration on R4

Configuration on DSW1

router eigrp 10
network 10.1.4.4 0.0.0.0
network 10.2.1.1 0.0.0.0
network 10.2.4.13 0.0.0.0

no auto-summary

Configuration on DSW2

router eigrp 10
network 10.1.4.8 0.0.0.0
network 10.2.2.1 0.0.0.0
network 10.2.4.14 0.0.0.0
no auto-summary

Configuration on R4

router eigrp 10
passive-interface default
redistribute ospf 1 route-map OSPF->EIGRP
network 10.1.4.4 0.0.0.3
network 10.1.4.8 0.0.0.3
default-metric 10000 100 255 1 10000
no auto-summary

What is the solution to the fault condition?

A. Configure auto summary on the EIGRP process.
B. Remove “Passive interface” under EIGRP 1 (or in Interface f0/1 and f0/0, something like this)
C. Remove “Passive interface” under EIGRP 10 (or in Interface f0/1 and f0/0, something like this)
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: (none)
Explanation

Explanation/Reference:
Answer: Remove “Passive interface” under EIGRP 10 (or in Interface f0/1 and f0/0, something like this)

Exam O

QUESTION 1
(Ticket 14: IPv6 OSPF)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

The network setup for this trouble ticket is shown in Figure 3.

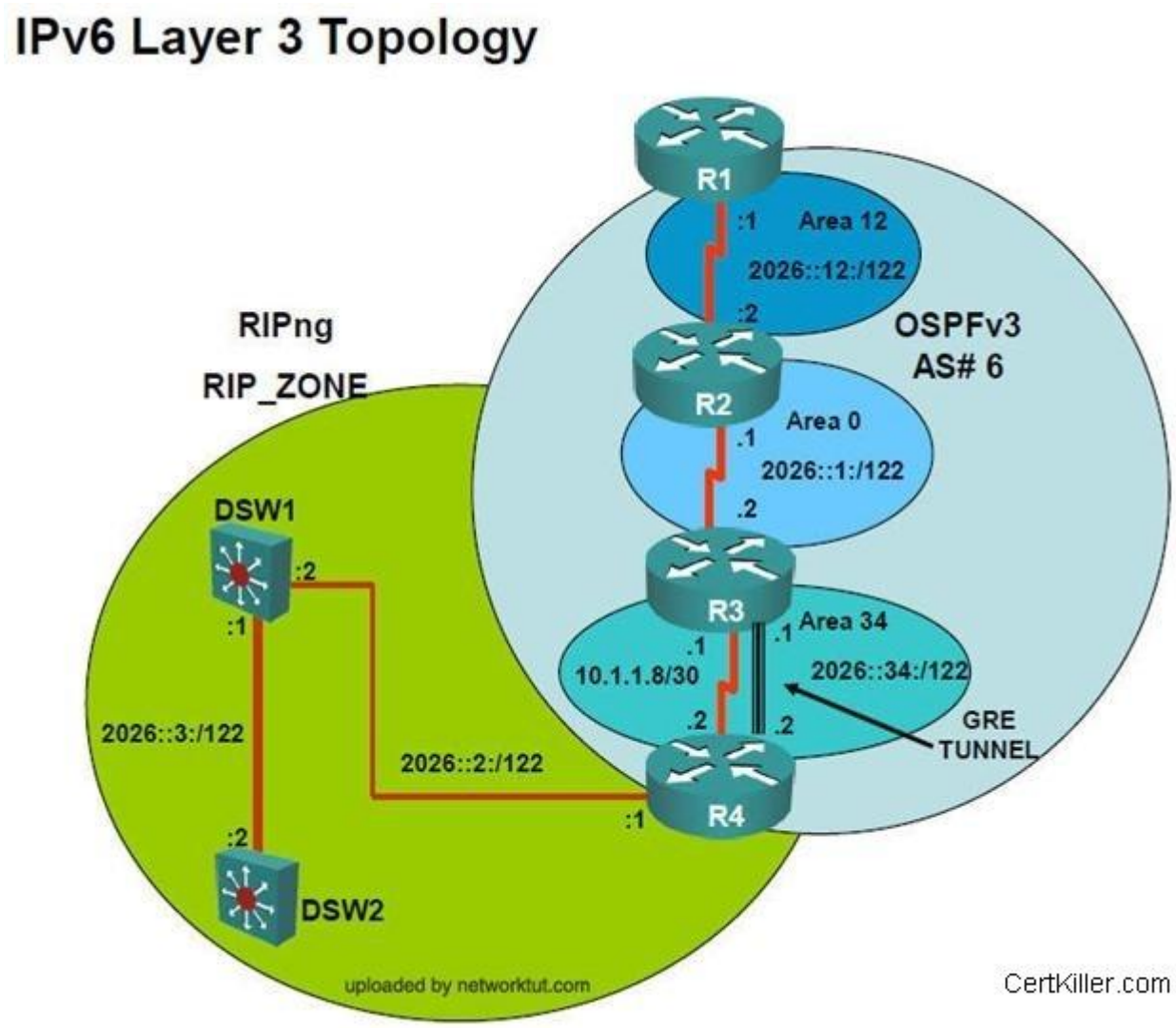


Figure 3

Trouble Ticket Statement

DSW1 and R4 cannot ping R2's loopback or R2's s0/0/0/0.12 IPv6 address. Initial troubleshooting shows and R2 is not an OSPFv3 neighbor on R3.

Configuration on R2

```
ipv6 unicast-routing
!
ipv6 router ospf 6
router-id 2.2.2.2
!
interface s0/0/0.23
ipv6 address 2026::1:1/123
```

Configuration on R3

```
ipv6 unicast-routing
!
ipv6 router ospf 6
router-id 3.3.3.3
!
interface s0/0/0.23
ipv6 address 2026::1:2/122
ipv6 ospf 6 area 0
```

On Which device is the fault condition located?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Answer: R2

QUESTION 2
(Ticket 11: IPv6 OSPF)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

The network setup for this trouble ticket is shown in Figure 3.

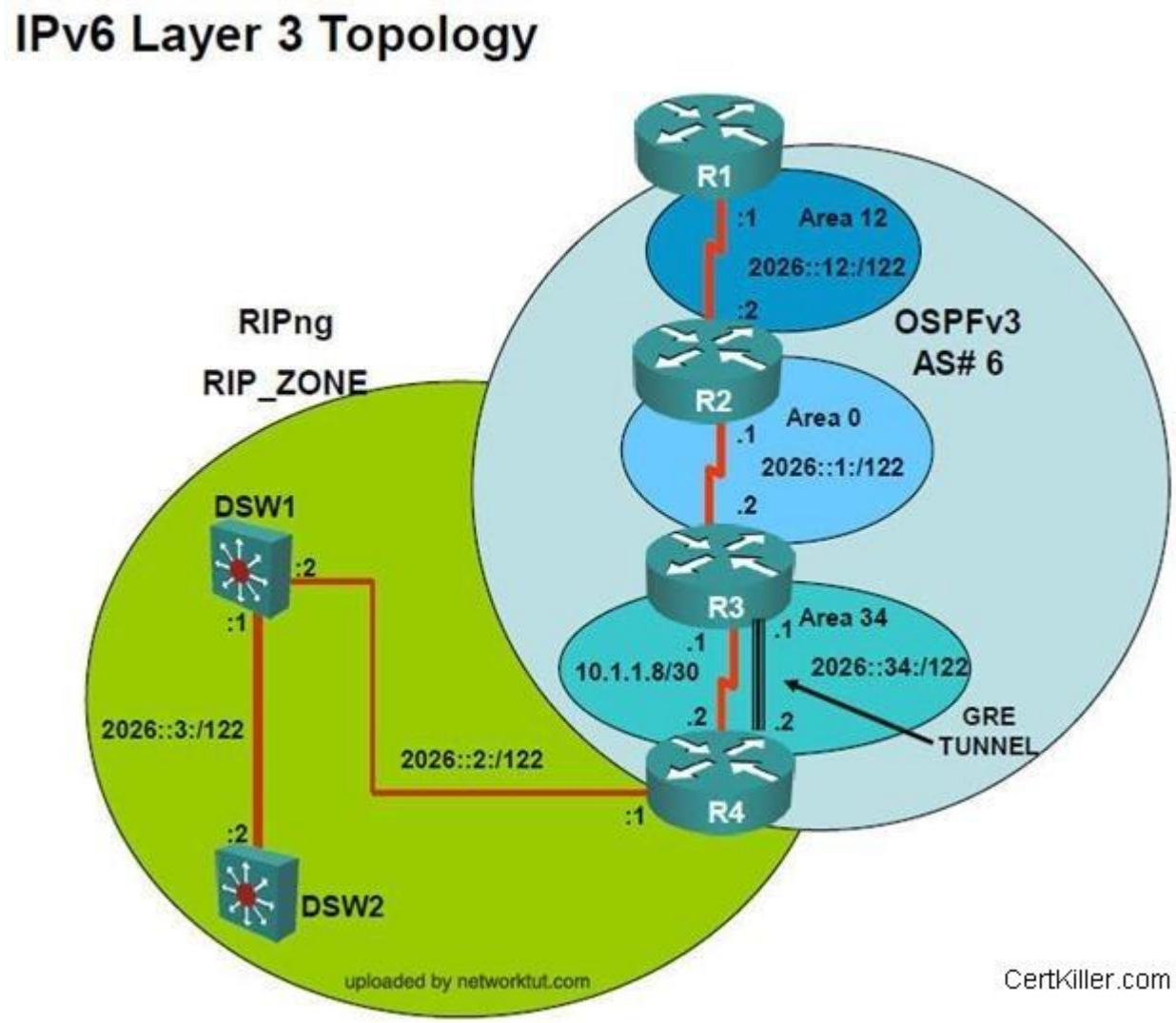


Figure 3

Trouble Ticket Statement

DSW1 and R4 cannot ping R2's loopback or R2's s0/0/0/0.12 IPv6 address. Initial troubleshooting shows and R2 is not an OSPFv3 neighbor on R3.

Configuration on R2

```
ipv6 unicast-routing
!
ipv6 router ospf 6
router-id 2.2.2.2
!
interface s0/0/0.23
ipv6 address 2026::1:1/123
```

Configuration on R3

```
ipv6 unicast-routing
!
ipv6 router ospf 6
router-id 3.3.3.3
!
interface s0/0/0.23
ipv6 address 2026::1:2/122
ipv6 ospf 6 area 0
```

The Fault Condition is related to which technology?

