300-135.prepaway.premium.exam.147q

Number: 300-135
Passing Score: 800
Time Limit: 120 min
File Version: 13.0

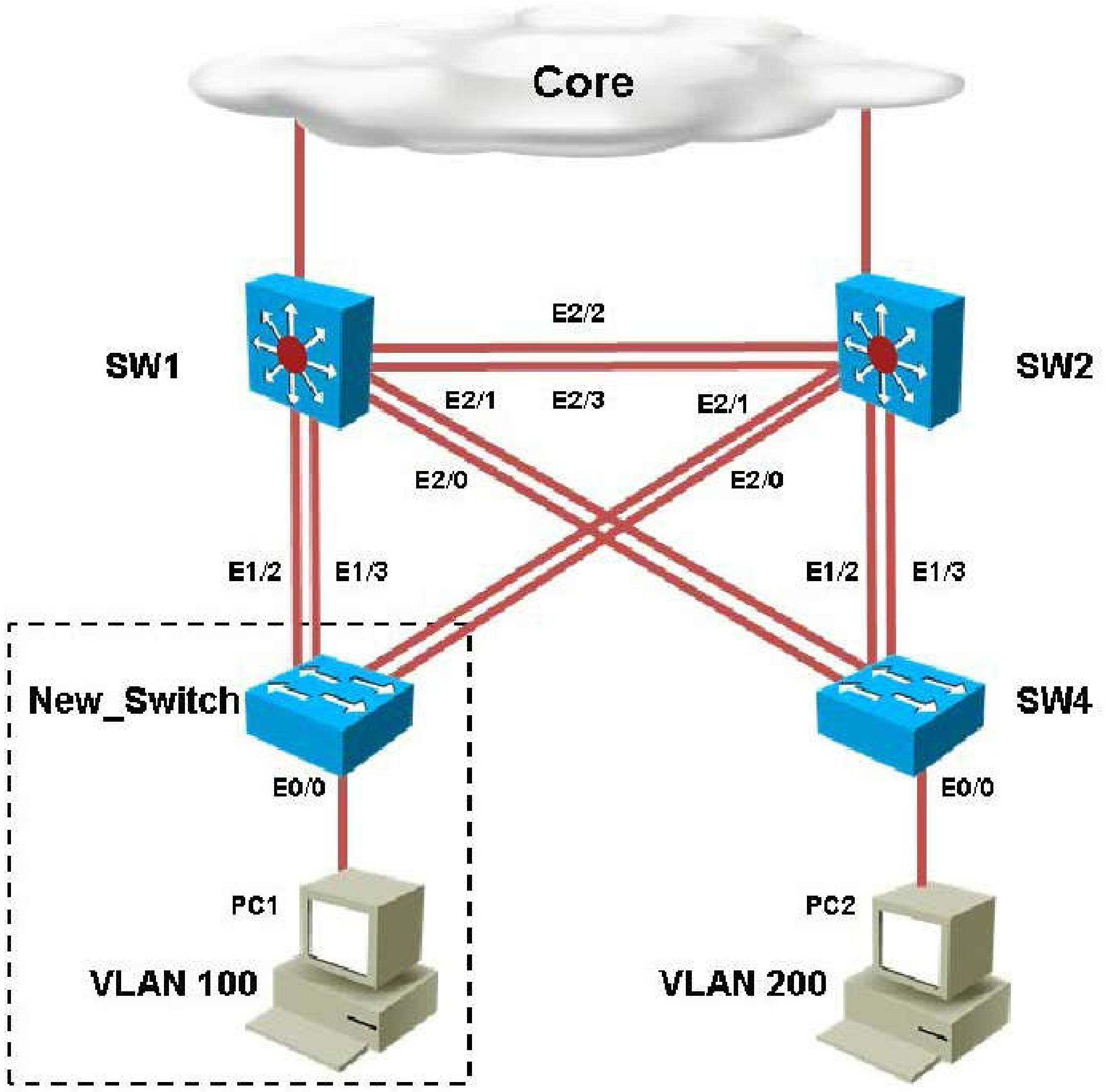
300-135

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

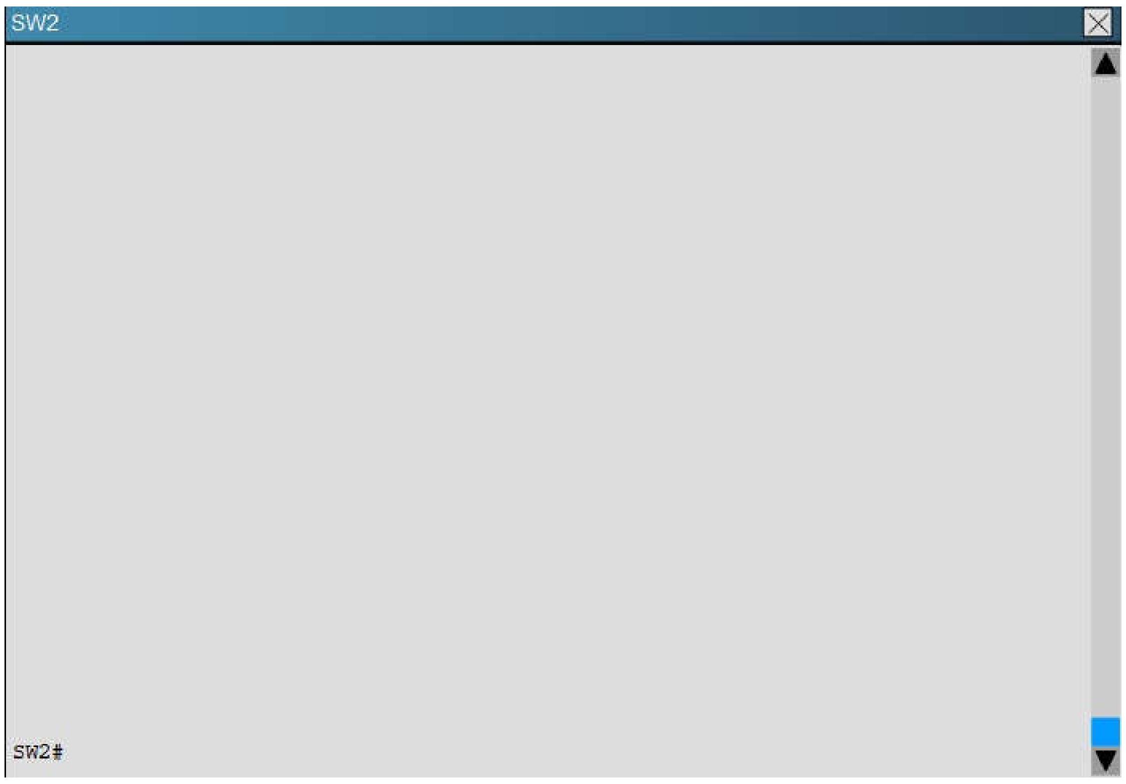
Version 13.0

Question Set 1

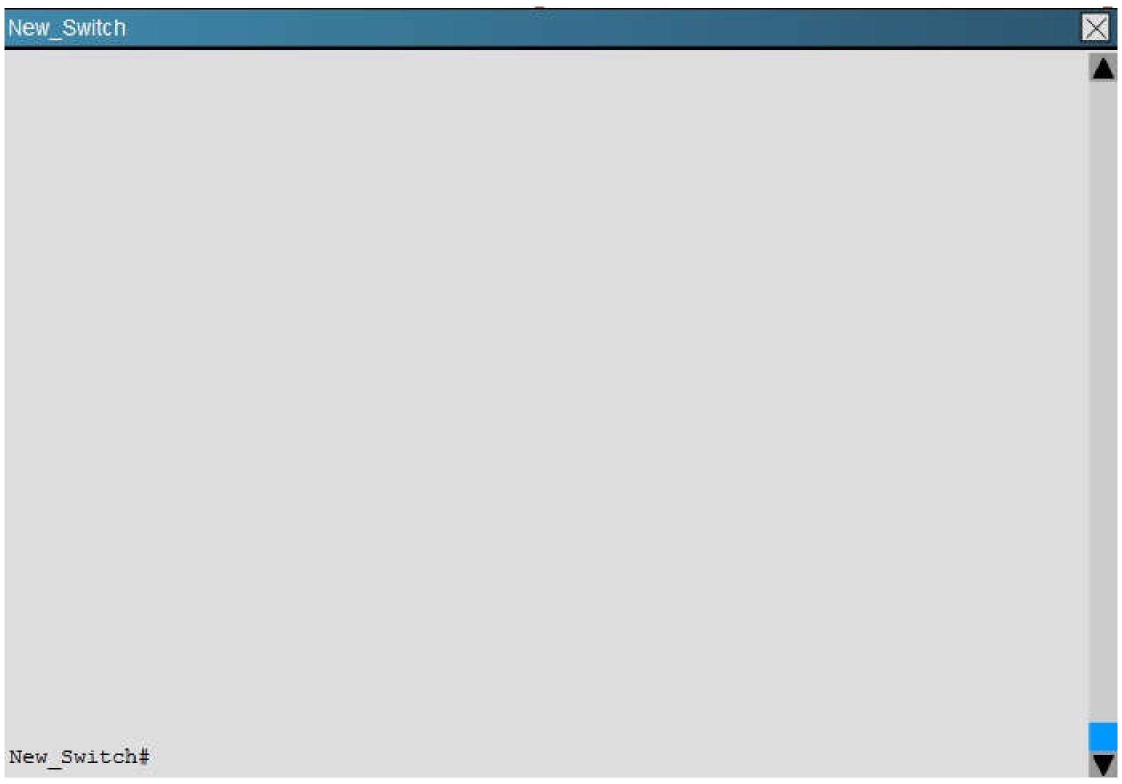
QUESTION 1
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.



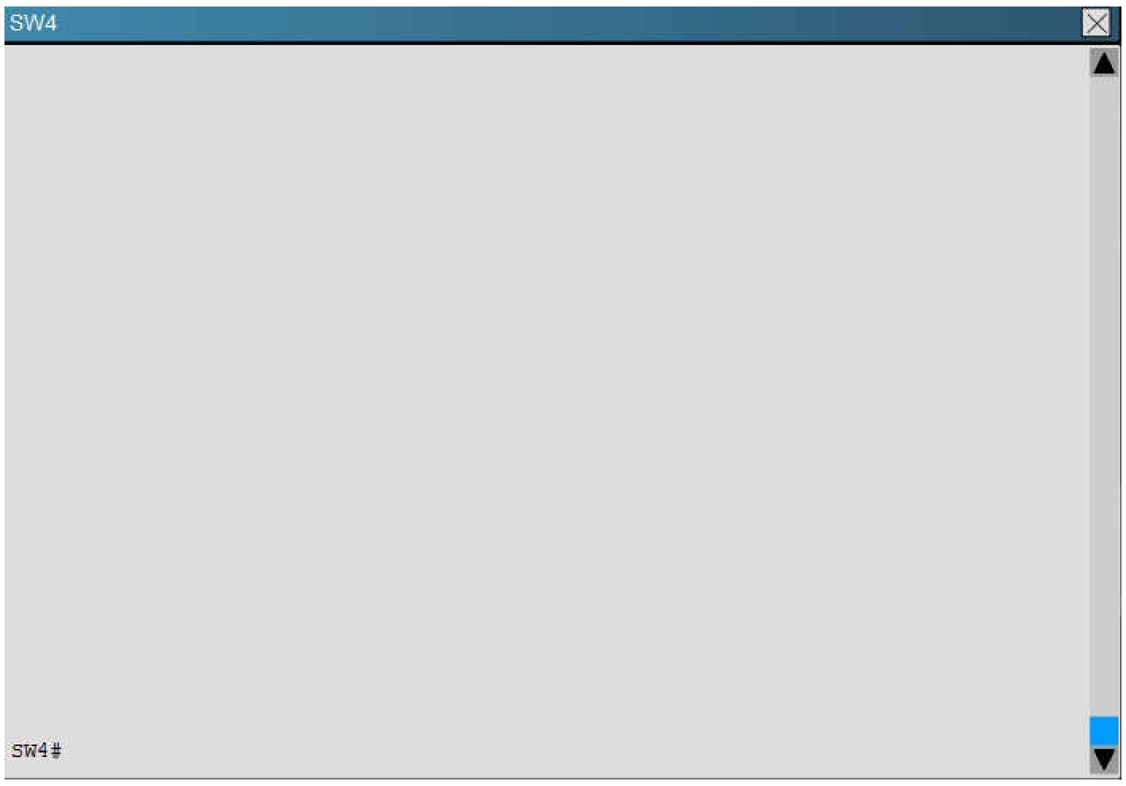
```
SW1#
```



```
SW2#
```



```
New_Switch#
```



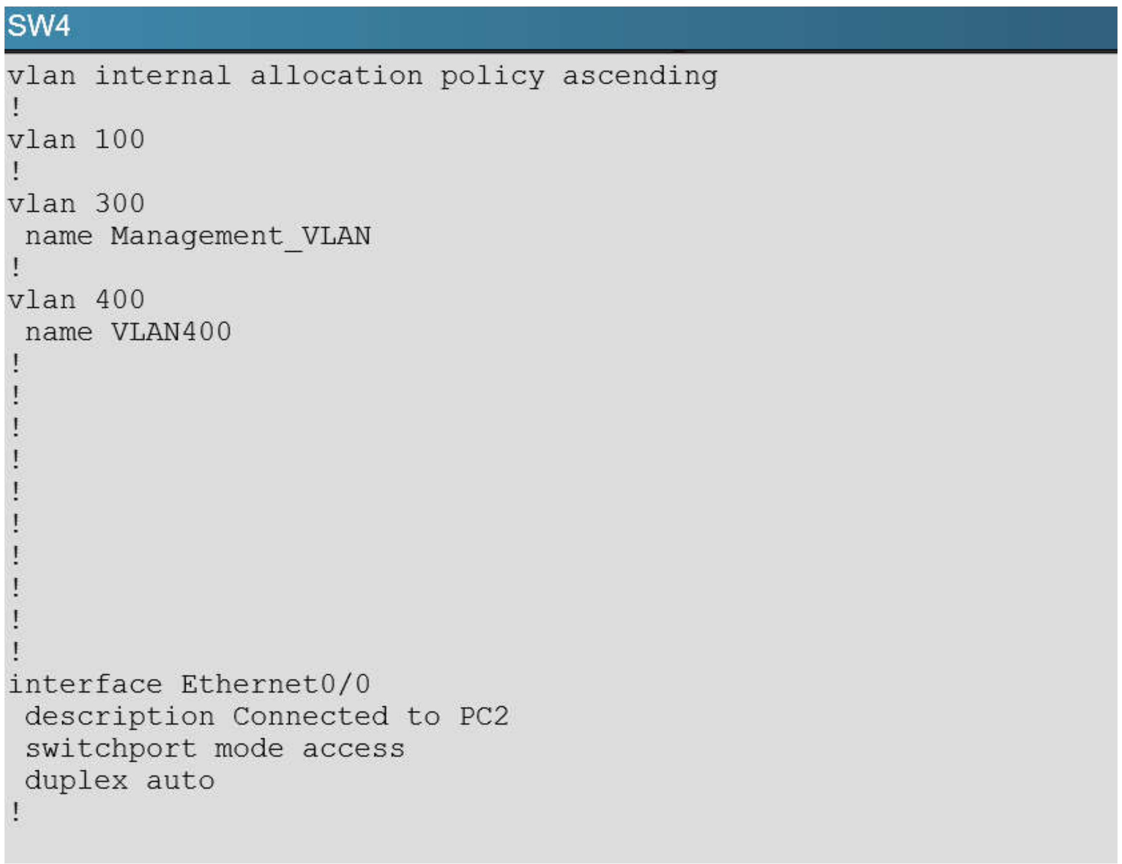
```
SW4#
```

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

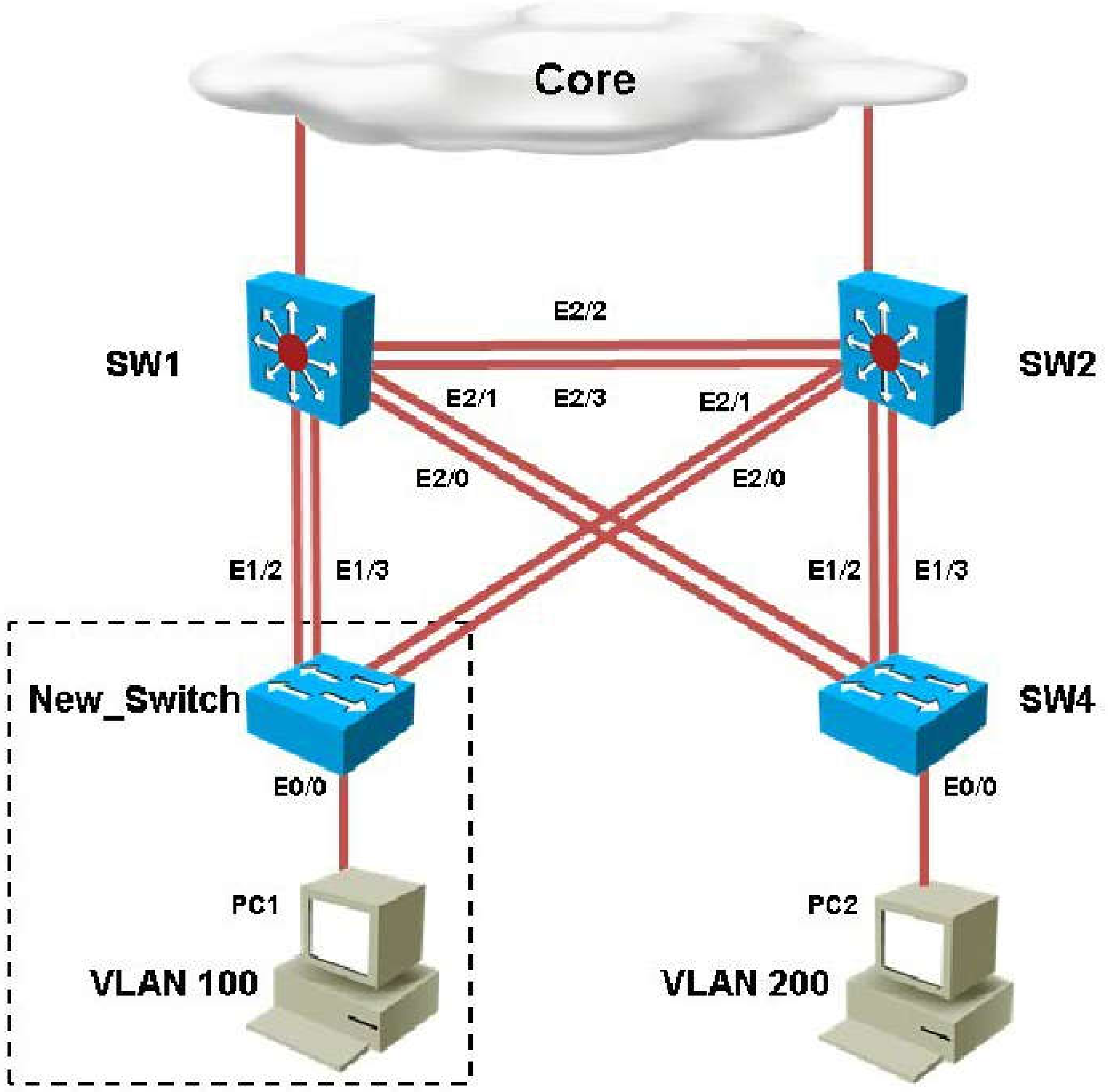
Explanation/Reference:
Explanation:
By looking at the configuration for SW2, we see that it is missing VLAN 200, and the “switchport access vlan 200” command is missing under interface eth 0/0:



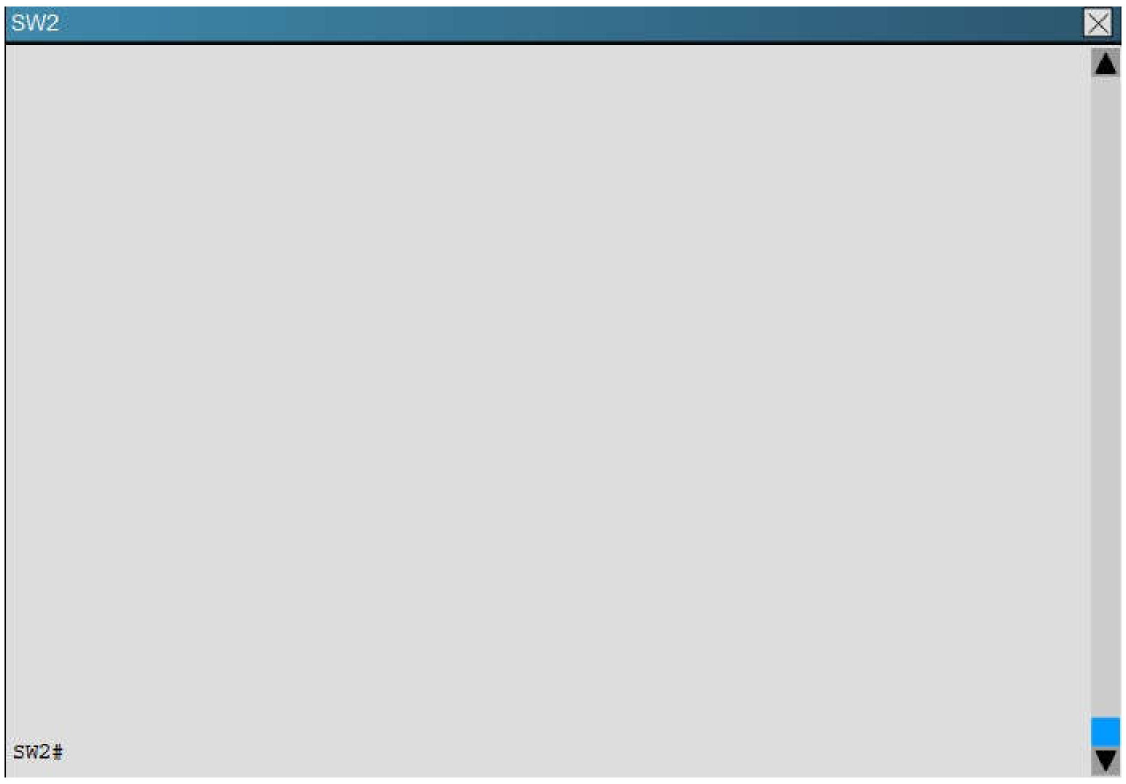
SW4

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

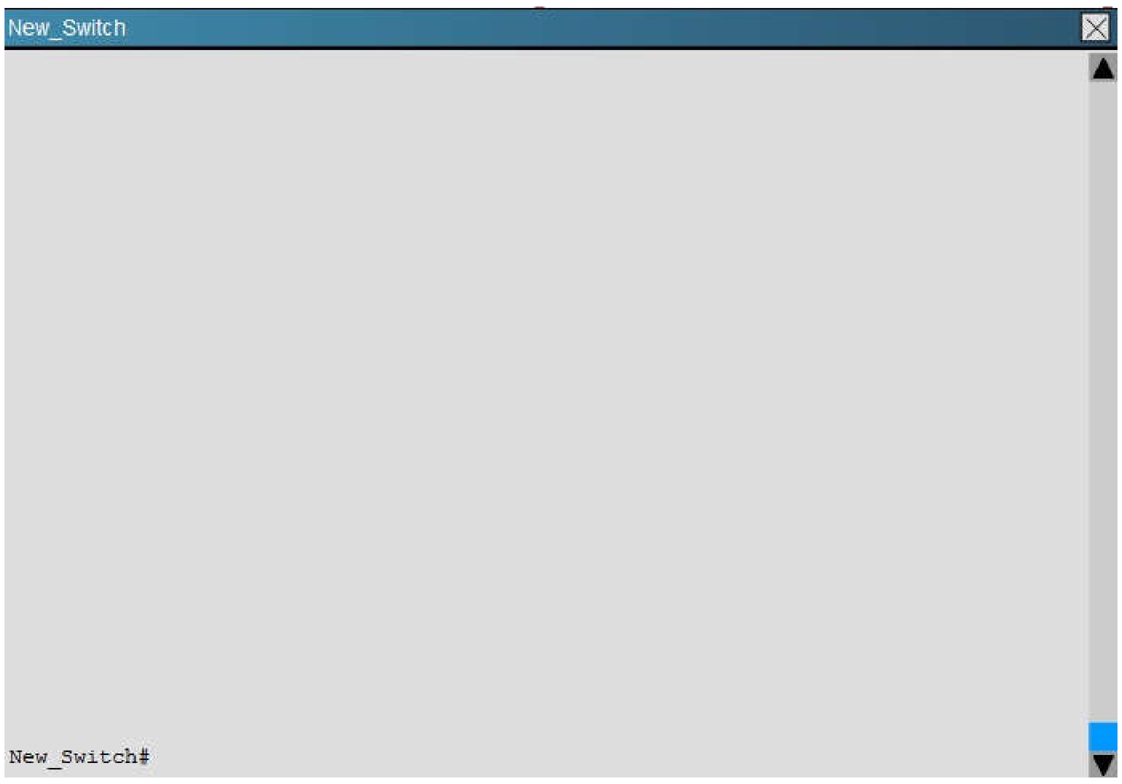
QUESTION 2
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.



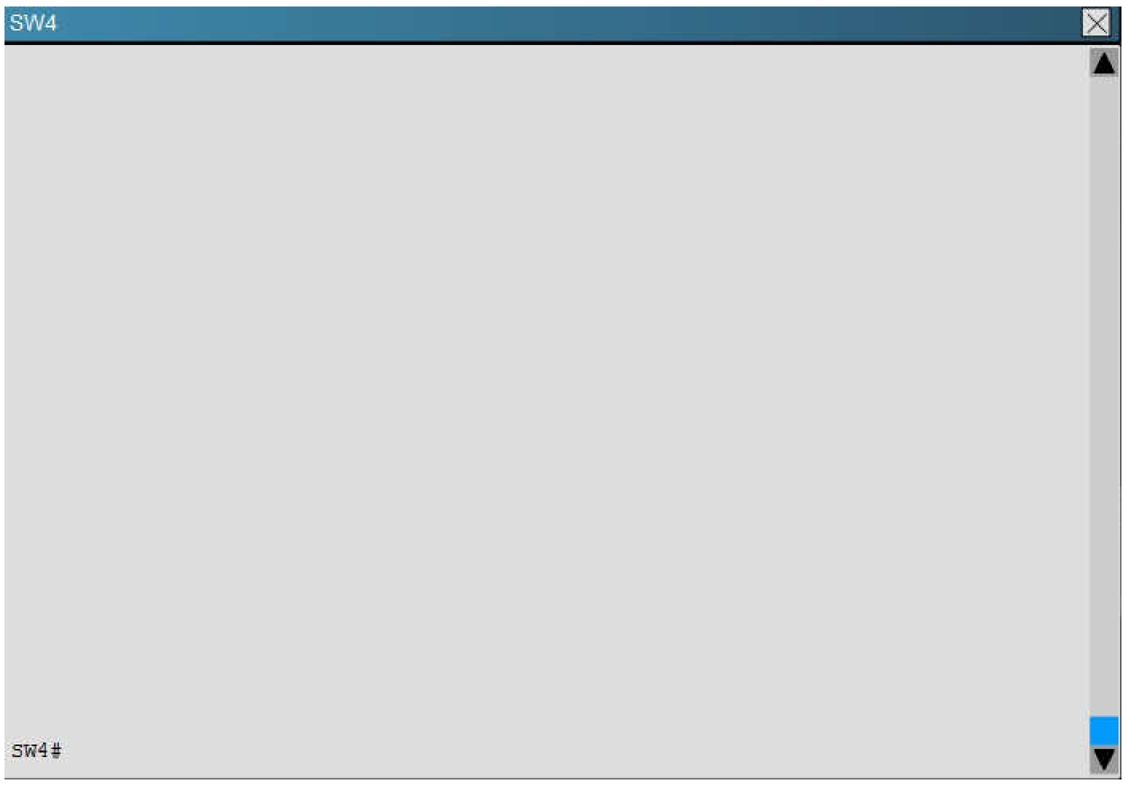
```
SW1#
```



```
SW2#
```



```
New_Switch#
```



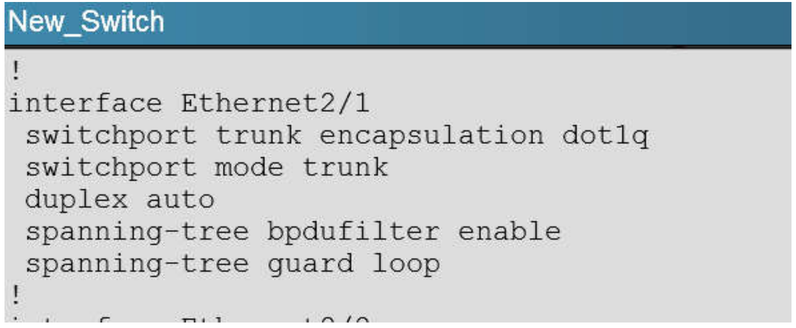
```
SW4#
```

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

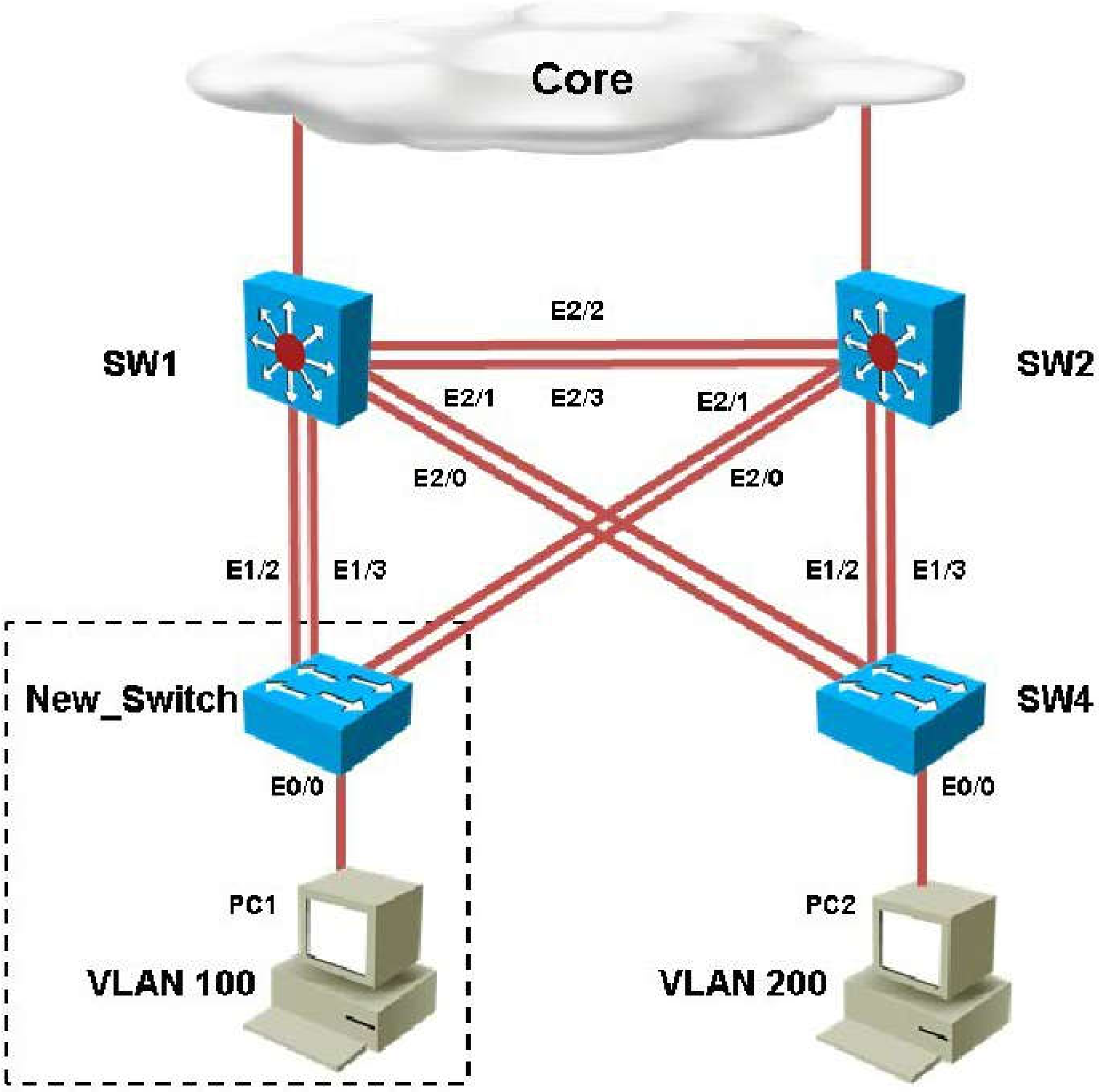
Explanation/Reference:
Explanation:
On the new switch, we see that loopguard has been configured with the "spanning-tree guard loop" command.



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

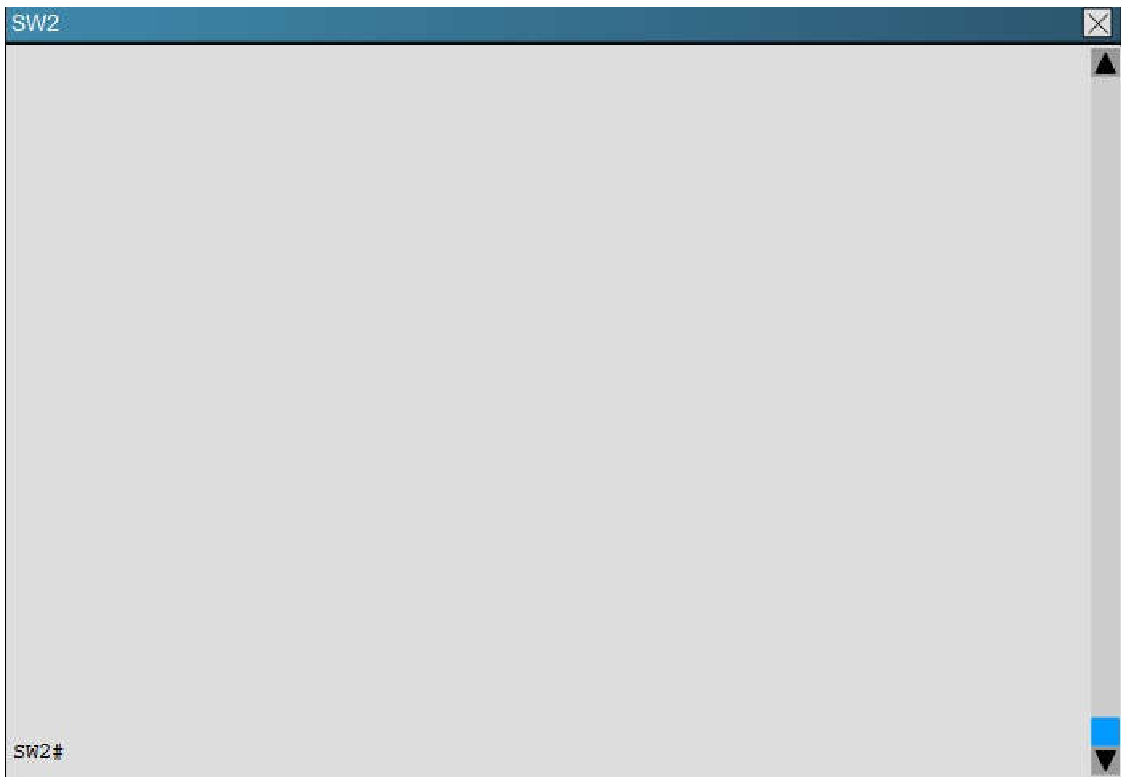
The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the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

QUESTION 3
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.