A. IPv6 Addressing
B. Route Redistribution
C. IPv6 OSPF Routing
D. RIPng
E. BGP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Notice: it may be has OSPFv3 for choice. you can try choose and then see next question that has correctly command to solve problem for choice or not

QUESTION 3
(Ticket 11: IPv6 OSPF)

Scenario: The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, 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.

The network setup for this trouble ticket is shown in Figure 3.

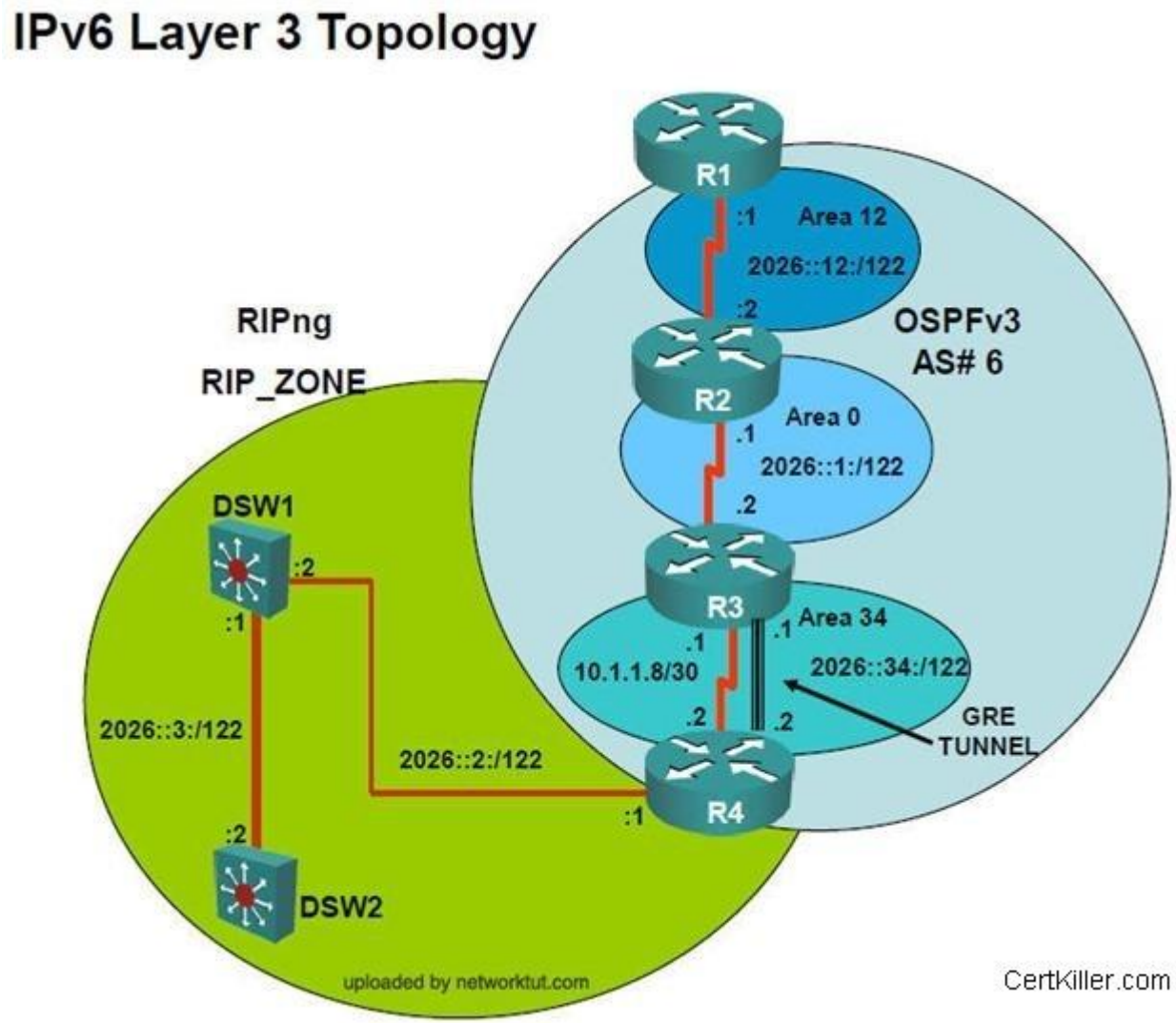


Figure 3

Trouble Ticket Statement

DSW1 and R4 cannot ping R2's loopback or R2's s0/0/0/0.12 IPv6 address. Initial troubleshooting shows and R2 is not an OSPFv3 neighbor on R3.

Configuration on R2

```
ipv6 unicast-routing
!
ipv6 router ospf 6
router-id 2.2.2.2
!
interface s0/0/0.23
ipv6 address 2026::1:1/123
```

Configuration on R3

```
ipv6 unicast-routing
!
ipv6 router ospf 6
router-id 3.3.3.3
!
interface s0/0/0.23
ipv6 address 2026::1:2/122
ipv6 ospf 6 area 0
```

What is the solution of the fault condition?

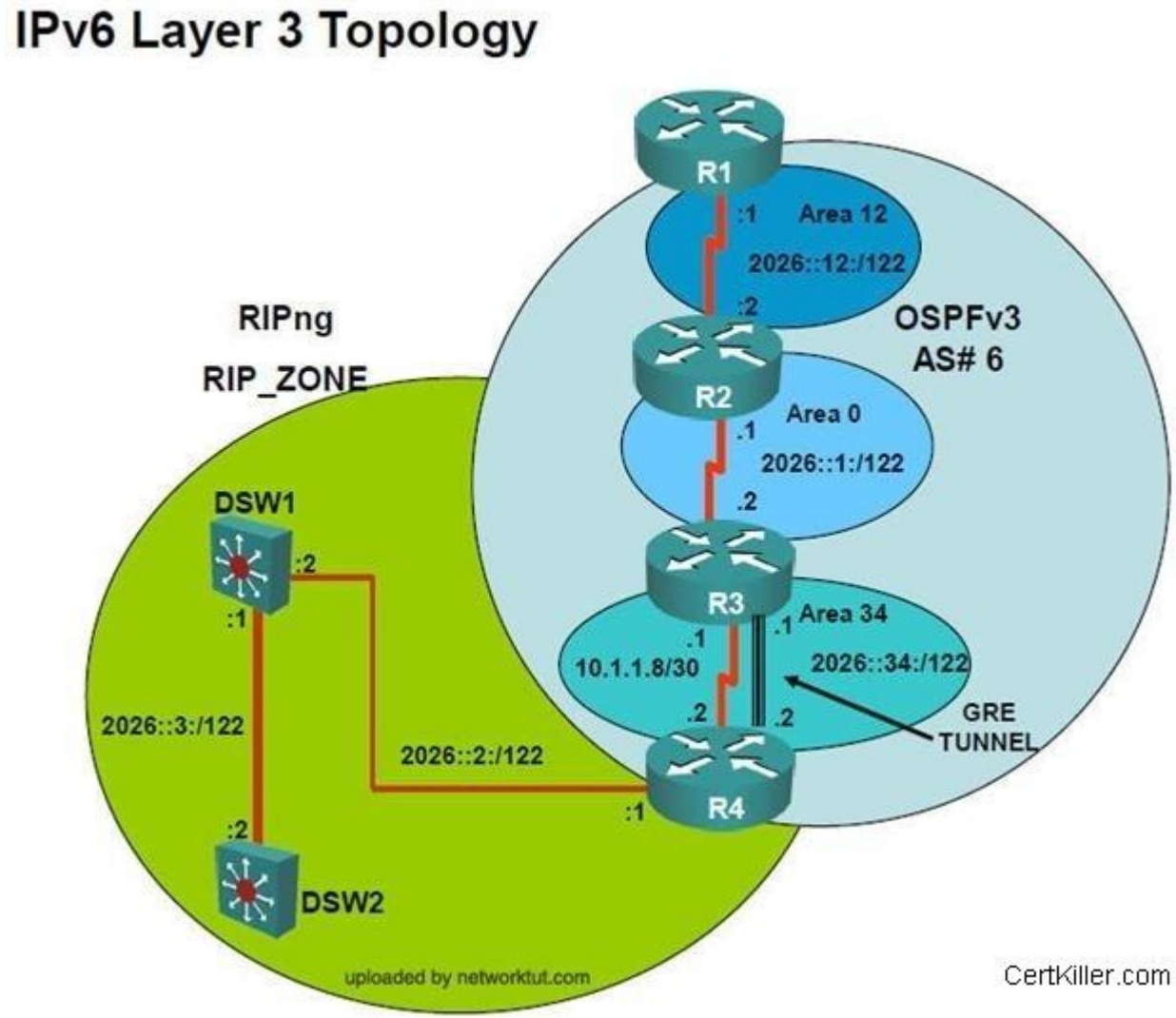
A. enter the command **ipv6 ospf 6 area 0** under S0/0/0.23 on R2
B. Add ipv6 ospf 6 area 6 under s0/0/0.23 on R2
C. Remove IPv6 address from s0/0/0.23 on R2
D. Enable IPv6 routing on s0/0/0.23 on R2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Answer: Add ipv6 ospf 6 area 0 under S0/0/0.23 on R2 (notice that it is "area 0″, not "area 12″). you maybe see incorrect subnet of IPv6 address at int

Exam P

QUESTION 1



Problem: Loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Configuration of R3:

!

interface Tunnel34

no ip address
ipv6 address 2026::34:1/122
ipv6 enable
ipv6 ospf 6 area 34
tunnel source Serial0/0/0.34
tunnel destination 10.1.1.10
tunnel mode ipv6
!
Configuration of R4:
interface Tunnel34
no ip address
ipv6 address 2026::34:2/122
ipv6 enable
ipv6 ospf 6 area 34
tunnel source Serial0/0/0
tunnel destination 10.1.1.9
!