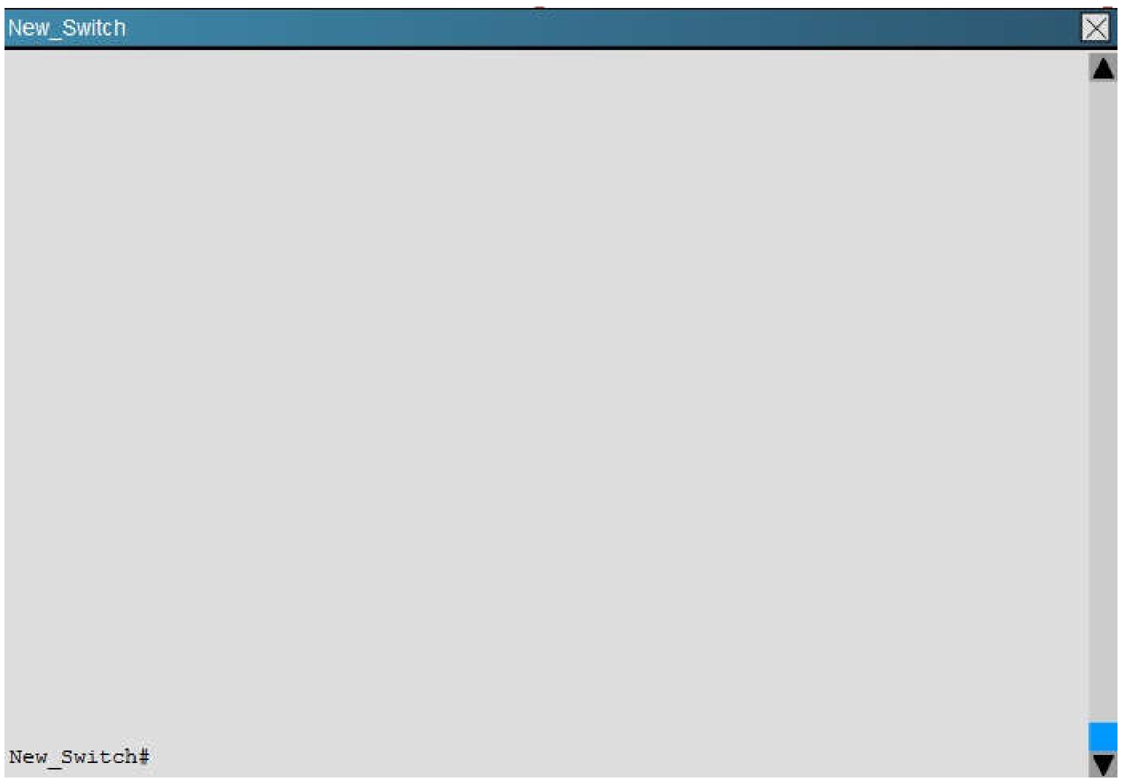

Core
SW1
E2/2
SW2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

SW1

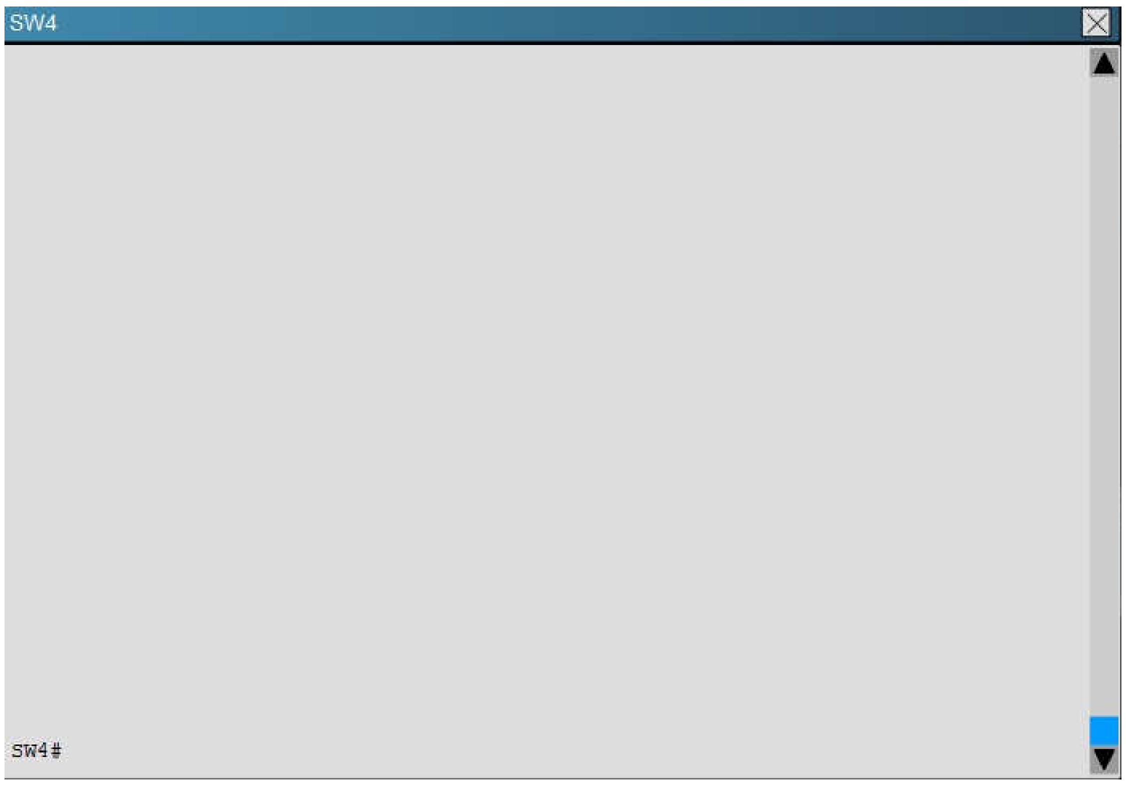
```
SW1#
```


SW2

```
SW2#
```



```
New_Switch#
```



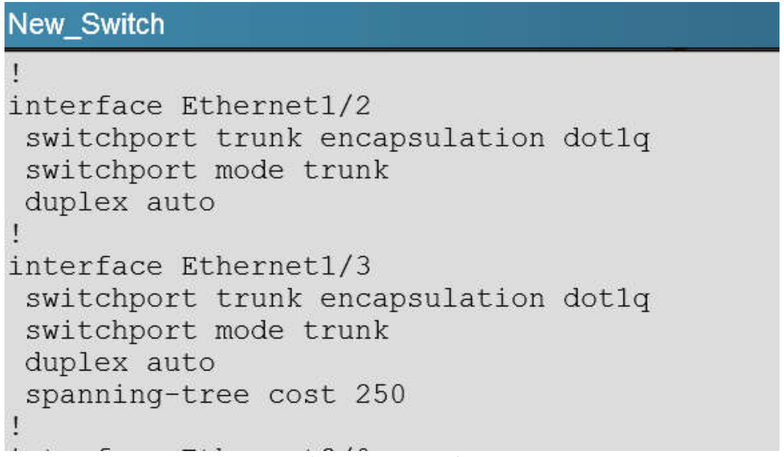
```
SW4#
```

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

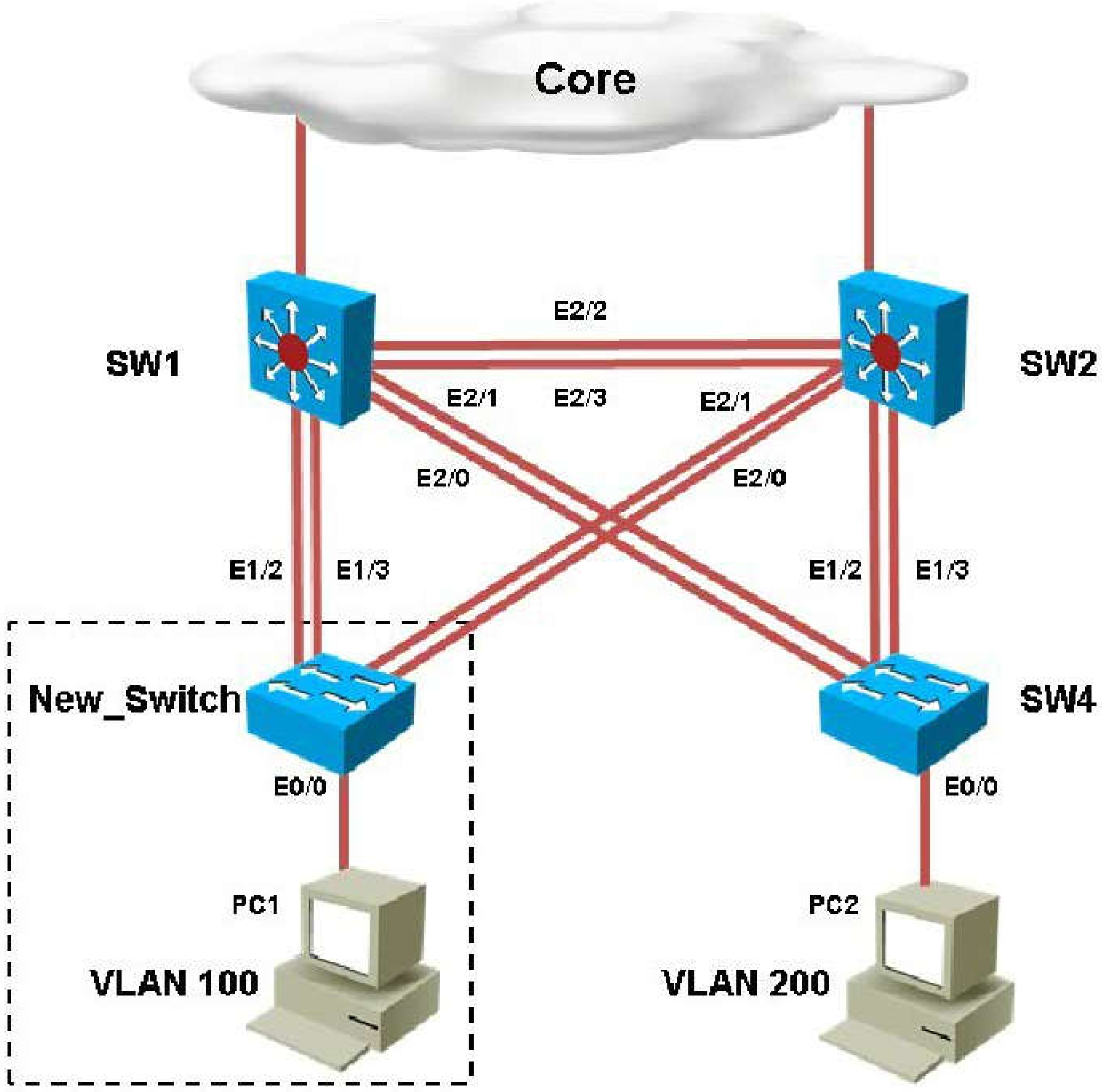
Explanation/Reference:
Explanation:
Here is the configuration found on the New_Switch:



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

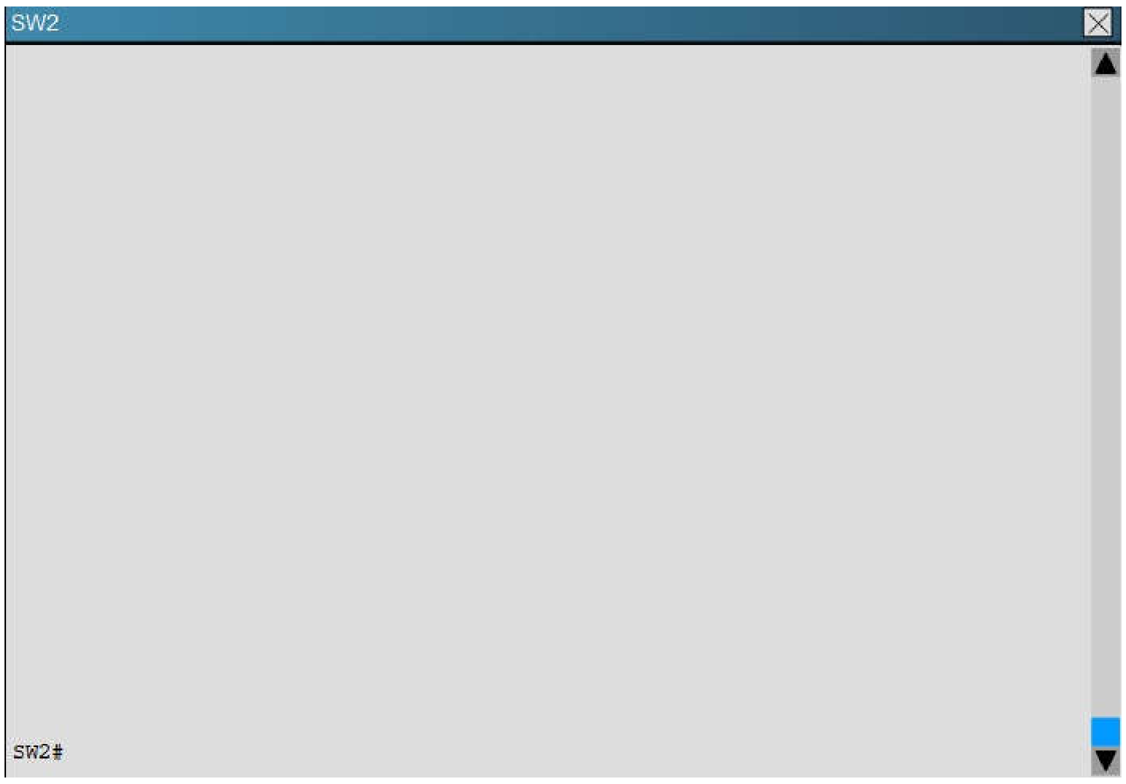
This causes the port cost for link eth 1/3 to increase the path cost to 250 for all VLANs, making that link less preferred so that only eth 1/2 will be used.

QUESTION 4
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.

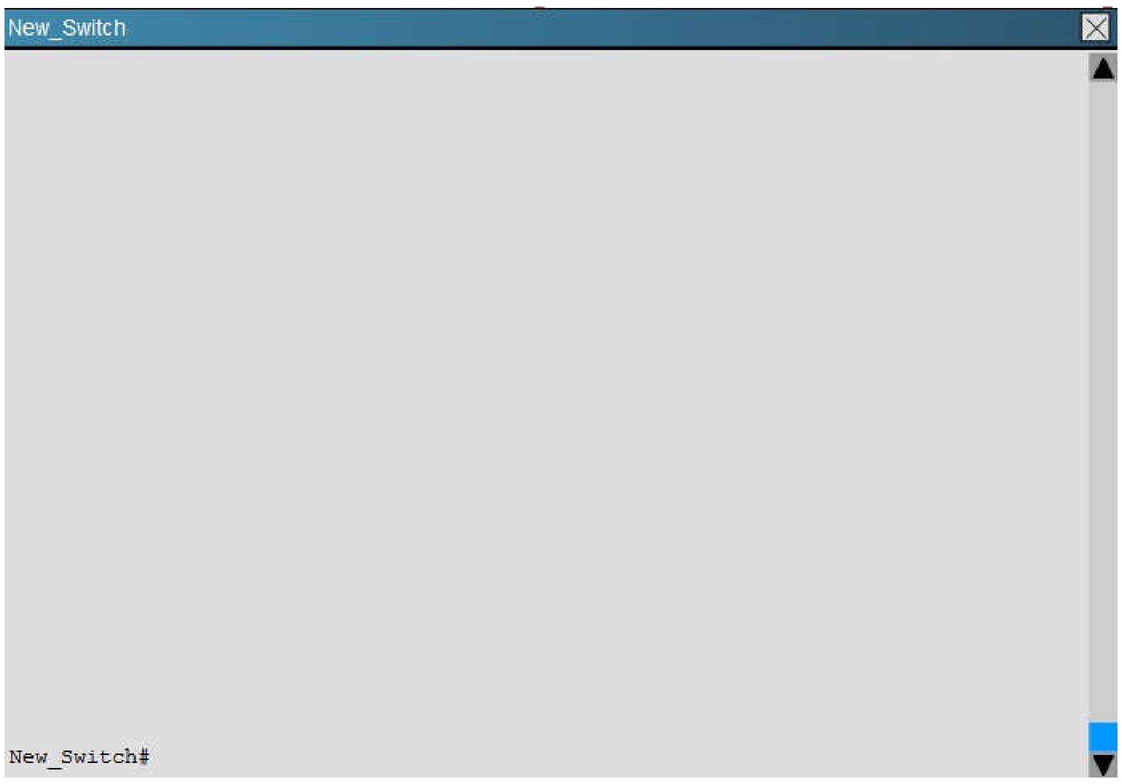

Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

SW1

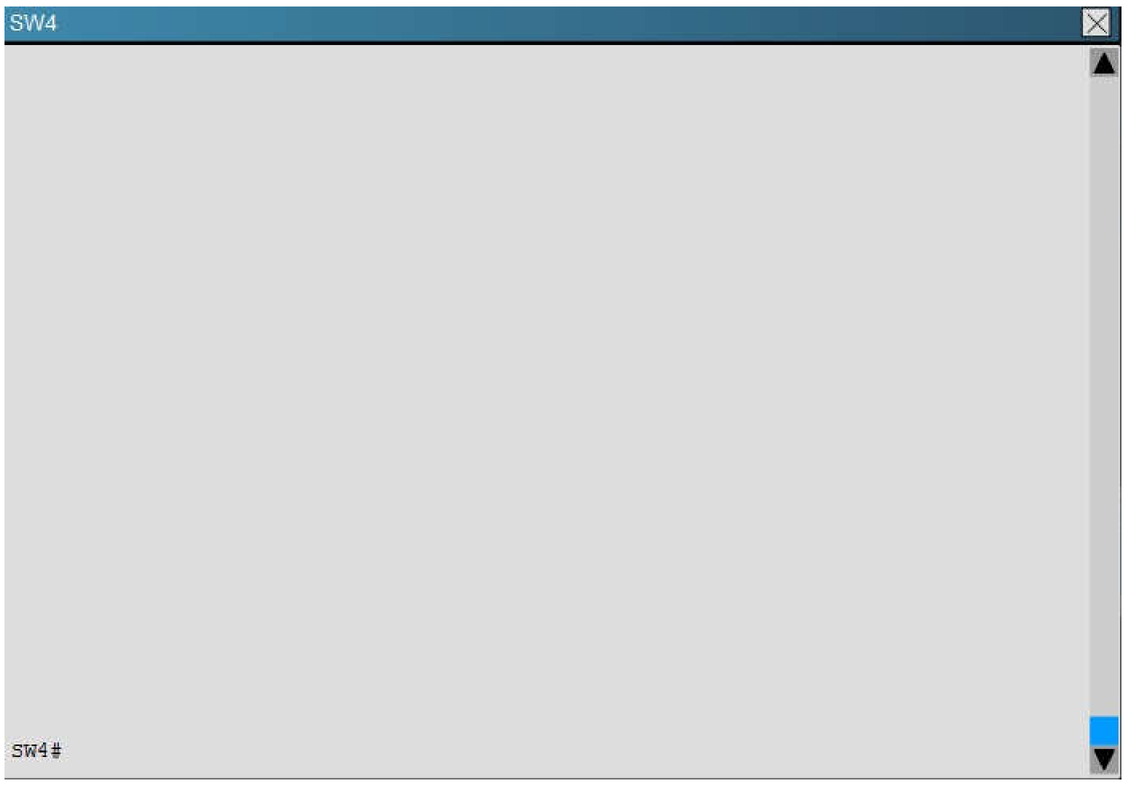
```
SW1#
```


SW2

```
SW2#
```



```
New_Switch#
```



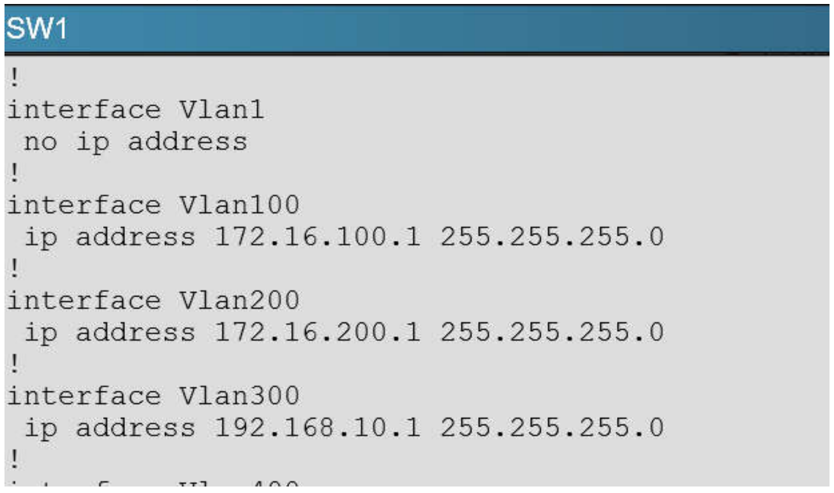
```
SW4#
```

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

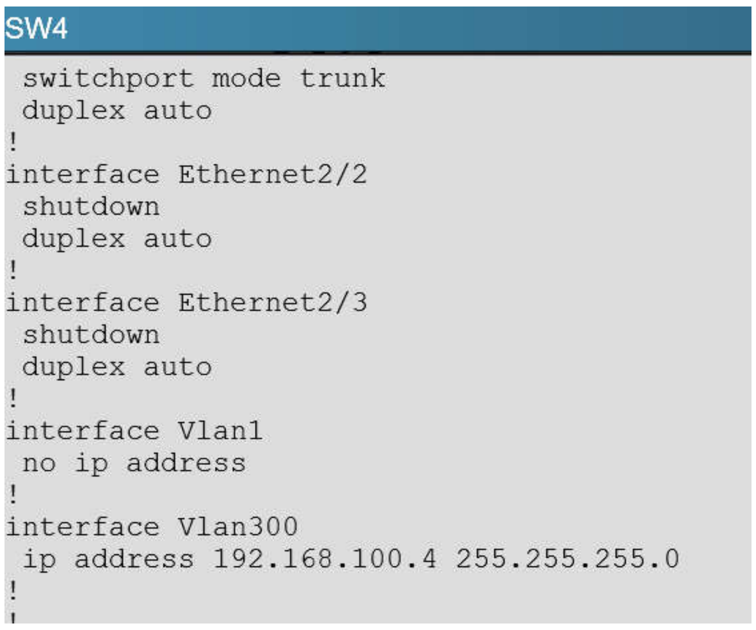
A. Management VLAN not allowed in the trunk links between SW1 and SW4
B. Management VLAN not allowed in the trunk links between SW1 and SW2
C. Management VLAN not allowed in the trunk link between SW2 and SW4
D. Management VLAN ip address on SW4 is configured in wrong subnet
E. Management VLAN interface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

Correct Answer: D
Section: [none]
Explanation

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



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

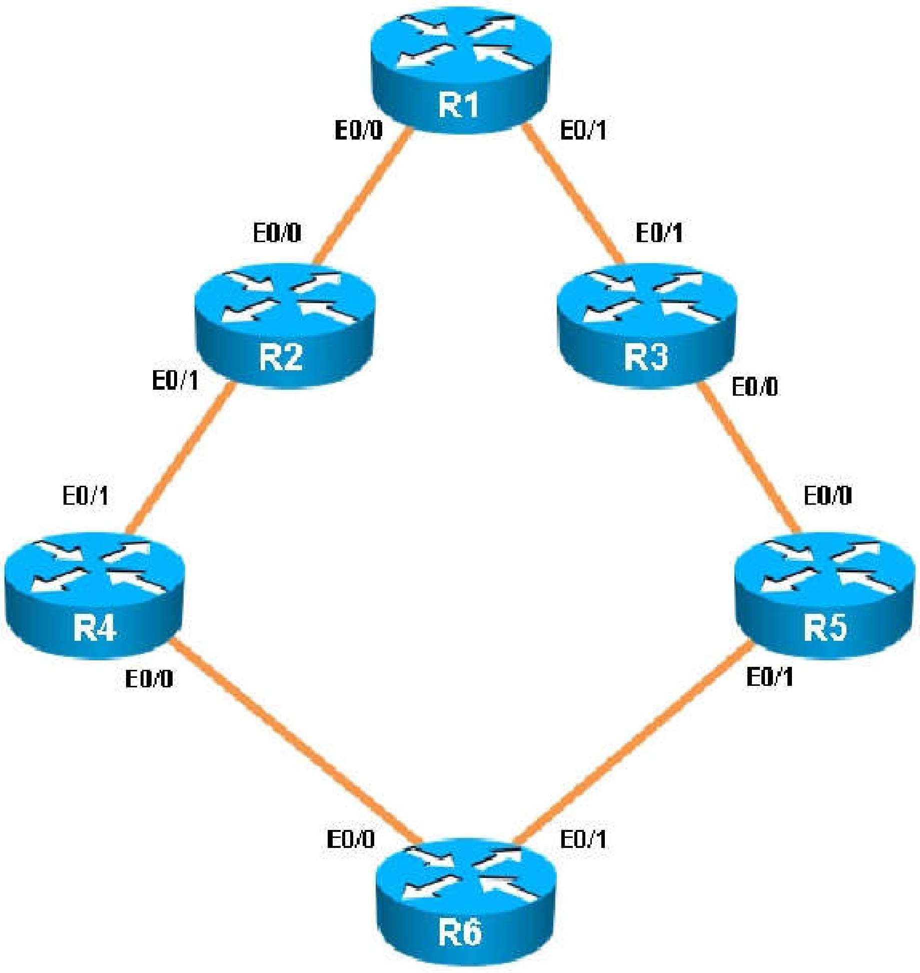


```
 switchport mode trunk
 duplex auto
!
interface Ethernet2/2
 shutdown
 duplex auto
!
interface Ethernet2/3
 shutdown
 duplex auto
!
interface Vlan1
 no ip address
!
interface Vlan300
 ip address 192.168.100.4 255.255.255.0
!
!
```

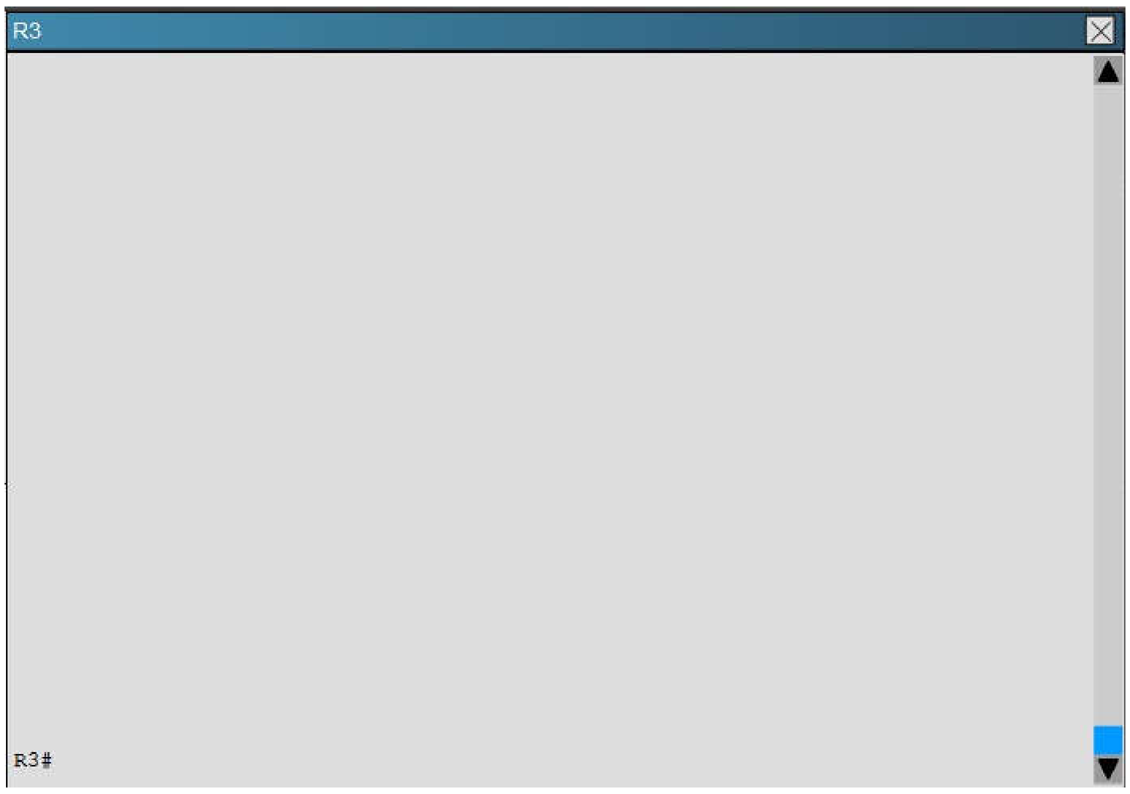
Question Set 1

QUESTION 1

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



```
R1#
```



```
R3#
```

```
R5#
```

```
R6#
```

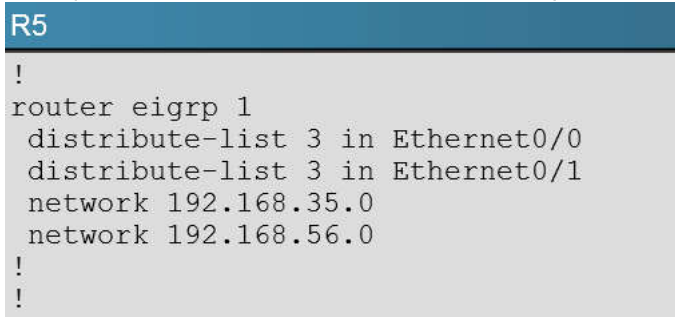
R5 has become partially isolated from the remainder of the network. R5 can reach devices on directly connected networks but nothing else. What is causing the problem?

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

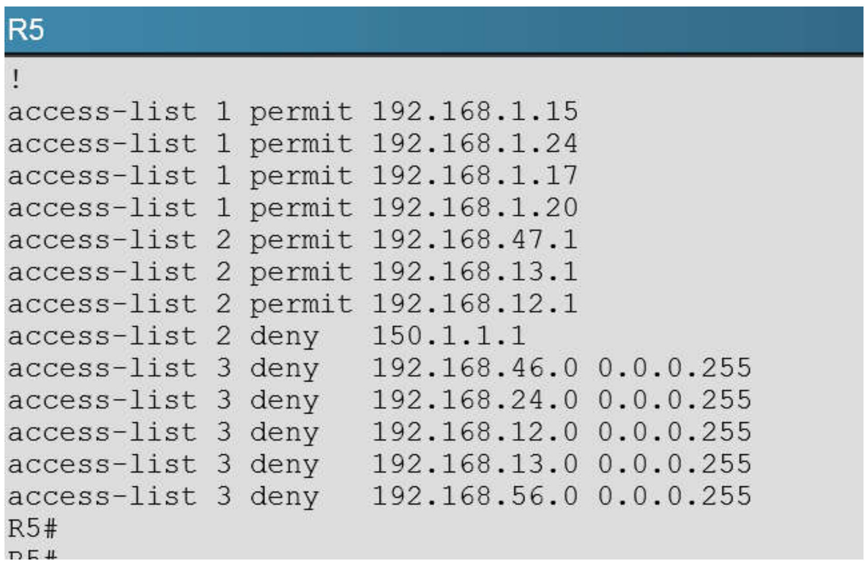
Section: [none]
Explanation

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



R5

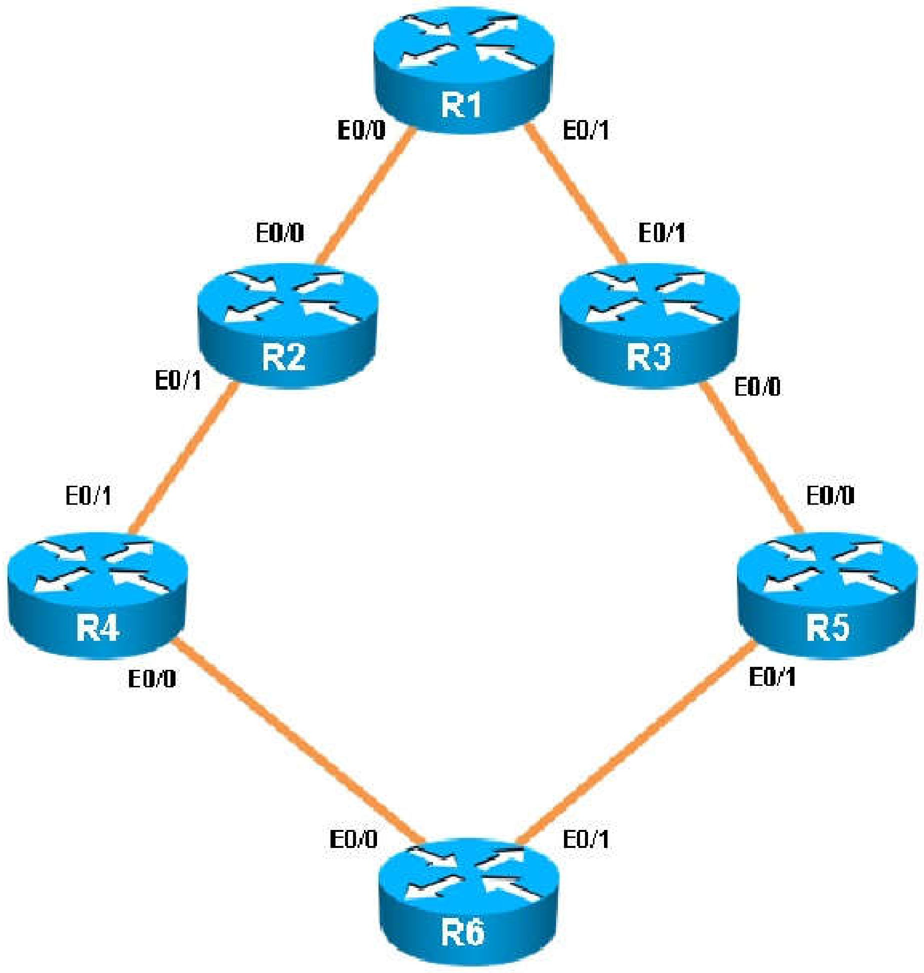
```
!
router eigrp 1
 distribute-list 3 in Ethernet0/0
 distribute-list 3 in Ethernet0/1
 network 192.168.35.0
 network 192.168.56.0
!
!
```



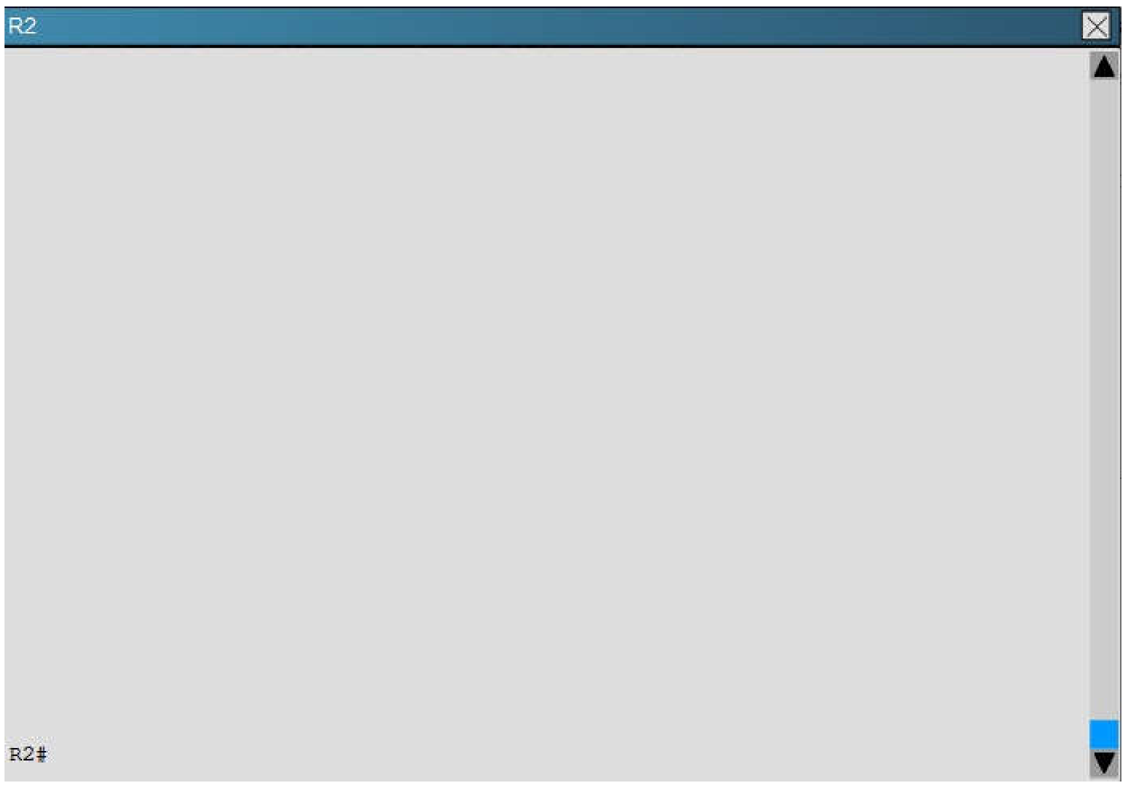
R5

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

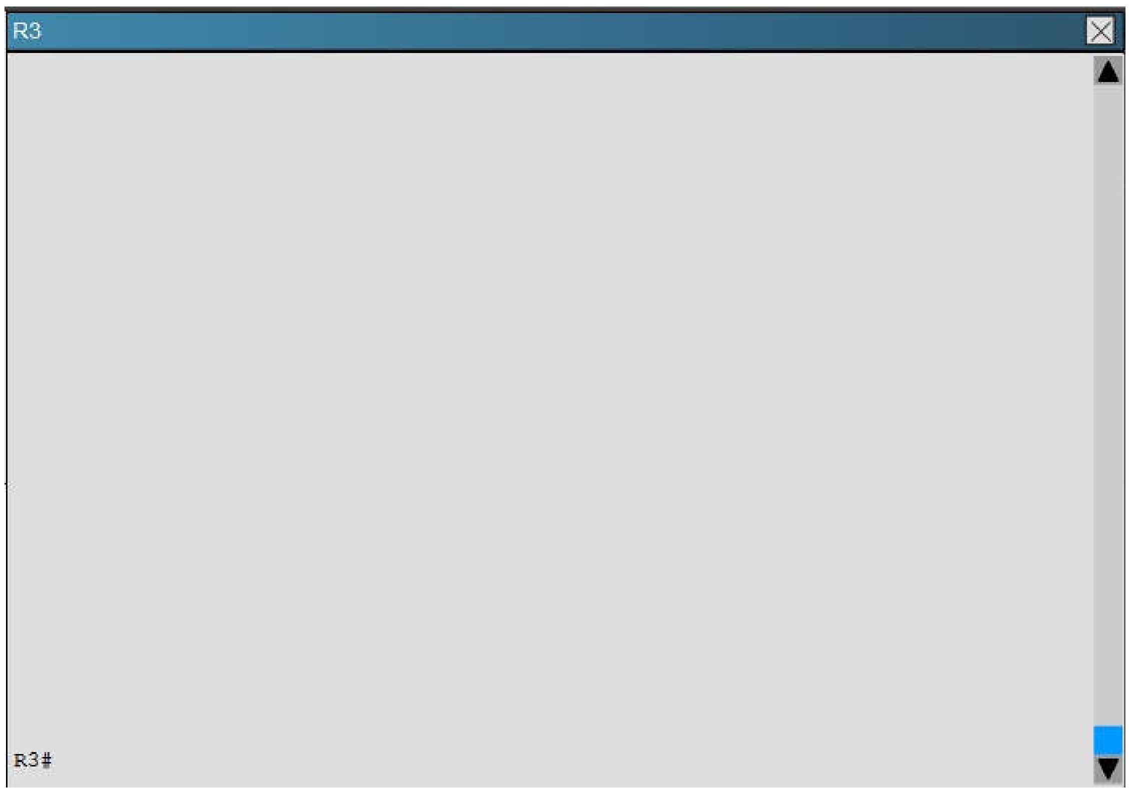
QUESTION 2
Scenario:
You have been brought in to troubleshoot an EIGRP network. You have resolved the initial issue between routers R2 and R4, but another issue remains. You are to locate the problem and suggest solution to resolve the issue.
The customer has disabled access to the show running-config command.