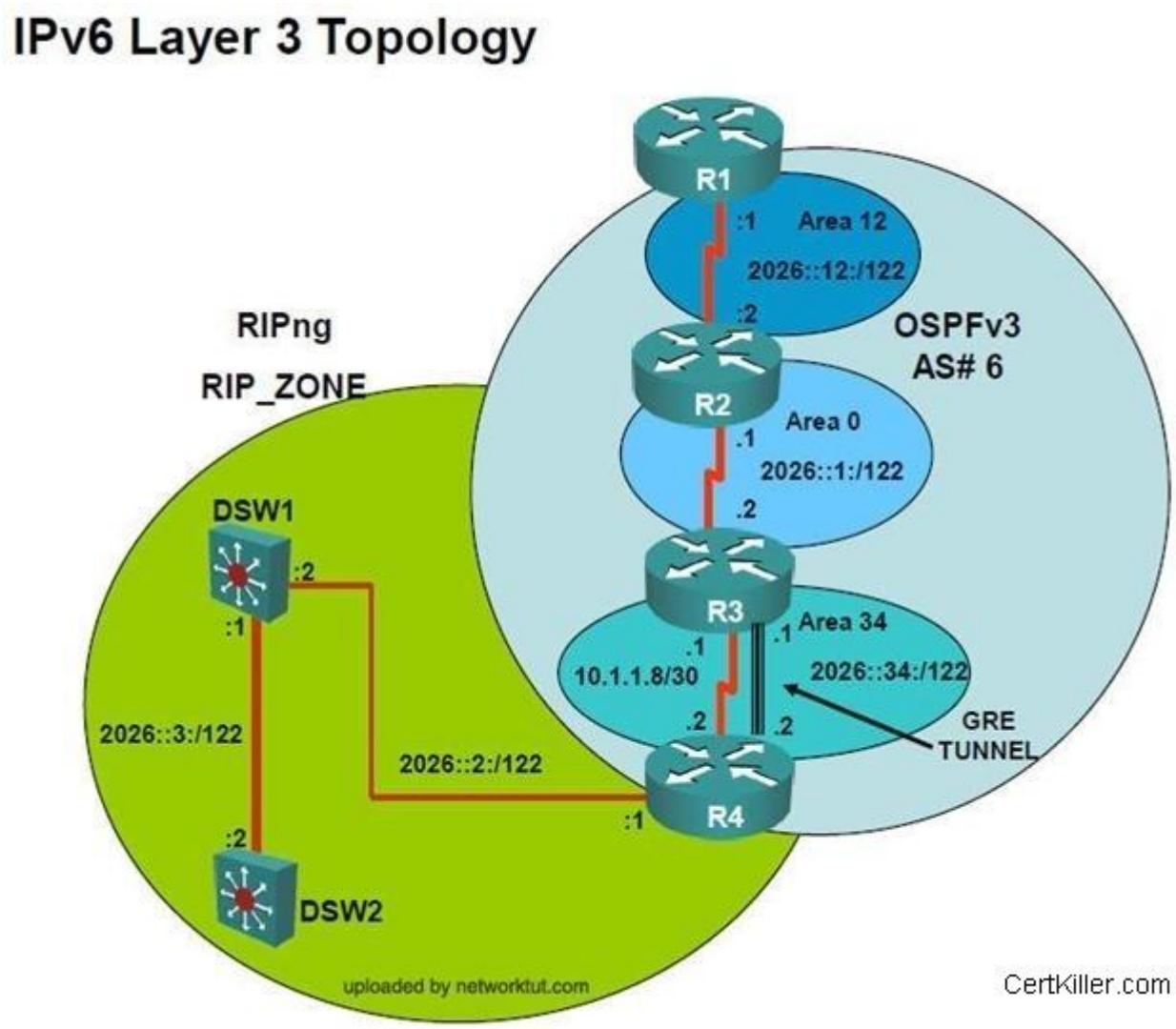
On Which device is the fault condition located?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2



Problem: Loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Configuration of R3:

!
interface Tunnel34
no ip address
ipv6 address 2026::34:1/122
ipv6 enable

ipv6 ospf 6 area 34
tunnel source Serial0/0/0.34
tunnel destination 10.1.1.10
tunnel mode ipv6
!
Configuration of R4:
interface Tunnel34
no ip address
ipv6 address 2026::34:2/122
ipv6 enable
ipv6 ospf 6 area 34
tunnel source Serial0/0/0
tunnel destination 10.1.1.9
!

The Fault Condition is related to which technology?

A. IPv6 OSPF Routing
B. Ipv4 and Ipv6 Interoperability
C. IPv6 RIP Routing
D. OSPFv3
E. IPv6 Addressing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

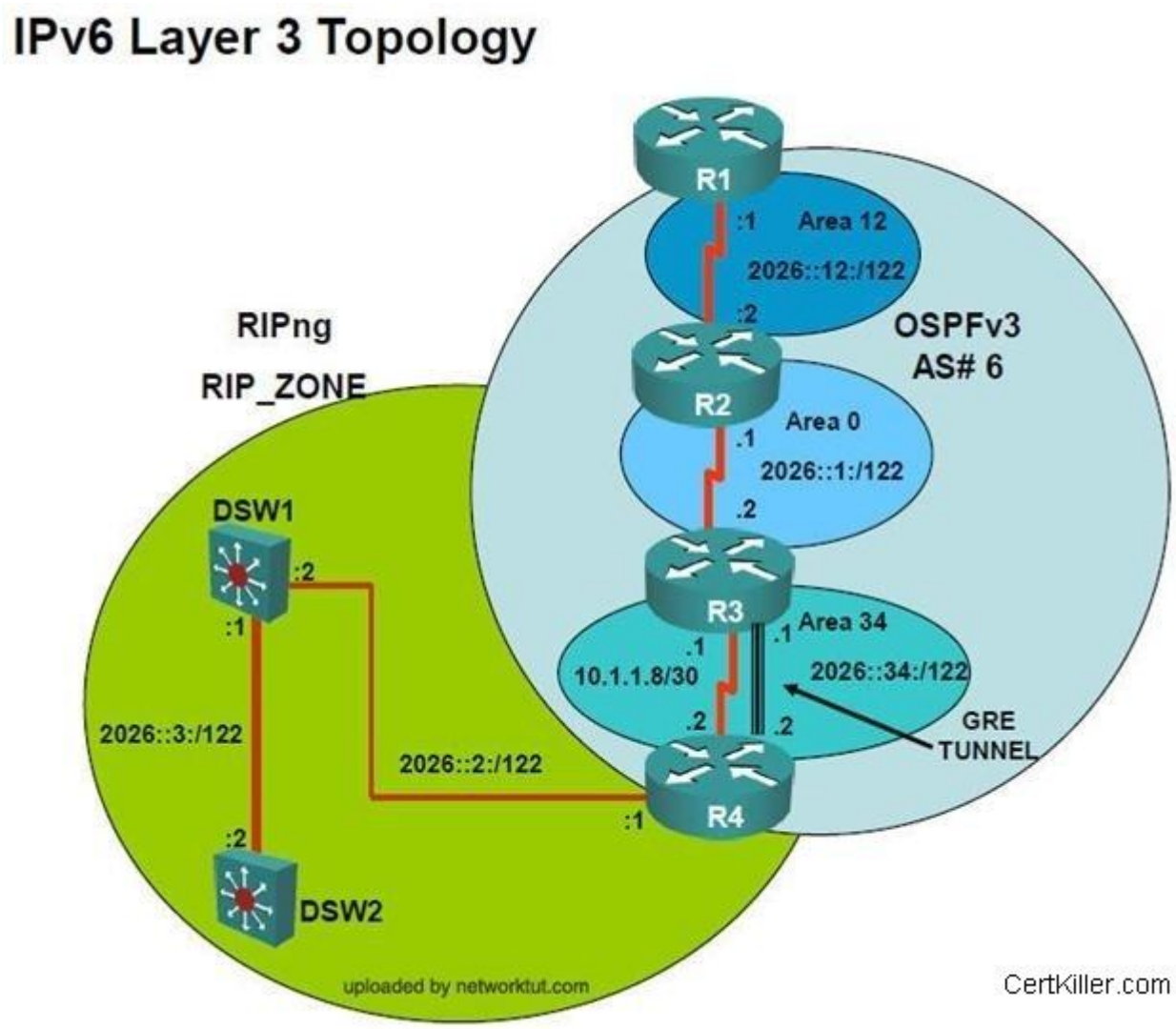
Configuration of R3:

```
!
interface Tunnel34
no ip address
ipv6 address 2026::34:1/122
ipv6 enable
ipv6 ospf 6 area 34
tunnel source Serial0/0/0.34
tunnel destination 10.1.1.10
tunnel mode ipv6
!
```

Configuration of R4:

```
interface Tunnel34
no ip address
ipv6 address 2026::34:2/122
ipv6 enable
ipv6 ospf 6 area 34
tunnel source Serial0/0/0
tunnel destination 10.1.1.9
!
```

QUESTION 3



Problem: Loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Configuration of R3:

!
interface Tunnel34
no ip address
ipv6 address 2026::34:1/122
ipv6 enable

ipv6 ospf 6 area 34
tunnel source Serial0/0/0.34
tunnel destination 10.1.1.10
tunnel mode ipv6
!
Configuration of R4:
interface Tunnel34
no ip address
ipv6 address 2026::34:2/122
ipv6 enable
ipv6 ospf 6 area 34
tunnel source Serial0/0/0
tunnel destination 10.1.1.9
!

What is the solution of fault condition?