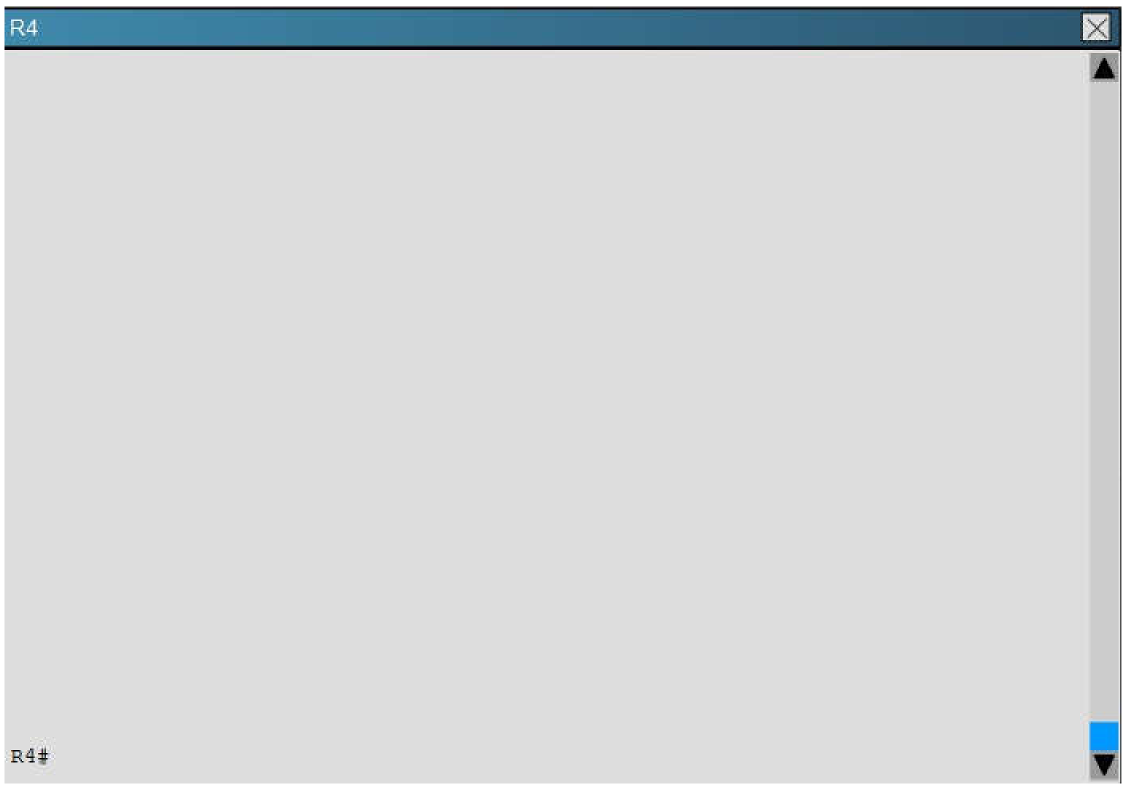
```
R1#
```



```
R2#
```



```
R3#
```



```
R4#
```

```
R5#
```

```
R6#
```

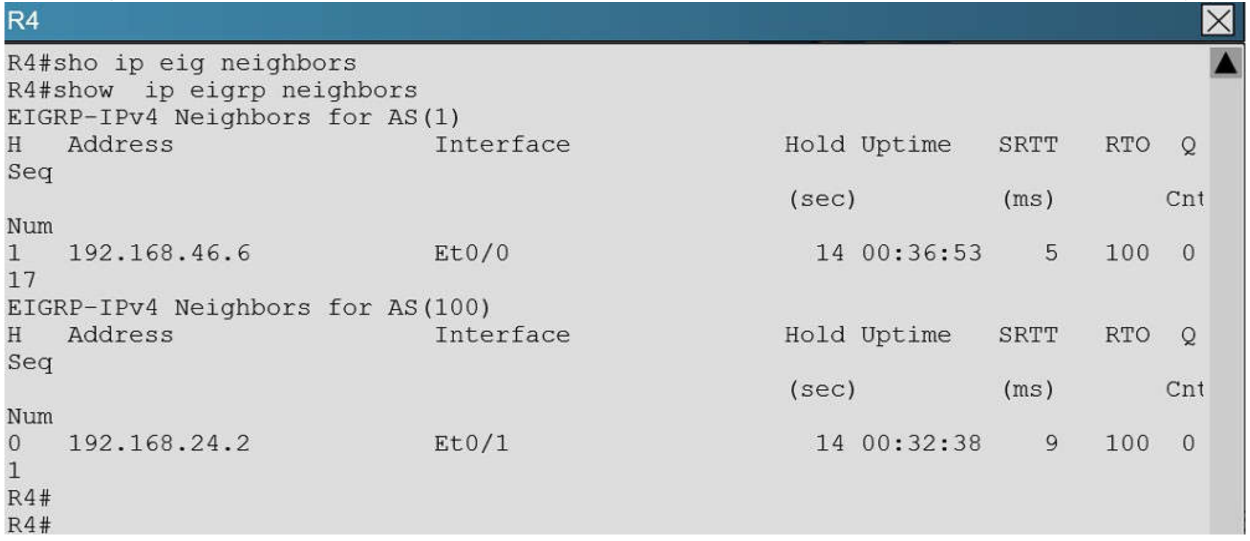
The network segment between R2 and R4 has become disconnected from the remainder of the network. How should this issue be resolved?

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.

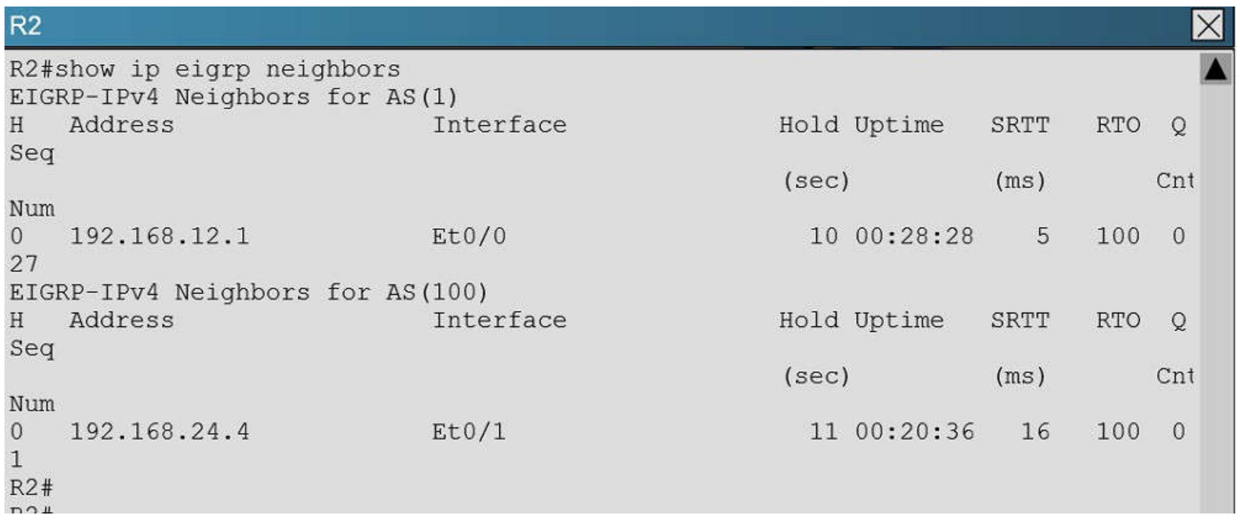
Correct Answer: B

Section: [none]
Explanation

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



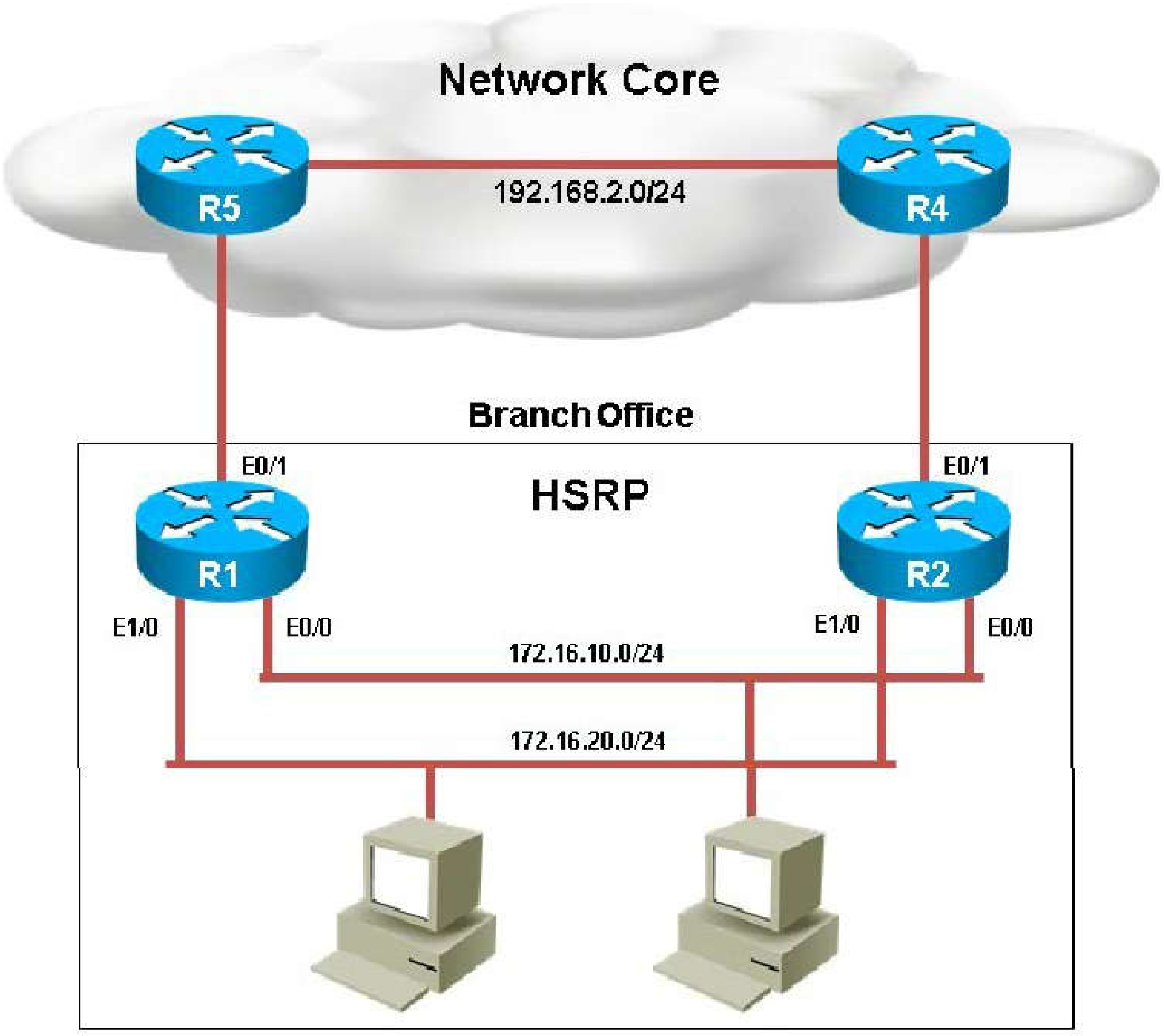
```
R4#sho ip eig neighbors
R4#show  ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
1   192.168.46.6            Et0/0             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



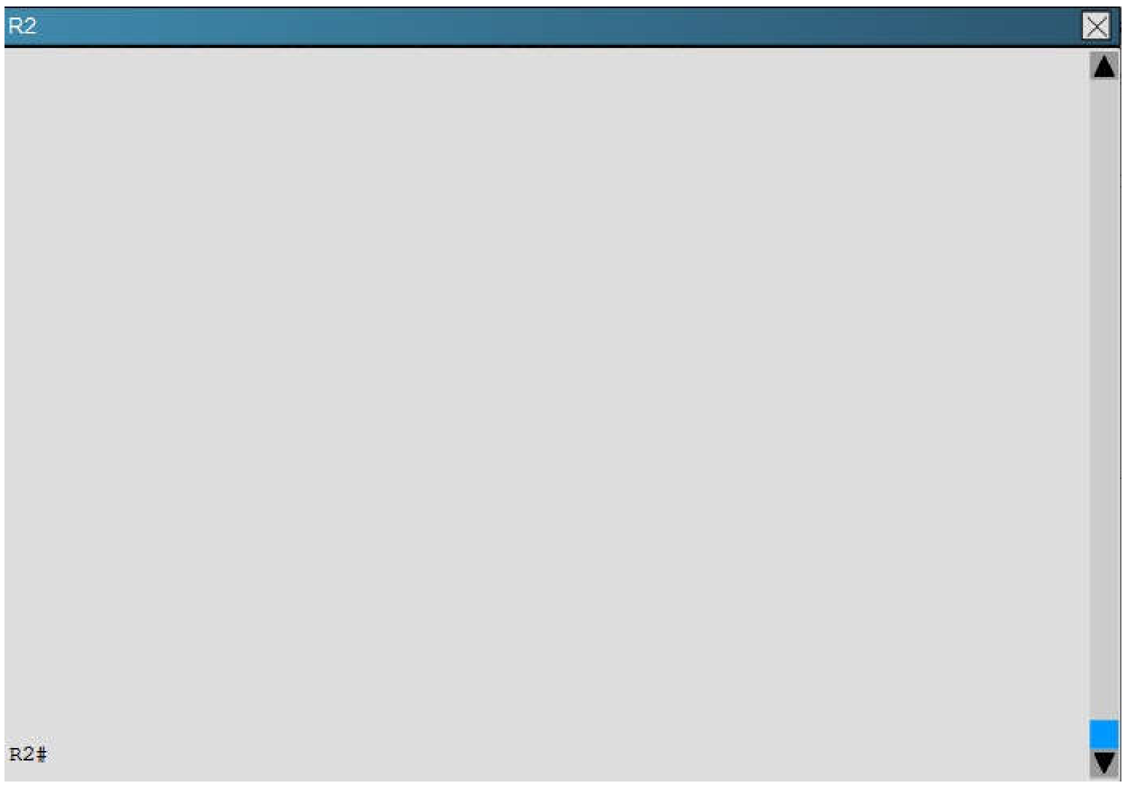
```
R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q
Seq
                                                   (sec)         (ms)       Cnt
Num
0   192.168.12.1            Et0/0                    10 00:28:28    5  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

Question Set 1

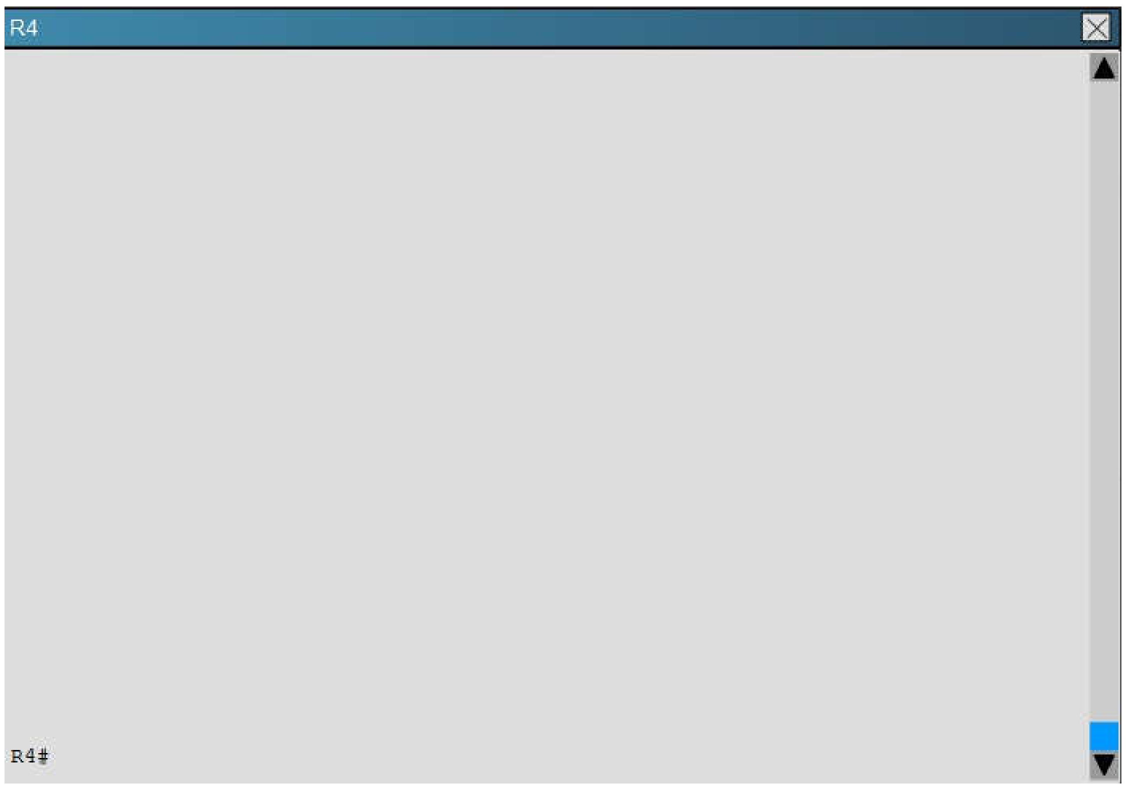
QUESTION 1
Scenario:
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.



```
R1#
```



```
R2#
```



```
R4#
```

```
R5#
```

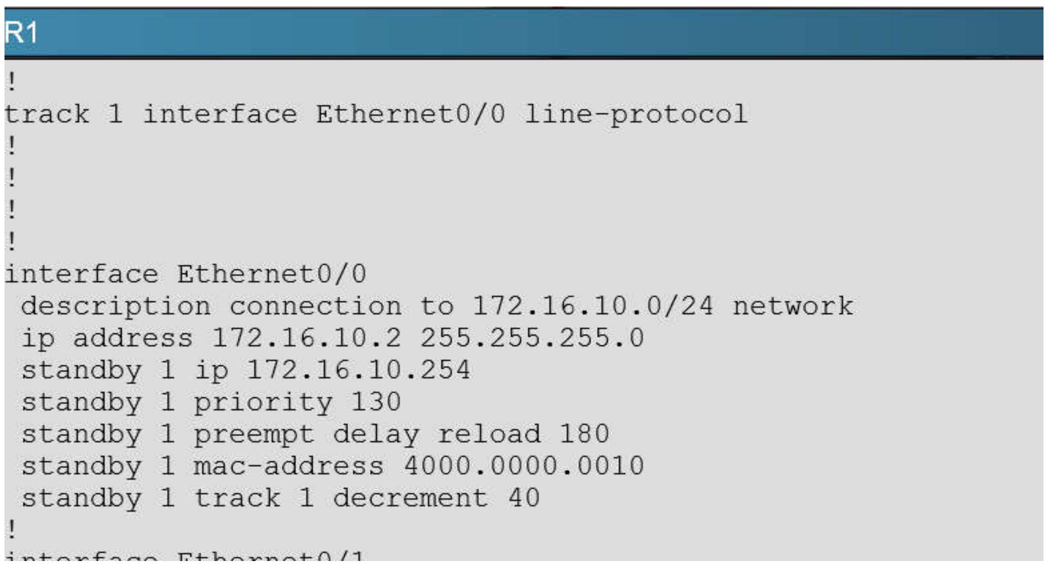
You have received notification from network monitoring system that link between R1 and R5 is down and you noticed that the active router for HSRP group 1 has not failed over to the standby router for group 1. You are required to troubleshoot and identify the issue.

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

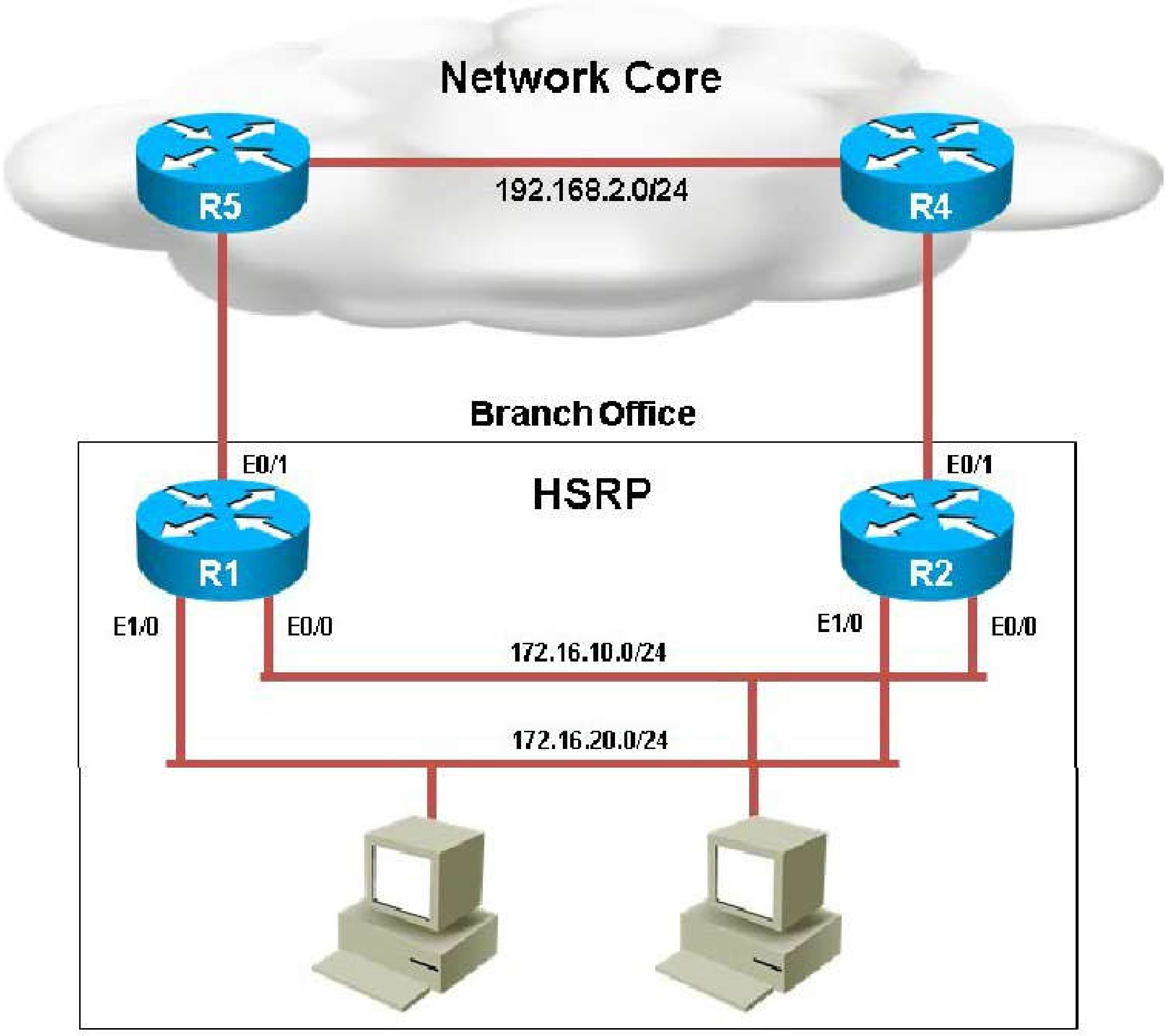


R1

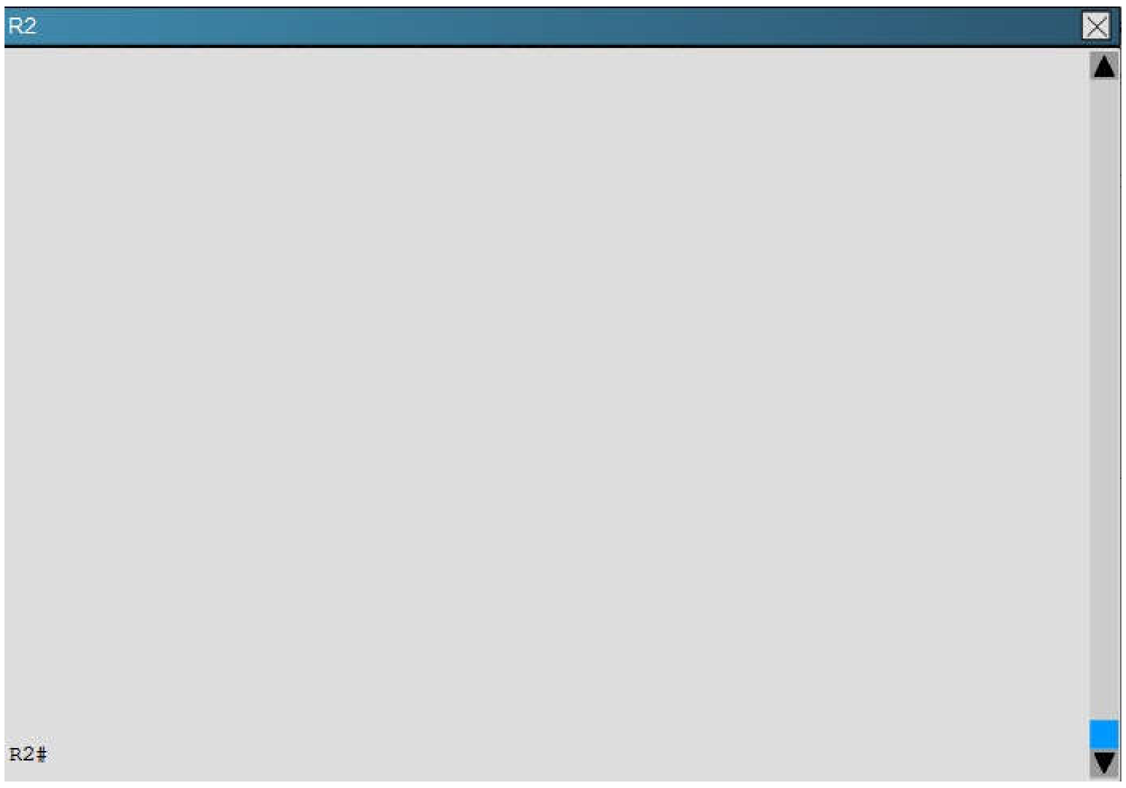
```
!
track 1 interface Ethernet0/0 line-protocol
!
!
!
!
interface Ethernet0/0
 description connection to 172.16.10.0/24 network
 ip address 172.16.10.2 255.255.255.0
 standby 1 ip 172.16.10.254
 standby 1 priority 130
 standby 1 preempt delay reload 180
 standby 1 mac-address 4000.0000.0010
 standby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

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

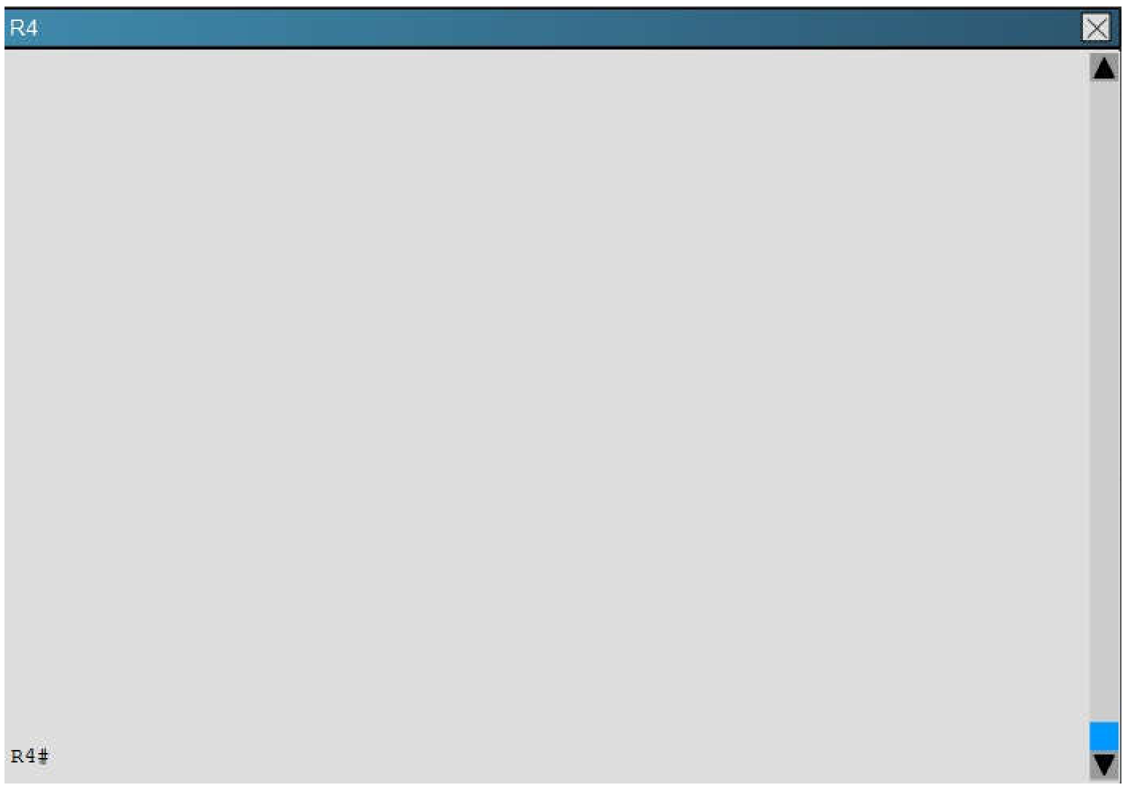
QUESTION 2
Scenario:
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.



```
R1#
```



```
R2#
```



```
R4#
```

```
R5#
```

The following debug messages are noticed for HSRP group 2. But still neither R1 nor R2 has identified one of them as standby router. Identify the reason causing the issue.

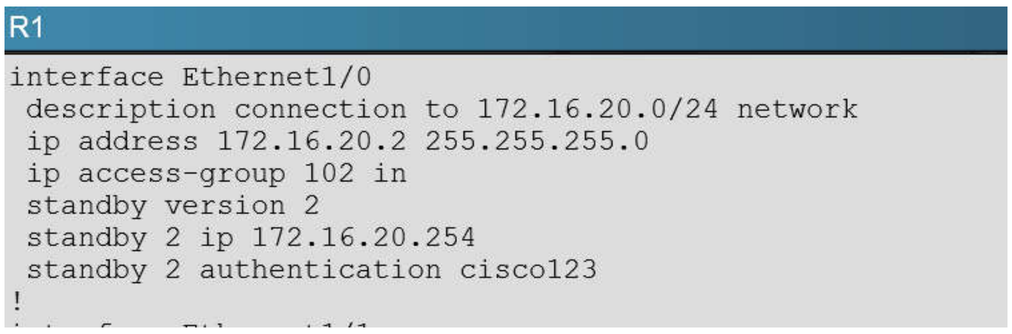
Note: only show commands can be used to troubleshoot the ticket.

```
R1#
'Mar 26 11:17:39.234: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:40.034: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
R1#
'Mar 26 11:17:40.364: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
R1#
'Mar 26 11:17:41.969: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:42.719: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
'Mar 26 11:17:42.918: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
R1#
'Mar 26 11:17:44.869: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:45.485: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
'Mar 26 11:17:45.718: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
R1#
'Mar 26 11:17:47.439: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:48.252: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
'Mar 26 11:17:48.322: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
R1#
'Mar 26 11:17:50.389: HSRP: Et1/0 Grp 2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:50.735: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
'Mar 26 11:17:50.921: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active prj 130 vIP
172.16.10.254
R1#
'Mar 26 11:17:53.089: HSRP: Et1/0 Grp2 Hello out 172.16.20.2 Active pri 100 vIP
172.16.20.254
'Mar 26 11:17:53.338: HSRP: EtO/0 Grp 1 Hello out 172.16.10.2 Active pri130vIP
172.16.10.254
'Mar 26 11:17:53.633: HSRP: EtO/0 Grp 1 Hello in 172.16.10.1 Standby pri 100 vIP
172.16.10.254
```

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

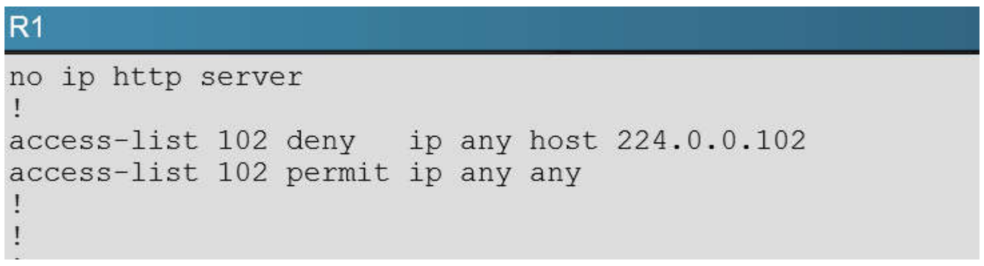
Correct Answer: E
Section: [none]
Explanation

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



R1