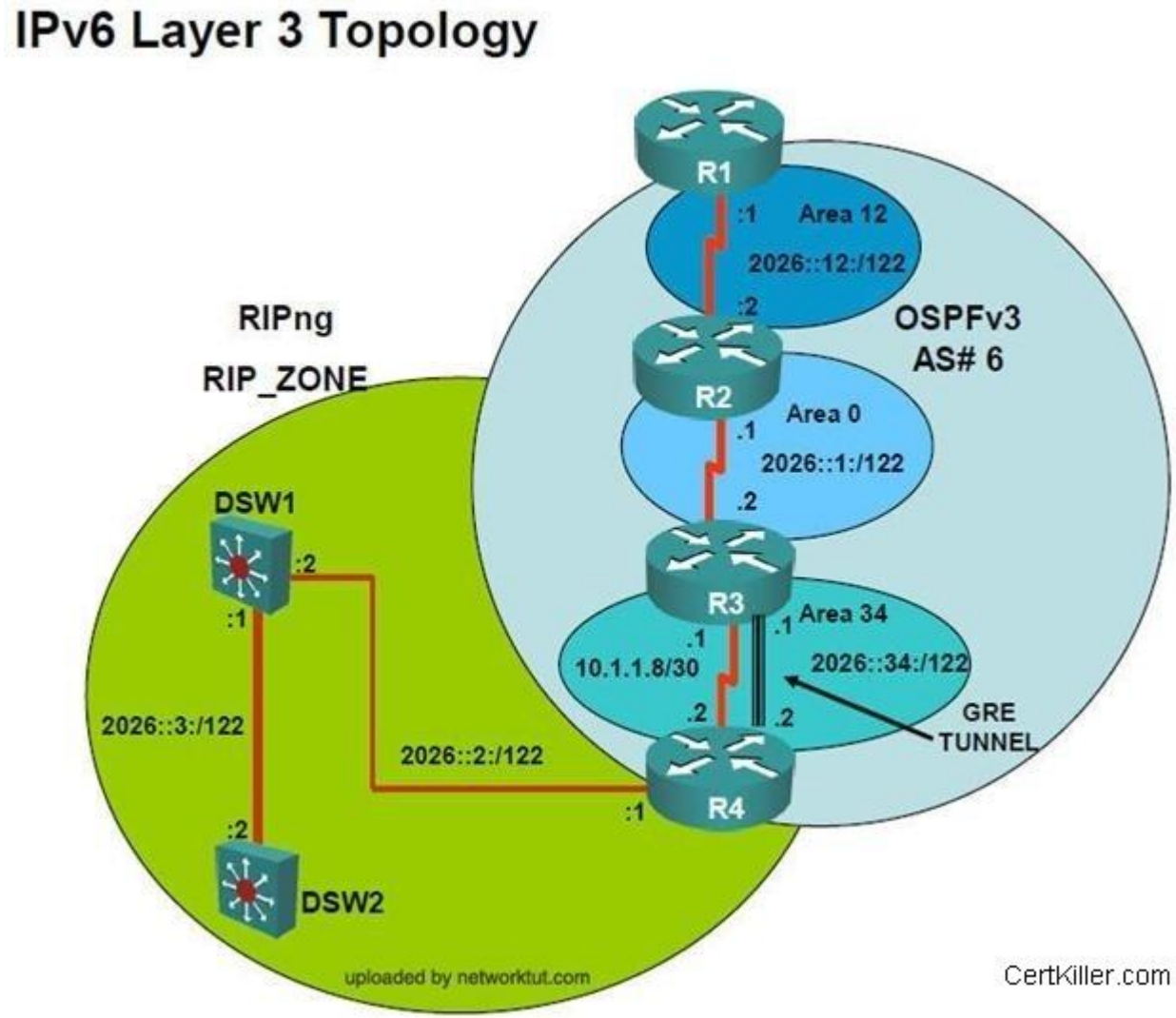
A. R2 address was 2026::1:1/123 when R3 had 2026::1:2/122
B. Under the interface Tunnel34, remove ‘tunnel mode ipv6′ command
C. Enable IPv6 routing on s0/0/0/0.34 on R3
D. Under the interface Tunnel34, remove ‘tunnel mode ipv6ip′ command
E. Under ipv6 ospf process add the ‘redistribute rip RIP_Zone include-connected’ command

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
B or D see command in config at R3 write ipv6 or ipv6ip

Exam Q

QUESTION 1



Problem: Loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Configuration of R4:

ipv6 router ospf 6

log-adjacency-changes

!
ipv6 router rip RIP_ZONE
redistribute ospf 6 metric 2 include-connected
!

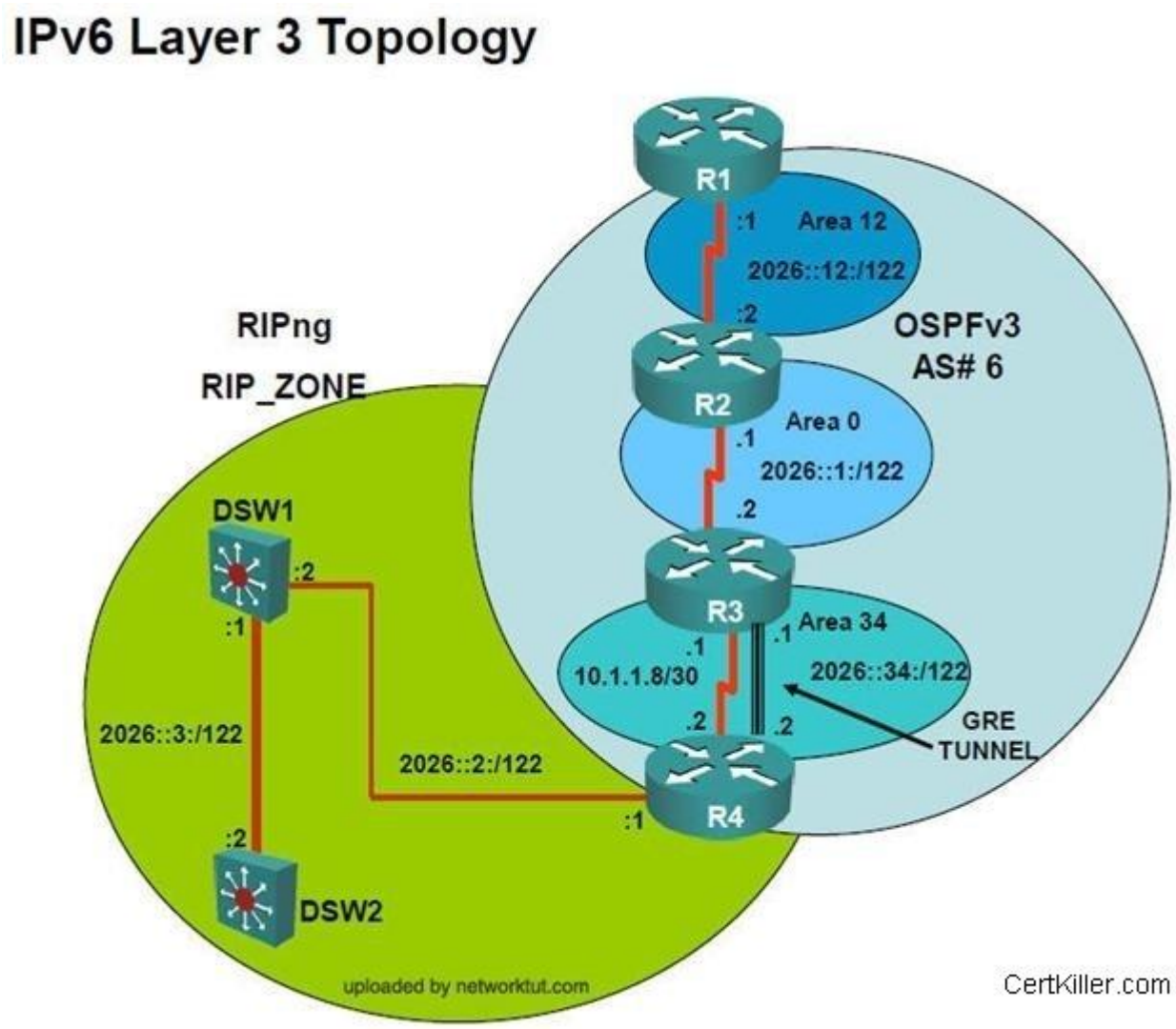
On Which device is the fault condition located?

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2



Problem: Loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Configuration of R4:

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

!

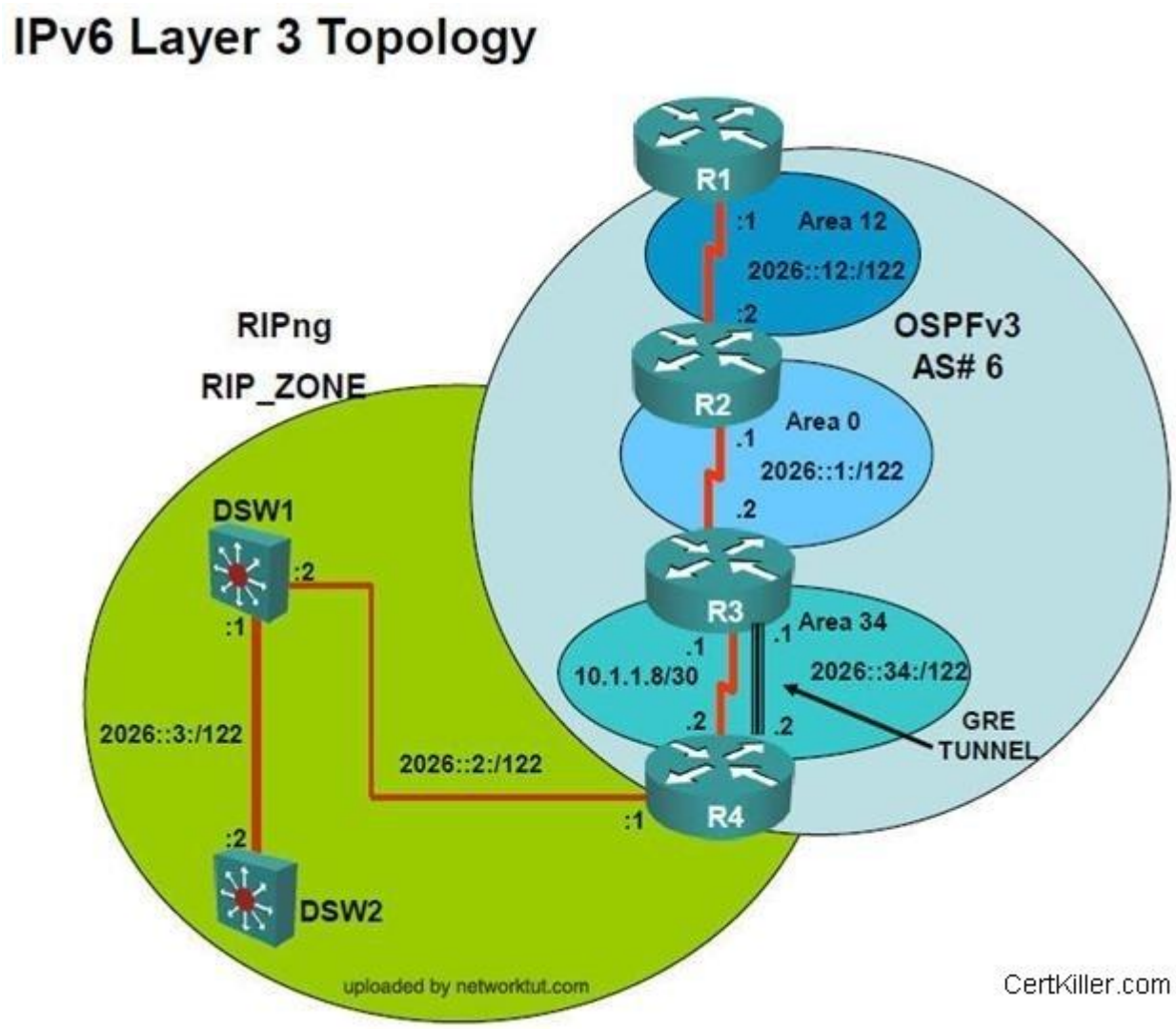
The Fault Condition is related to which technology?