```
interface Ethernet1/0
 description connection to 172.16.20.0/24 network
 ip address 172.16.20.2 255.255.255.0
 ip access-group 102 in
 standby version 2
 standby 2 ip 172.16.20.254
 standby 2 authentication cisco123
!
interface Ethernet1/1
```



R1

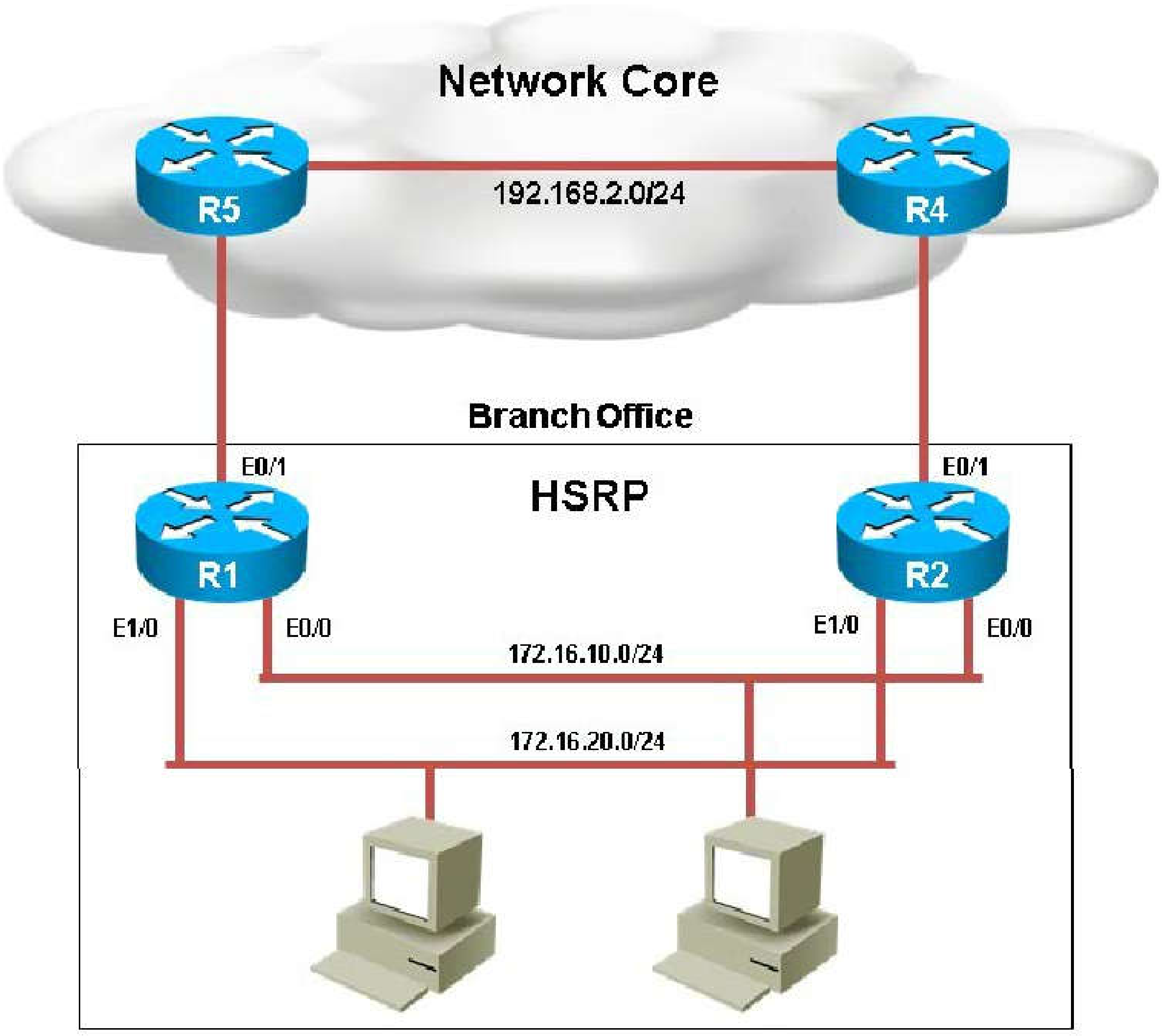
```
no ip http server
!
access-list 102 deny   ip any host 224.0.0.102
access-list 102 permit ip any any
!
!
```

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

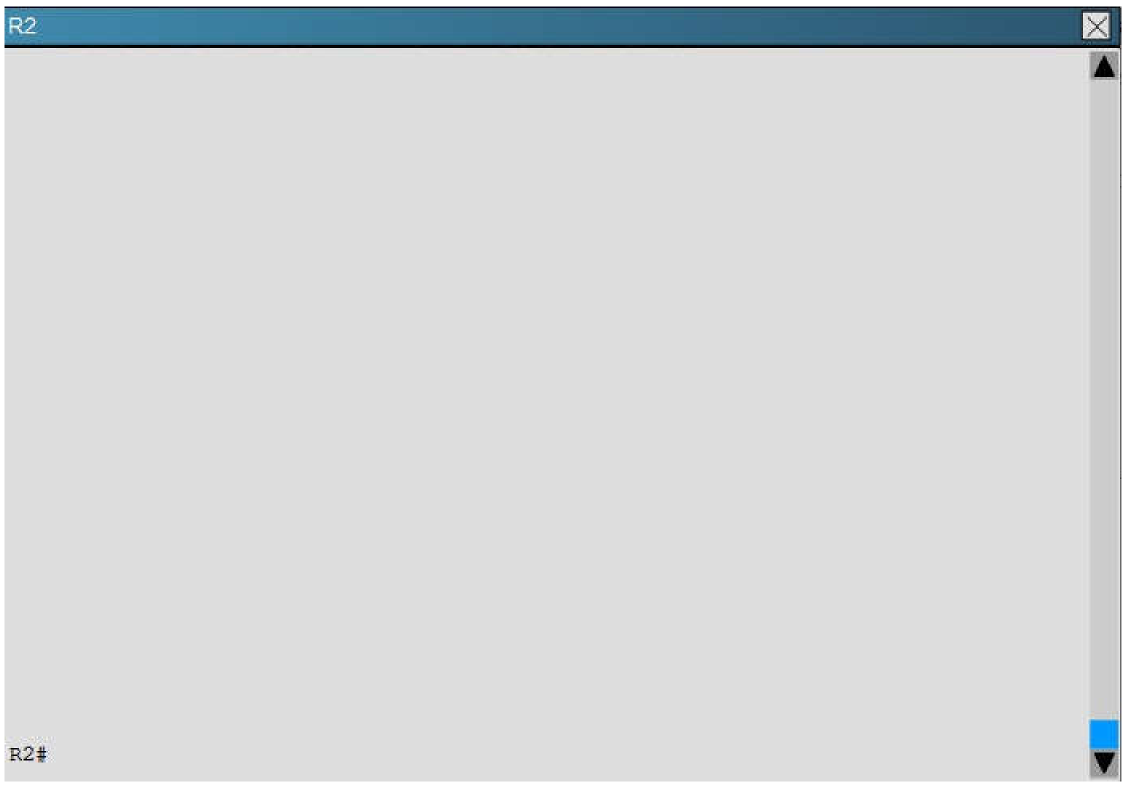
QUESTION 3

Scenario:

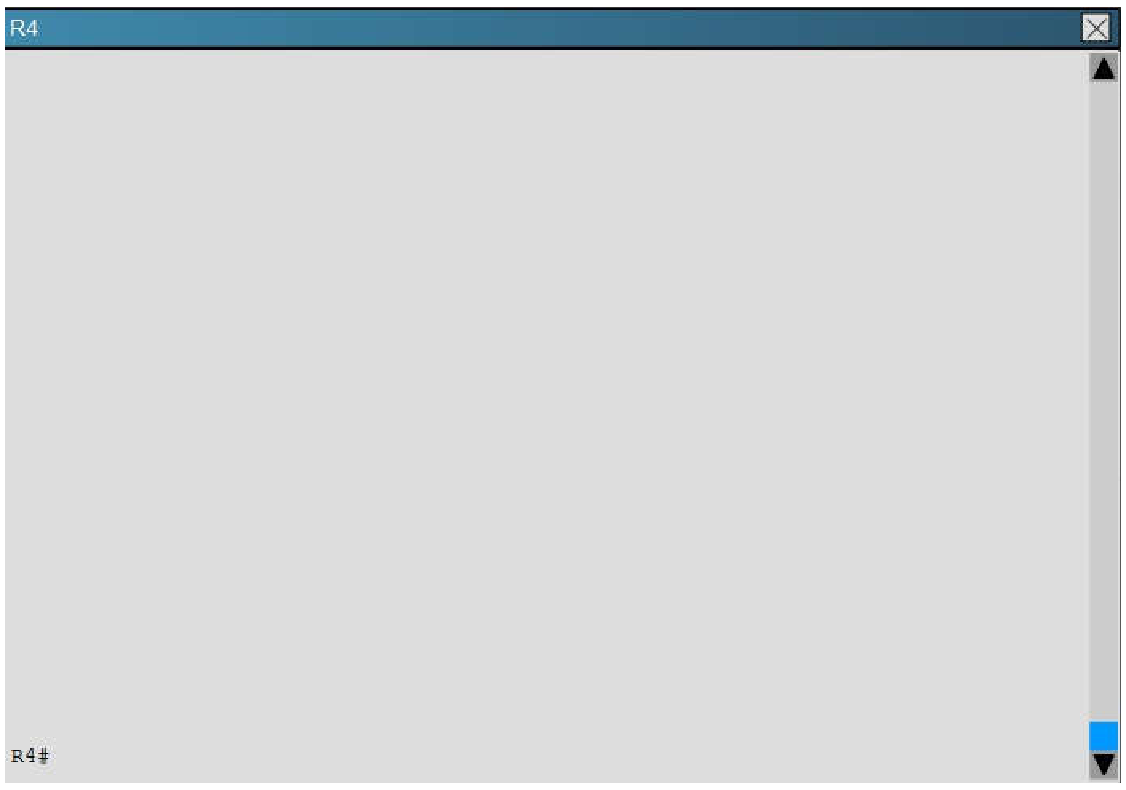
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.



```
R1#
```



```
R2#
```



```
R4#
```

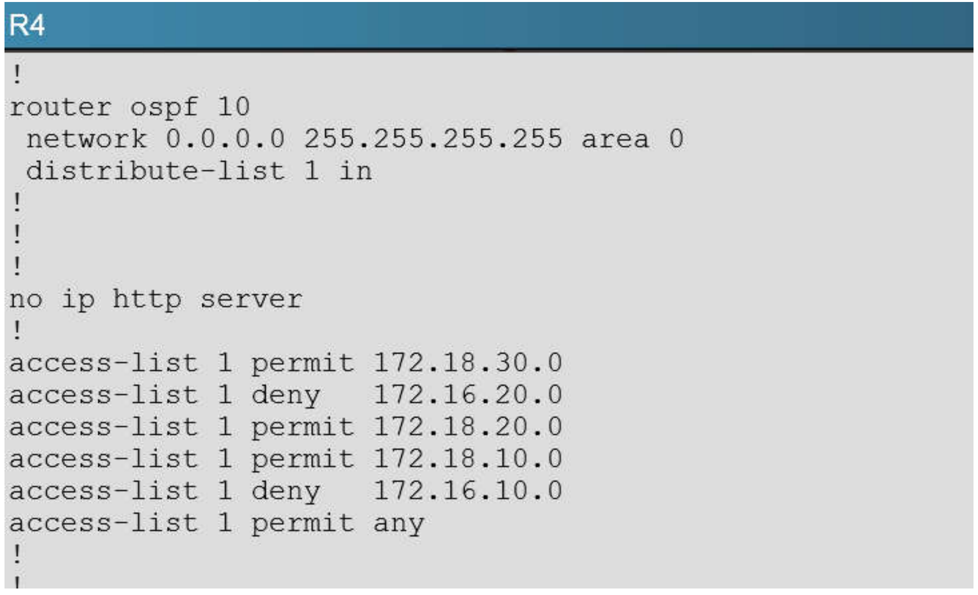
```
R5#
```

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

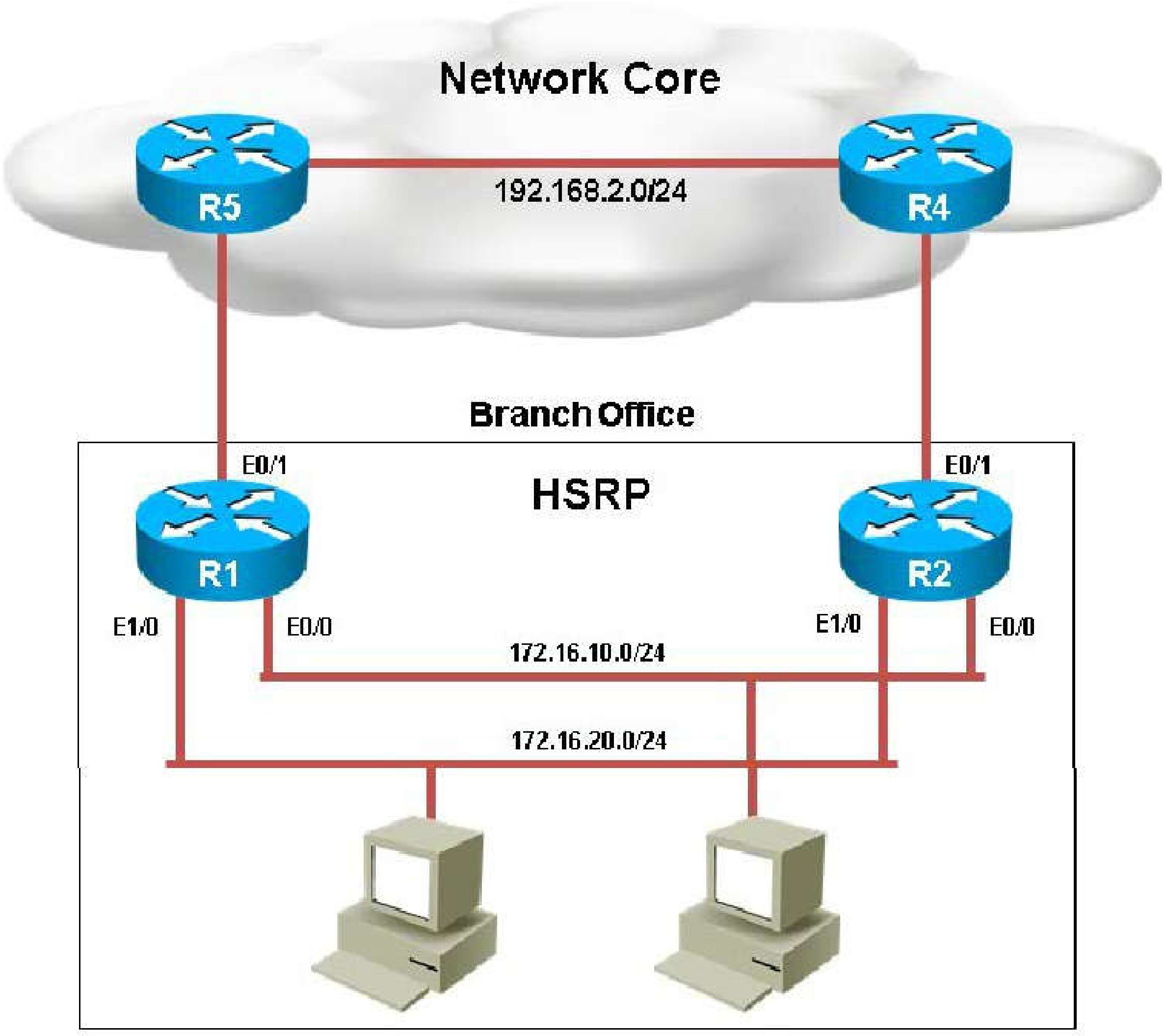
Correct Answer: D
Section: [none]
Explanation

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



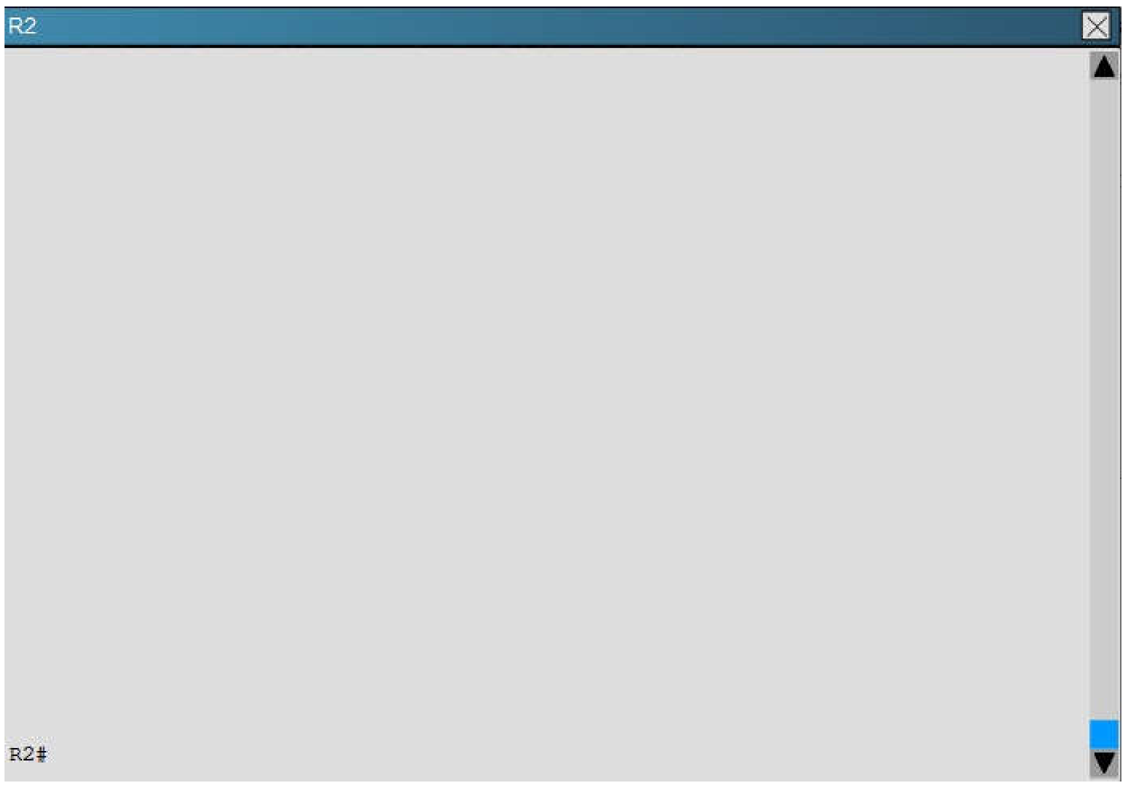
```
!
router ospf 10
 network 0.0.0.0 255.255.255.255 area 0
 distribute-list 1 in
!
!
!
no ip http server
!
access-list 1 permit 172.18.30.0
access-list 1 deny   172.16.20.0
access-list 1 permit 172.18.20.0
access-list 1 permit 172.18.10.0
access-list 1 deny   172.16.10.0
access-list 1 permit any
!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

QUESTION 4
Scenario:
You have been asked by your customer to help resolve issues in their routed network. Their network engineer has deployed HSRP. On closer inspection HSRP doesn't appear to be operating properly and it appears there are other network problems as well. You are to provide solutions to all the network problems.

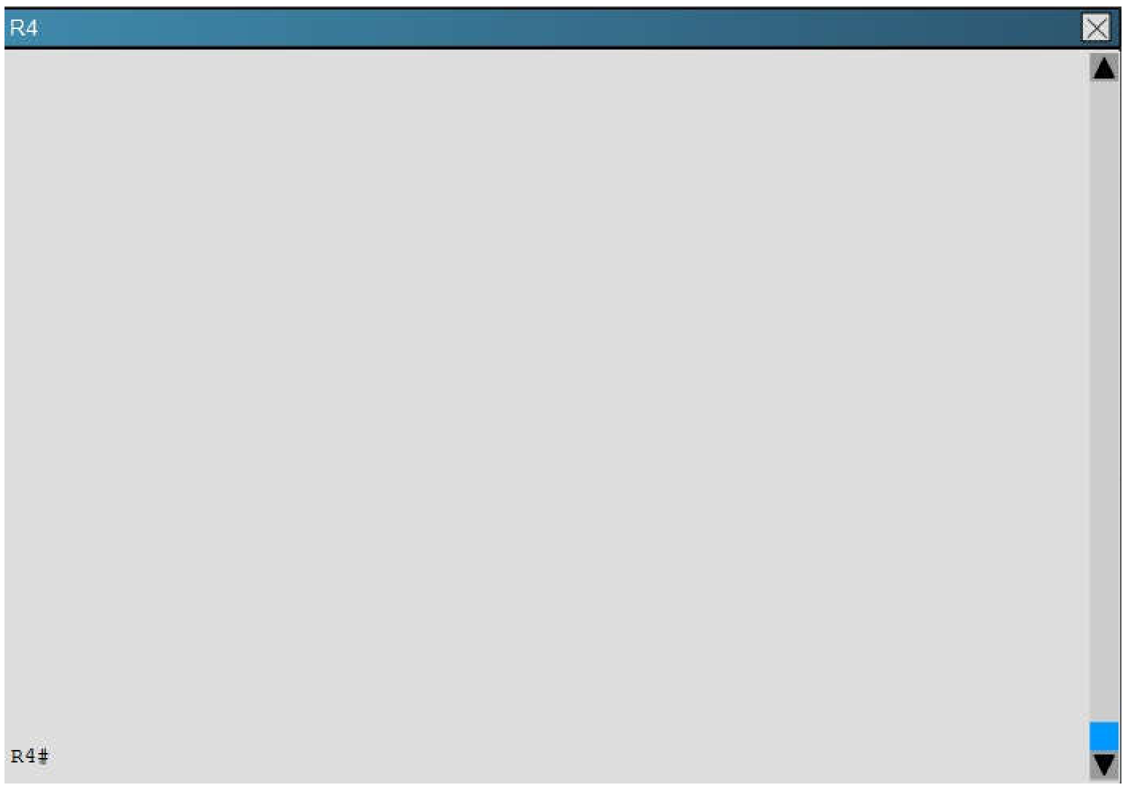

Network Core
R5
192.168.2.0/24
R4
Branch Office
E0/1
HSRP
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24

R1

```
R1#
```



```
R2#
```



```
R4#
```

```
R5#
```

You examine the configuration on R5 and discover that no routes are being learned from R4. Which issue prevents the route entries from being installed in the routing table?