A. IPv6 OSPF Routing
B. Ipv4 and Ipv6 Interoperability
C. IPv6 RIP Routing
D. VRRP
E. IPv6 Addressing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Under ipv6 ospf process add the ‘redistribute rip RIP_Zone include-connected’ command

QUESTION 3



Problem: Loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Configuration of R4:

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

!

What is the solution of fault condition?

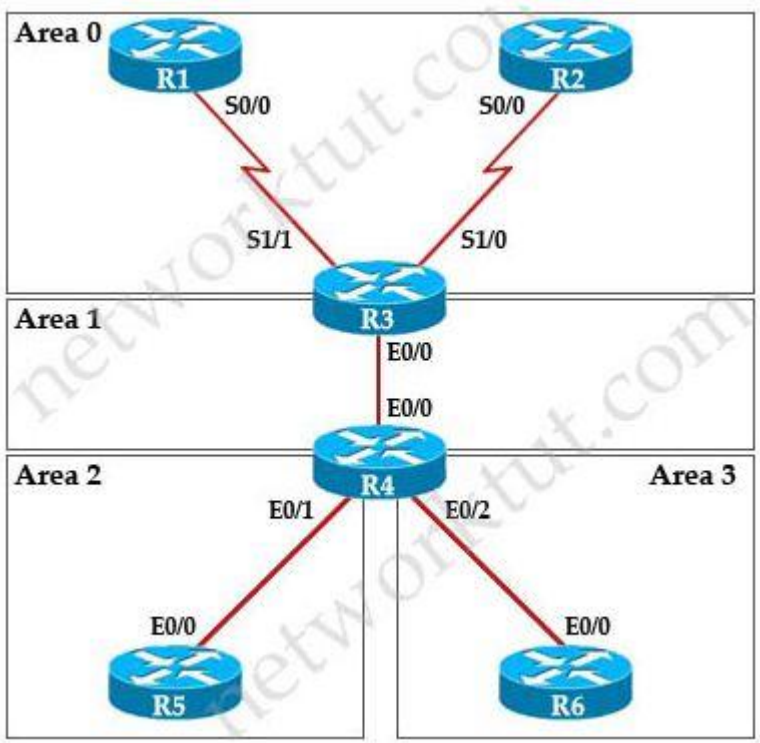
A. Under ipv6 ospf process add the ‘redistribute rip RIP_Zone include-connected’ command
B. Enable IPv6 routing on s0/0/0/0.34 on R4
C. R2 address was 2026::1:1/123 when R3 had 2026::1:2/122
D. Under the interface Tunnel34, remove ‘tunnel mode ipv6ip’ command
E. Add ipv6 ospf 6 area 0 under s0/0/0/0.23 on R2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam R

QUESTION 1
OSPF Sim



The OSPF neighbor 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: (none)
Explanation

Explanation/Reference:
Check the ports connecting between R1 and R3 via the “show running-config” command:

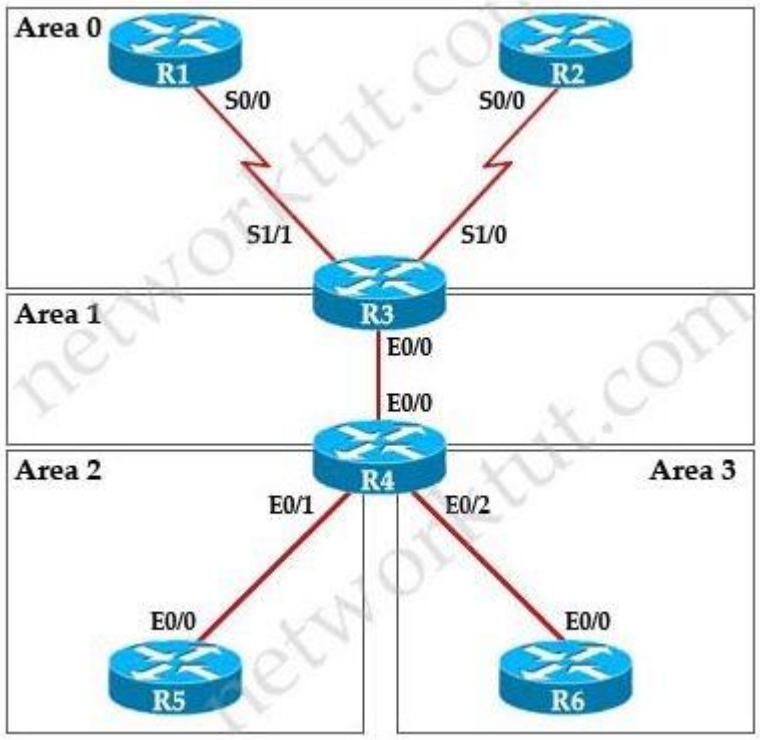
R1#show running-config
<<output omitted>>
interface Serial0/0
ip address 192.168.13.1 255.255.255.0
ip ospf network non-broadcast

R3#show running-config
<<output omitted>>
interface Serial1/1
ip address 192.168.13.3 255.255.255.0
ip ospf network point-to-multipoint non-broadcast

Or you can check these interfaces via the “show ip ospf interface S0/0″ on R1 or “show ip ospf interface S1/1″ on R3 you will see the Network types are “NON_BROADCAST” or “POINT_TO_MULTIPOINT”, respectively. For example:

```
R1#show ip ospf interface serial 0/0
Serial1/0 is up, line protocol is up
  Internet Address 192.168.23.3/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type NON_BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.23.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.23.2
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 7
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

QUESTION 2



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: (none)
Explanation

Explanation/Reference:
We can check the OSPF neighborship on R3 first via the "show ip ospf neighbor" command:

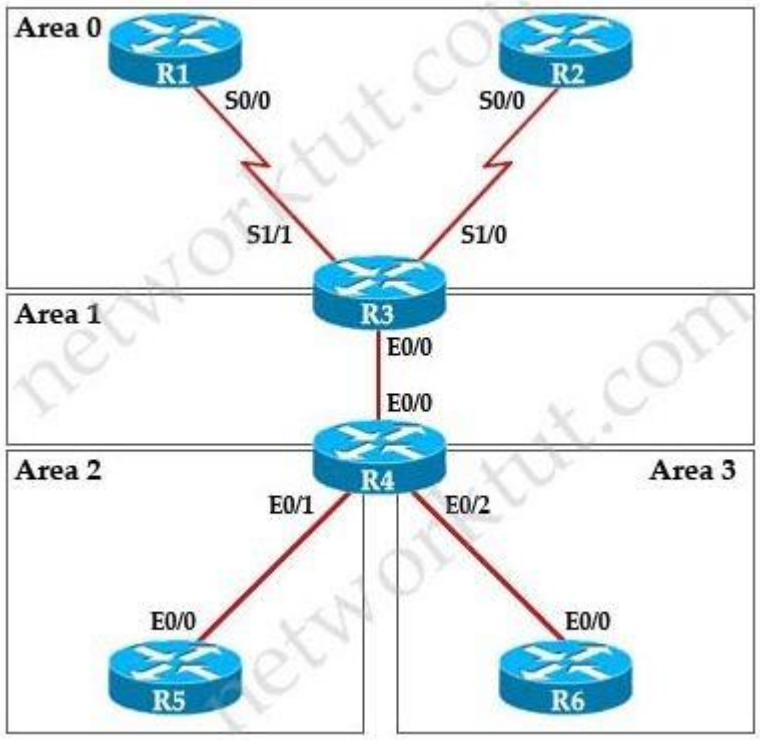
```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:35    192.168.23.2    Serial1/1
2.2.2.2           1   FULL/  -        00:01:40    192.168.13.1    Serial1/0
```

We don't see the OSPF neighborship between R3 and R4 (neighbor 4.4.4.4) so something was wrong with OSPF. So we continue checking with the "show running-config" command and pay attention to the OSPF config between R3 and R4.

```
R3#show running-config
<<output omitted>>
router ospf 100
 router-id 3.3.3.3
 log-adjacency-changes
 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
```

We can realize the link between R3 and R4 is not running OSPF (missing the command "network 192.168.34.0 0.0.0.255 area 1″).

QUESTION 3



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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Check the configuration of R5 with the “show running-config” command:

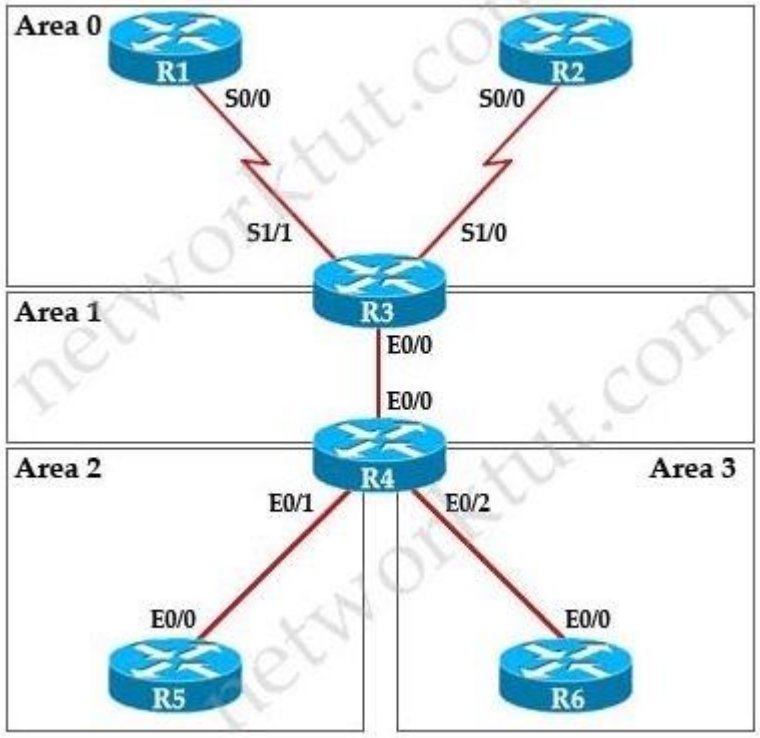
```
R5#show running-config
<<output omitted>>
interface Ethernet0/0
 ip address 192.168.45.5 255.255.255.0
 ip ospf authentication-key CISCO
!
<<output omitted>>
router ospf 100
 router-id 5.5.5.5
 auto-cost reference-bandwidth 3000
 area 2 authentication
 area 2 nssa
 area 2 range 5.5.0.0 255.255.252.0
 network 192.168.45.5 0.0.0.0 area 2
 distribute-list 45 in Ethernet0/1
```

Interface E0/0 of R5 is configured with OSPF authentication so we should check the configuration on interface E0/0 of R4:

```
R4#show running-config
<<output omitted>>
interface Ethernet0/1
 ip address 192.168.45.4 255.255.255.0
!
```

There is no OSPF authentication under E0/1 of R4 so R4 cannot establish OSPF neighborship with R5.

QUESTION 4



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: (none)
Explanation

Explanation/Reference:
Only the 6.6.0.0 subnets are not reachable from R4 so maybe something blocking it (OSPF neighborship is still formed between R4 and R6. You can verify with the “show ip ospf neighbor” command). Check the configuration of R6 with the “show running-config” command and pay attention to the

OSPF part of R6:

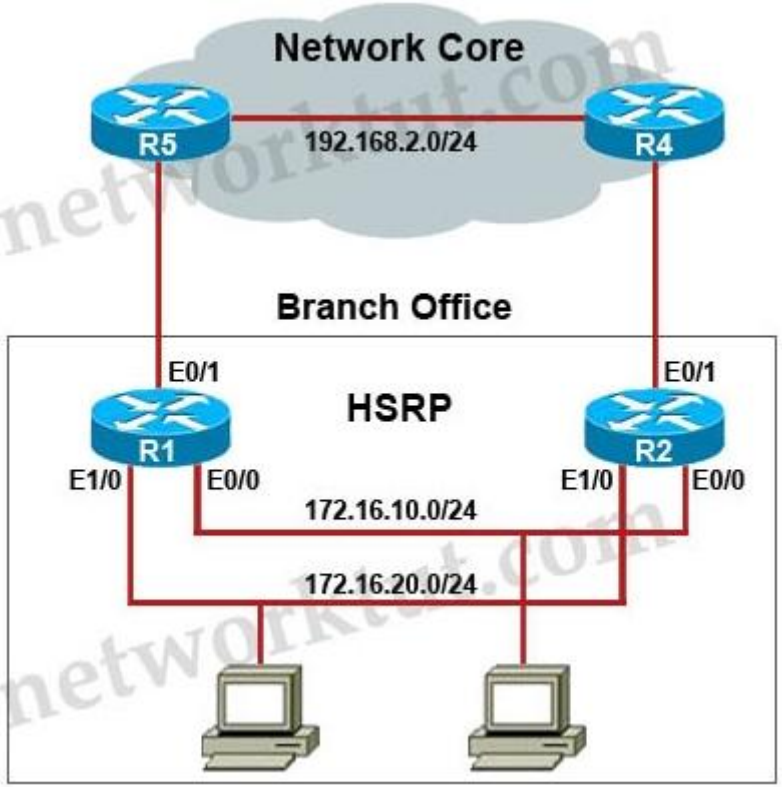
```
R6#show running-config
<<output omitted>>
router ospf 100
 router-id 6.6.6.6
 auto-cost reference-bandwidth 3000
 area 3 stub no-summary
 redistribute connected
 network 192.168.46.0 0.0.0.255 area 3
 distribute-list 64 in Ethernet0/1
 distribute-list 46 in Loopback0
 distribute-list 64 out
!
access-list 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
!
```

From the output we learn that R6 is using distribute-lists to filter routes. Especially distribute-list 64 (note: 64 is the access-list number) is applied to:
+ Inbound direction on E0/1 (distribute-list 64 in Ethernet0/1): this distribute-list is no harm because it only prevents 6.0.0.0/8 prefix from learning back from E0/1.
Notice that R6 can still advertise this prefix to the outside.
+ Outbound direction of all interfaces (distribute-list 64 out): this distribute-list is causing problem
because it prevents 6.0.0.0/8 prefix from advertising to the outside ->R4 does not know how to reach 6.6.0.0 subnets.
To fix this problem we should remove “distribute-list 64 out” on R6.

Note: Although the next line of this distribute-list allows prefix 6.6.0.0/16 but traffic for this prefix can never reach this line
because the above line “access-list 64 deny 6.0.0.0 0.255.255.255″ is always matched first and this prefix is dropped.

Exam S

QUESTION 1



```
R1#show running-config
<output omitted>
!
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
!
```

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: (none)
Explanation

Explanation/Reference:
Check the configuration of R1 with the “show running-config” command:

```
R1#show running-config
<output omitted>
!
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
!
```

R1 connects to R5 via E0/1 interface but R1 is tracking E0/0 which connects to R2 -> when the link between R1 & R5 fails the HSRP priority of R1 is still the same. To correct this problem we have to change the tracking interface to E0/1.

QUESTION 2
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: Et0/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP 172.16.10.254
R1#
`Mar 26 11:17:40.364: HSRP: Et0/0 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: Et0/0 Grp 1 Hello out 172.16.10.2 Active pri 130 vIP 172.16.10.254
`Mar 26 11:17:42.918: HSRP: Et0/0 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: Et0/0 Grp 1 Hello out 172.16.10.2 Active pri 130 vIP 172.16.10.254
`Mar 26 11:17:45.718: HSRP: Et0/0 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: Et0/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
`Mar 26 11:17:48.322: HSRP: Et0/0 Grp 1 Hello out 172.16.10.2 Active pri 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: Et0/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
`Mar 26 11:17:50.921: HSRP: Et0/0 Grp 1 Hello out 172.16.10.2 Active pri 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: Et0/0 Grp 1 Hello out 172.16.10.2 Active pri 130 vIP 172.16.10.254
`Mar 26 11:17:53.633: HSRP: Et0/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP 172.16.10.254
```

```
R1#show running-config
<output omitted>
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#show running-config
<output omitted>
!
access-list 102 deny ip any host 224.0.0.102
access-list 102 permit ip any any
!
```

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: (none)
Explanation

Explanation/Reference:
Check the link between R1 & R2 where HSRP group 2 is running (interface E1/0)

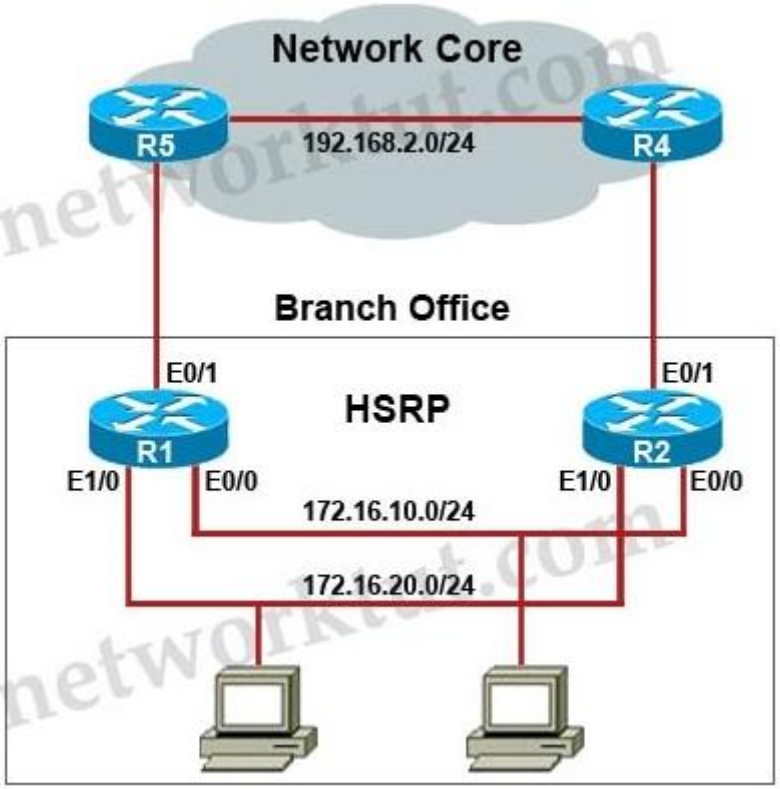
```
R1#show running-config
<output omitted>
interface Ethernet1/0
 description connection to 172.16.20.0/24 network
 ip address 172.16.20.2 255.255.255.0
 ip access-group 102 in
 standby version 2
 standby 2 ip 172.16.20.254
 standby 2 authentication cisco123
```

As we see R1 is using access-list 102 to filter traffic coming to interface E1/0 (inbound direction). Continue checking the access-list 102 of R1:

```
R1#show running-config
<output omitted>
!
access-list 102 deny ip any host 224.0.0.102
access-list 102 permit ip any any
!
```

R1 is blocking any traffic send to 224.0.0.102. Notice that in the syntax of an access-list, the source address is always defined before the destination address. “224.0.0.102” is the muticast address which HSRP version 2 uses to send Hello packets to (instead of 224.0.0.2 of HSRP version 1). Therefore all HSRP sent from neighbor (R2 in this case) to R1 is dropped. R1 keeps sending HSRP Hello packets and think it is the active HSRP router.

QUESTION 3




```
R4#show running-config
<output omitted>
!
router ospf 10
 network 0.0.0.0 255.255.255.255 area 0
 distribute-list 1 in
!
```

```
R4#show running-config
<output omitted>
!
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
!
```

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: (none)
Explanation

Explanation/Reference:
Checking what is preventing the two networks 172.16.10.0/24 & 172.16.20.0/24 from learning on R4.

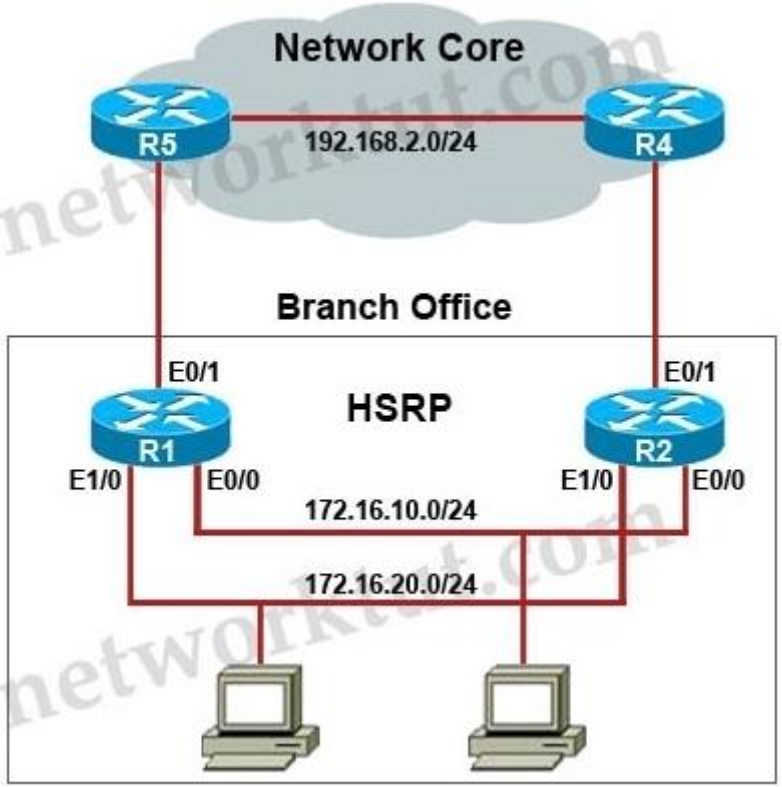
```
R4#show running-config
<output omitted>
!
router ospf 10
 network 0.0.0.0 255.255.255.255 area 0
 distribute-list 1 in
!
```

There is a distribute-list applied on R4. Notice that a distribute-list is often used to control which routing updates should be sent or received on a router. So we should check what this distribute-list is used for. This distribute-list is based on access-list 1 so we will continue checking this access-list:

```
R4#show running-config
<output omitted>
!
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
!
```

This access-list explicitly blocks the two networks 172.16.10.0/24 & 172.16.20.0/24 from populating into R4 routing table.

QUESTION 4



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 R5 and 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: (none)
Explanation

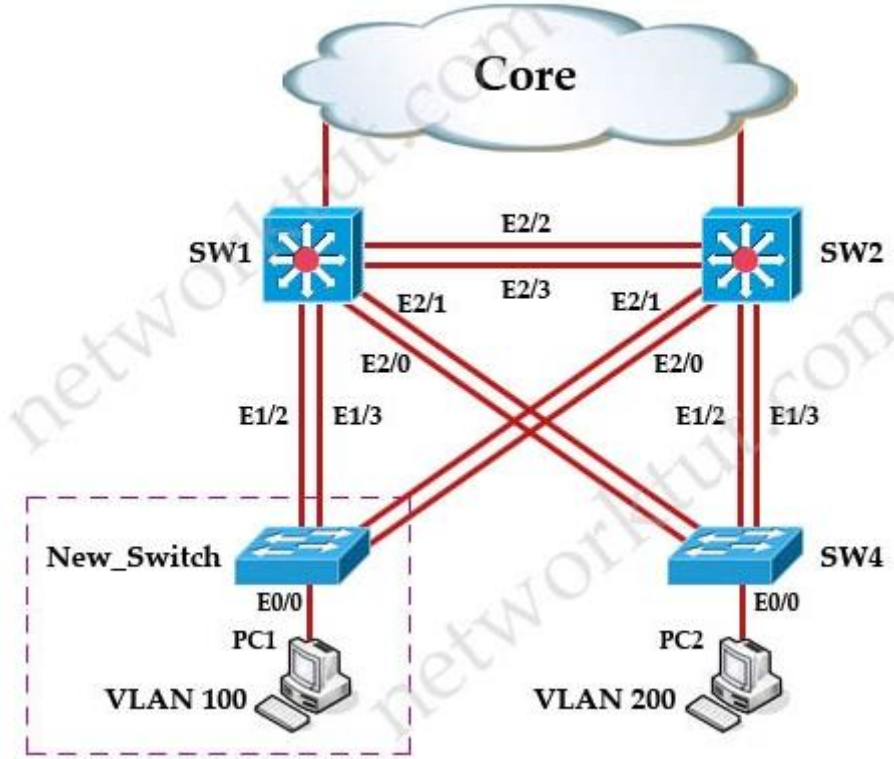
Explanation/Reference:
We don't have enough information to solve this question. But check the OSPF neighbor between R4 and R5 via the command "show ip ospf neighbors" we will not see any entries so we can conclude there is a OSPF issue between R5 & R4 or a distribute-list configured on R5 is blocking the multicast address of OSPF (224.0.0.5 & 224.0.0.6) so you should check the configs of R4 & R5 carefully.

-"sh ip int br" on both R4 and R5, the link between those routers does NOT have ip add for both routers' interface; state that DHCP up/up.

IF Both R4/R5 has an interface up/up with dhcp enabled with no ip address So ANS: c - DHCP issue

Exam T

QUESTION 1




```
New_Switch#show running-config
<output omitted>
interface Ethernet2/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
 spanning-tree bpdufilter enable
 spanning-tree guard loop
!
```

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

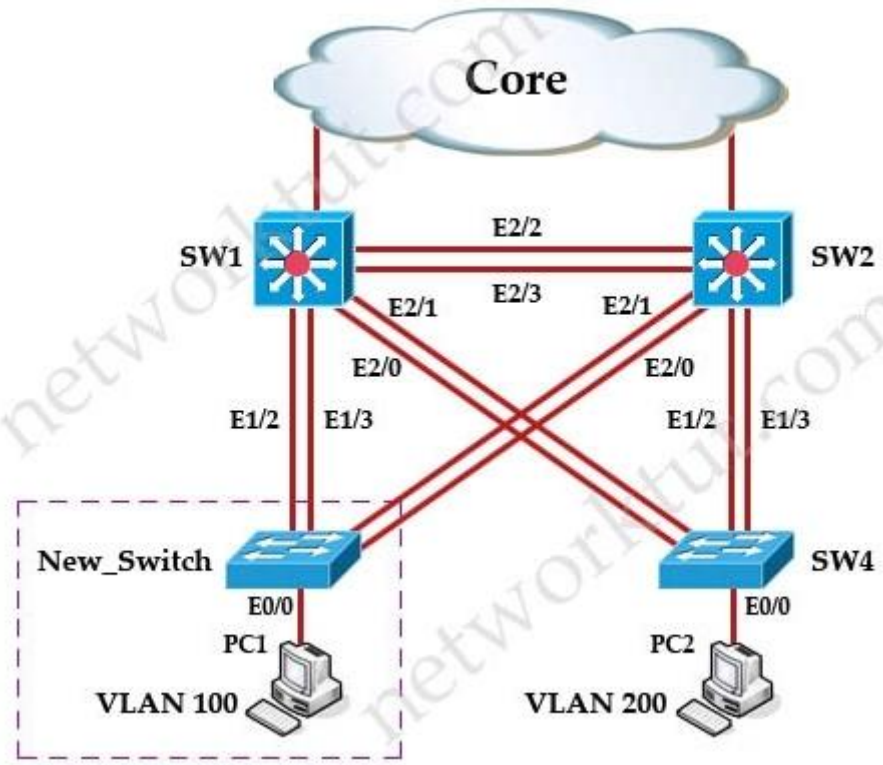
A. Loopguard configured on the New_Switch places the ports in loop inconsistent state
B. Rootguard configured on SW1 places the ports in root inconsistent state
C. Bpduguard configured on the New_Switch places the access ports in error-disable
D. Rootguard configured on SW2 places the ports in root inconsistent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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
We don't have enough information to answer this question.. But under interface Ethernet2/1 of the New_Switch we see Loopguard is configured so answer A is correct. But it may not a STP issue if Ethernet2/1 is blocked because Loopguard should be placed on blocked/alternative ports to prevent unidirectional links.

```
New_Switch#show running-config
<output omitted>
interface Ethernet2/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
 spanning-tree bpdufilter enable
 spanning-tree guard loop
!
```

QUESTION 2




```
New_Switch#show running-config
<output omitted>
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
!
```

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

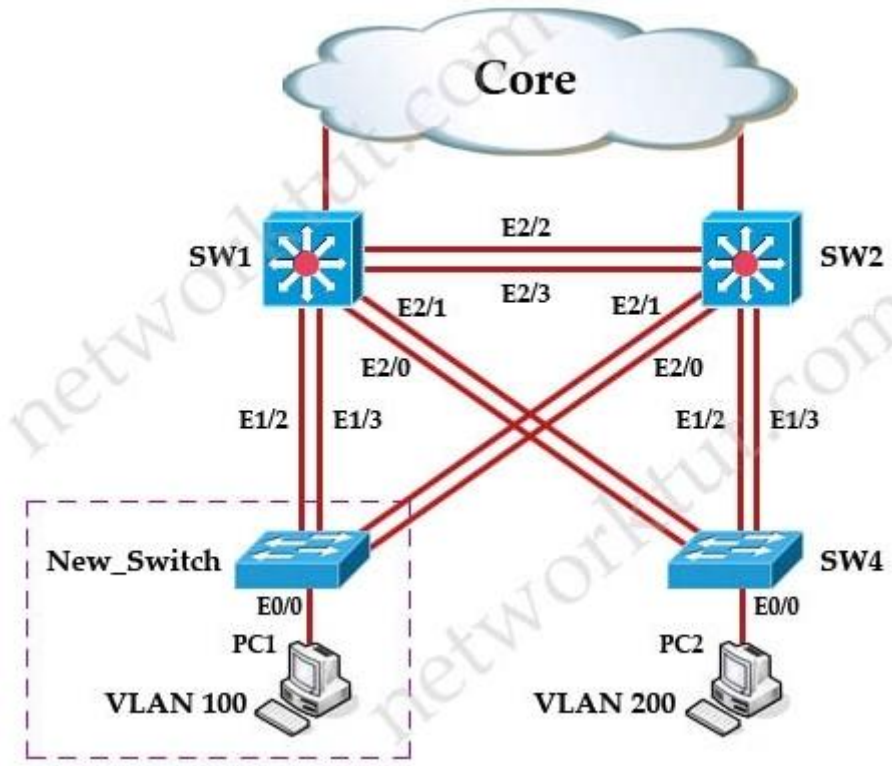
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Check interfaces E1/2 & E1/3 of New_Switch which are directly connected to SW1 with the “show running-config” command:

```
New_Switch#show running-config
<output omitted>
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
!
```

We can see the STP cost of E1/3 was configured to 250 so traffic will not go through this interface but E1/2 is still using the default value (STP cost of 100 for Ethernet port). If we use the default settings then traffic will go directly from SW1 to the New_Switch via E1/2. To force traffic to go through the links E2/2 and E2/3 of SW1.
we can increase the cost of E1/2 (should be greater than 200 because by default the STP cost from SW1 -> SW2 -> New_Switch is 200).

QUESTION 3




```
interface Ethernet0/0
 description Connected to PC2
 switchport mode access
 duplex auto
!
```

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: D
Section: (none)

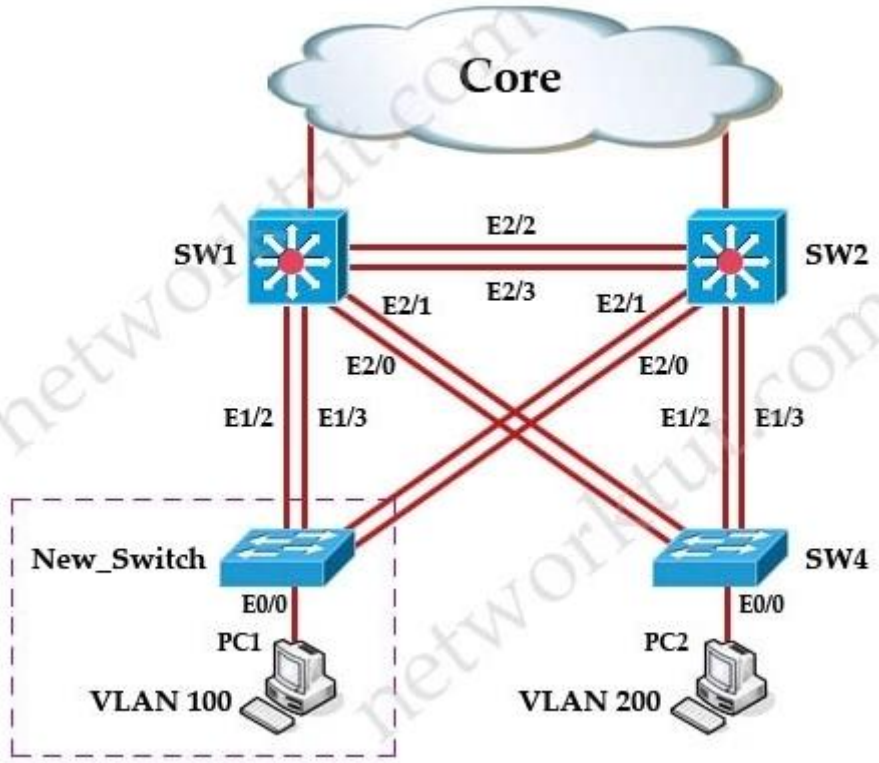
Explanation

Explanation/Reference:
Check the interface E0/0 of SW4 via the “show running-config” command:

```
interface Ethernet0/0
 description Connected to PC2
 switchport mode access
 duplex auto
!
```

E0/0 is in access mode but no VLAN is associated with this interface so it belongs to VLAN 1 by default. Note: You can double check with the “show vlan” command to see no vlan 200 was created on SW4.

QUESTION 4



```
SW1#show running-config
<output omitted>
!
interface Vlan300
 ip address 192.168.10.1 255.255.255.0
!
```

```
SW4#show running-config
<output omitted>
!
interface Vlan300
 ip address 192.168.100.4 255.255.255.0
!
```

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: (none)
Explanation

Explanation/Reference:
From the output of the “show vlan” (or “show running-config”) command on SW1, we learn VLAN 300 is named “Management_VLAN” so we need to check the connection of VLAN 300 between SW1 and SW4.

Issue the “show running-config” on SW1 & SW4 to check the IP addresses of their Interface VLAN:

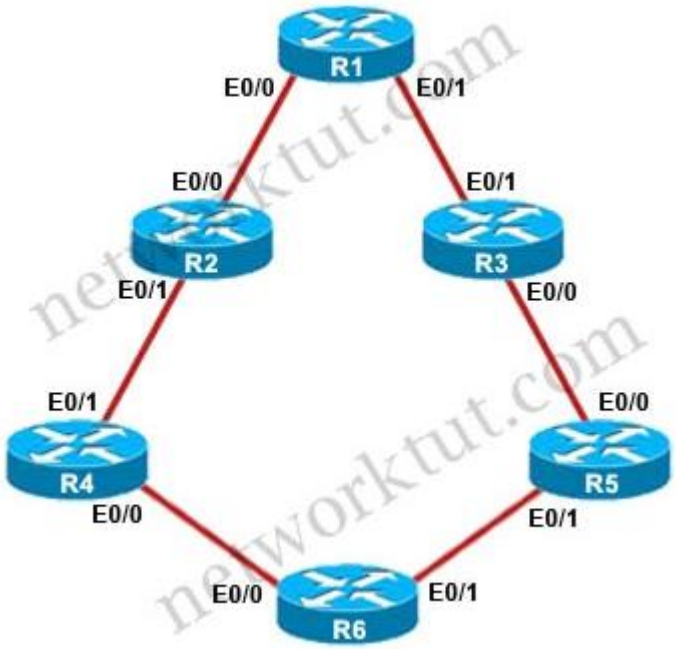
```
SW1#show running-config
<output omitted>
!
interface Vlan300
 ip address 192.168.10.1 255.255.255.0
!
```

```
SW4#show running-config
<output omitted>
!
interface Vlan300
 ip address 192.168.100.4 255.255.255.0
!
```

We can see that the IP addresses of these two interfaces are not in the same subnets (192.168.10.1/24 & 192.168.100.4/24). We can double check the IP address of interface VLAN 30 on Sw2 to see it belongs to 192.168.10.0/24 subnet.

Exam U

QUESTION 1




```
R5#show running-config
<output omitted>
router eigrp 1
 distribute-list 3 in Ethernet0/0
 distribute-list 3 in Ethernet0/1
 network 192.168.35.0
 network 192.168.56.0
```

```
R5#show running-config
<output omitted>
!
access-list 1 permit 192.168.1.15
access-list 1 permit 192.168.1.24
access-list 1 permit 192.168.1.17
access-list 1 permit 192.168.1.20
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny 150.1.1.1
access-list 3 deny 192.168.46.0 0.0.0.255
access-list 3 deny 192.168.24.0 0.0.0.255
access-list 3 deny 192.168.12.0 0.0.0.255
access-list 3 deny 192.168.13.0 0.0.0.255
access-list 3 deny 192.168.56.0 0.0.0.255
!
```

R5 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: (none)
Explanation

Explanation/Reference:

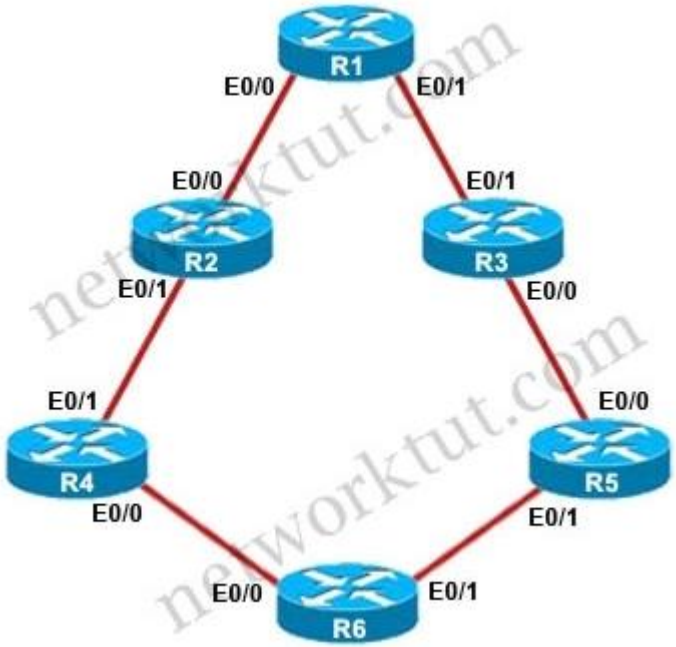
```
R5#show running-config
<output omitted>
router eigrp 1
 distribute-list 3 in Ethernet0/0
 distribute-list 3 in Ethernet0/1
 network 192.168.35.0
 network 192.168.56.0
```

R5 is using distribute-lists (with access-list 3) to filter traffic coming from E0/0 & E0/1. Therefore we continue checking access-list 3:

```
R5#show running-config
<output omitted>
!
access-list 1 permit 192.168.1.15
access-list 1 permit 192.168.1.24
access-list 1 permit 192.168.1.17
access-list 1 permit 192.168.1.20
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny 150.1.1.1
access-list 3 deny 192.168.46.0 0.0.0.255
access-list 3 deny 192.168.24.0 0.0.0.255
access-list 3 deny 192.168.12.0 0.0.0.255
access-list 3 deny 192.168.13.0 0.0.0.255
access-list 3 deny 192.168.56.0 0.0.0.255
!
```

There is no “permit” line in access-list 3 so all traffic is dropped because each access-list always has an implicit “deny all” statement at the end -> R5 cannot learn any routes advertised via EIGRP -> only directly connected will be in the routing table of R5.

QUESTION 2



```
R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.12.1            Et0/0            12 00:10:06    7   100  0  11
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.24.4            Et0/1            14 00:21:29    9   100  0  11
```

```
R4#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.46.6            Et0/0            14 00:11:26    7   100  0  11
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.24.2            Et0/1            14 00:21:29    9   100  0  11
```

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: (none)
Explanation

Explanation/Reference:
Check on R2 & R4 with the “show ip eigrp neighbors” command (or maybe the “show ip eigrp interfaces” command also works for this sim):

```
R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.12.1            Et0/0            12 00:10:06    7   100  0  11
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.24.4            Et0/1            14 00:21:29    9   100  0  11
```

```
R4#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.46.6            Et0/0            14 00:11:26    7   100  0  11
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.24.2            Et0/1            14 00:21:29    9   100  0  11
```

We see the segments R1 – R2; R4 – R6 are running EIGRP AS 1 while the segment R2 – R4 is running EIGRP AS 100 -> These segments cannot see each other. Therefore we have move the segment R2 – R4 to EIGRP AS 1.