A. HSRP issue between R5 and R4

B. There is an OSPF issue between R5and R4

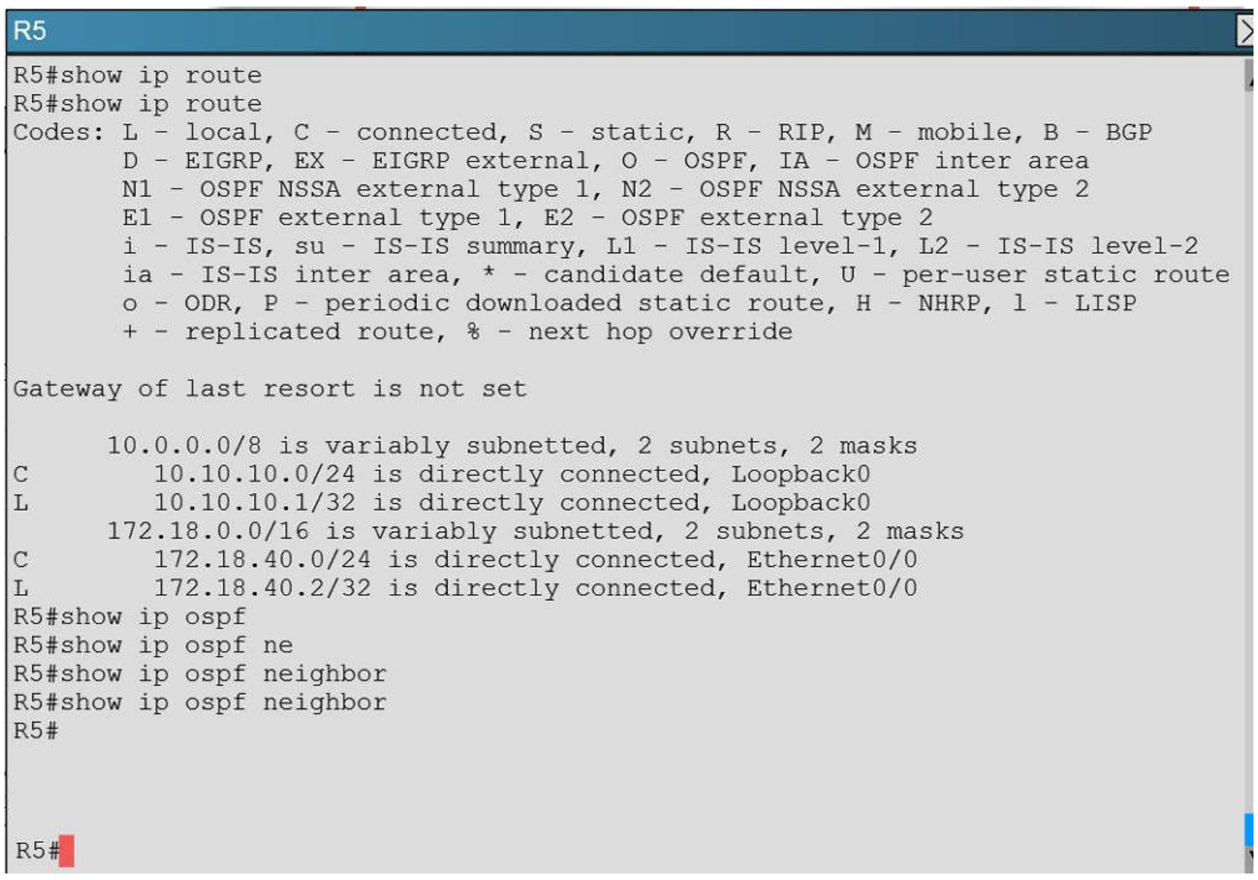
C. There is a DHCP issue between R5 and R4

D. The distribute-list configured on R5 is blocking route entries

E. The ACL configured on R5 is blocking traffic for the subnets advertised from R4.

Correct Answer: B
Section: [none]
Explanation

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

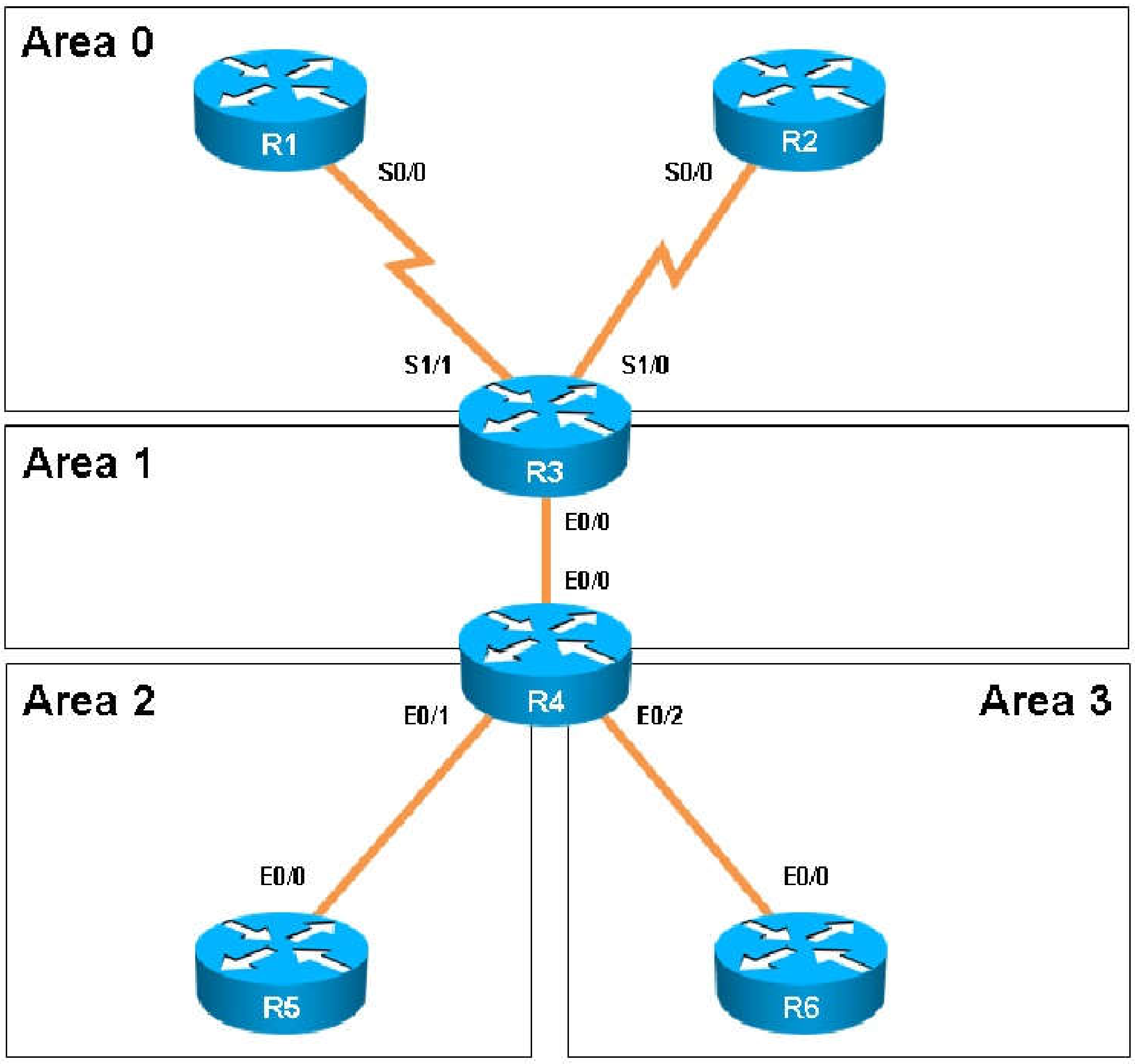


R5

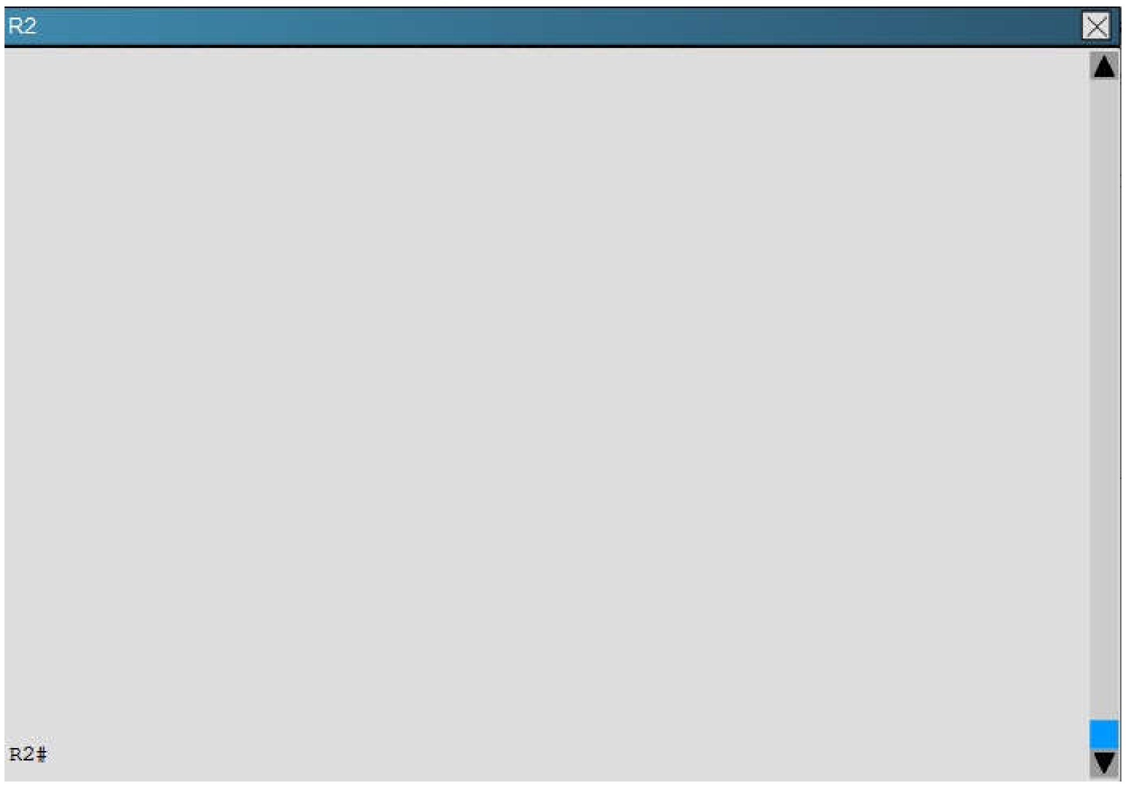
```
R5#show ip route
R5#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Loopback0
L        10.10.10.1/32 is directly connected, Loopback0
      172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.18.40.0/24 is directly connected, Ethernet0/0
L        172.18.40.2/32 is directly connected, Ethernet0/0
R5#show ip ospf
R5#show ip ospf ne
R5#show ip ospf neighbor
R5#show ip ospf neighbor
R5#



R5#
```

Question Set 1

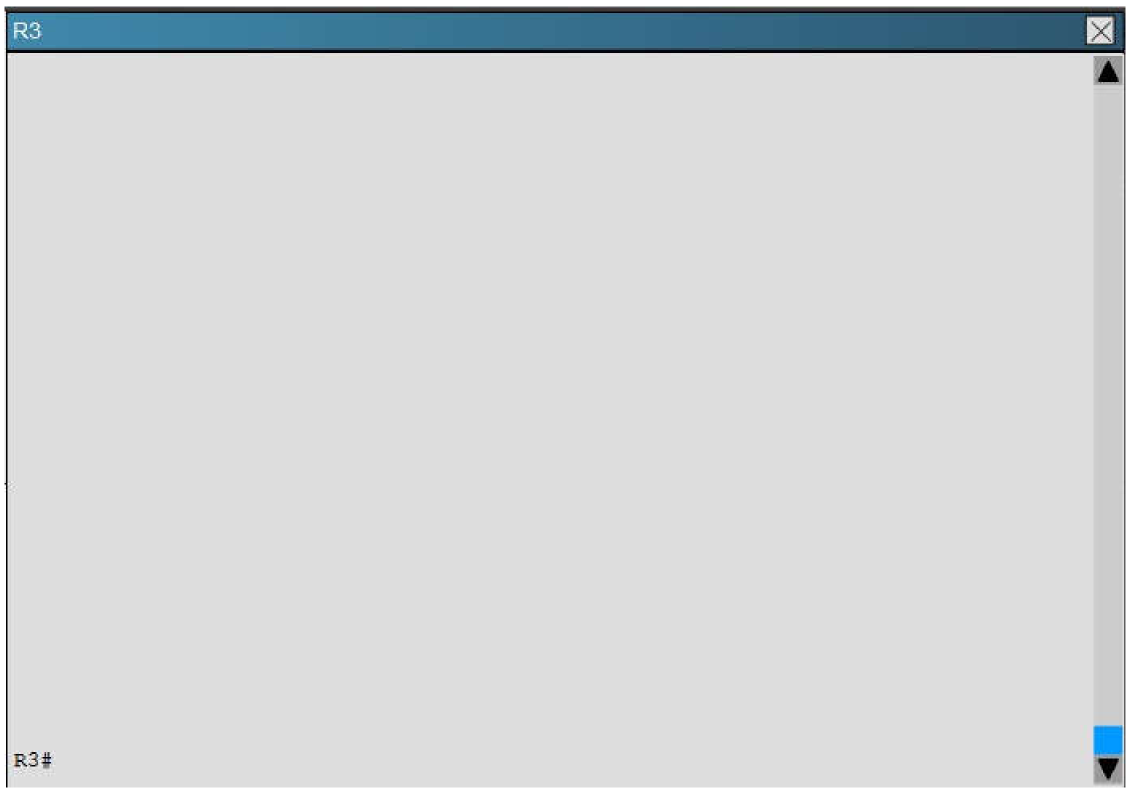
QUESTION 1
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.



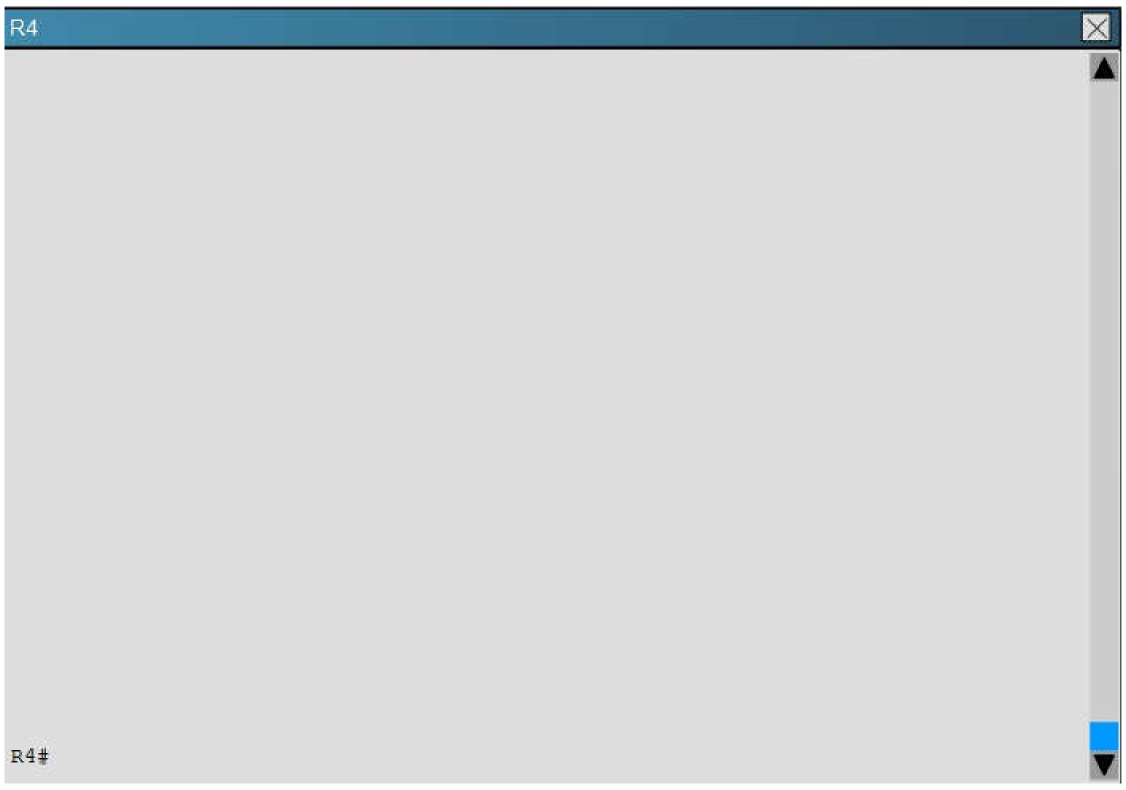
```
R1#
```



```
R2#
```



```
R3#
```



```
R4#
```

```
R5#
```

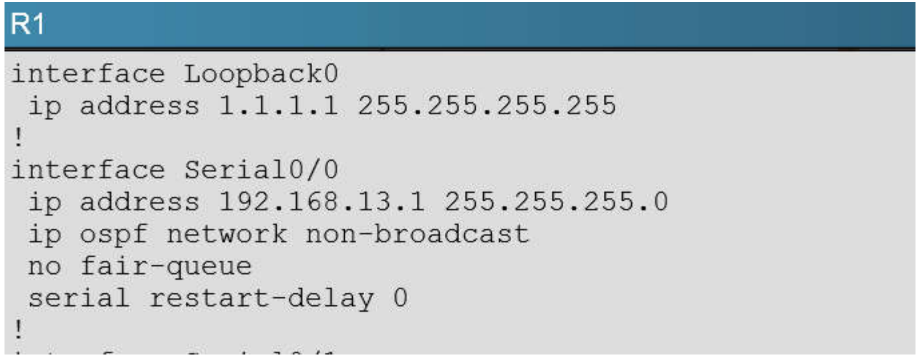
```
R6#
```

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

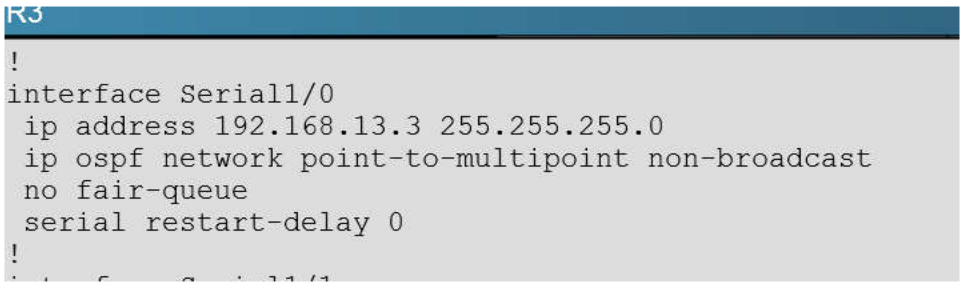
A. The serial interface in R1 should be taken out of the shutdown state.
B. A neighbor statement needs to be configured in R1 and R3 pointing at each other.
C. The R1 network type should be changed to point-to-multipoint non-broadcast.
D. The hello, dead and wait timers on R1 need to be reconfigured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

Correct Answer: C
Section: [none]
Explanation

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

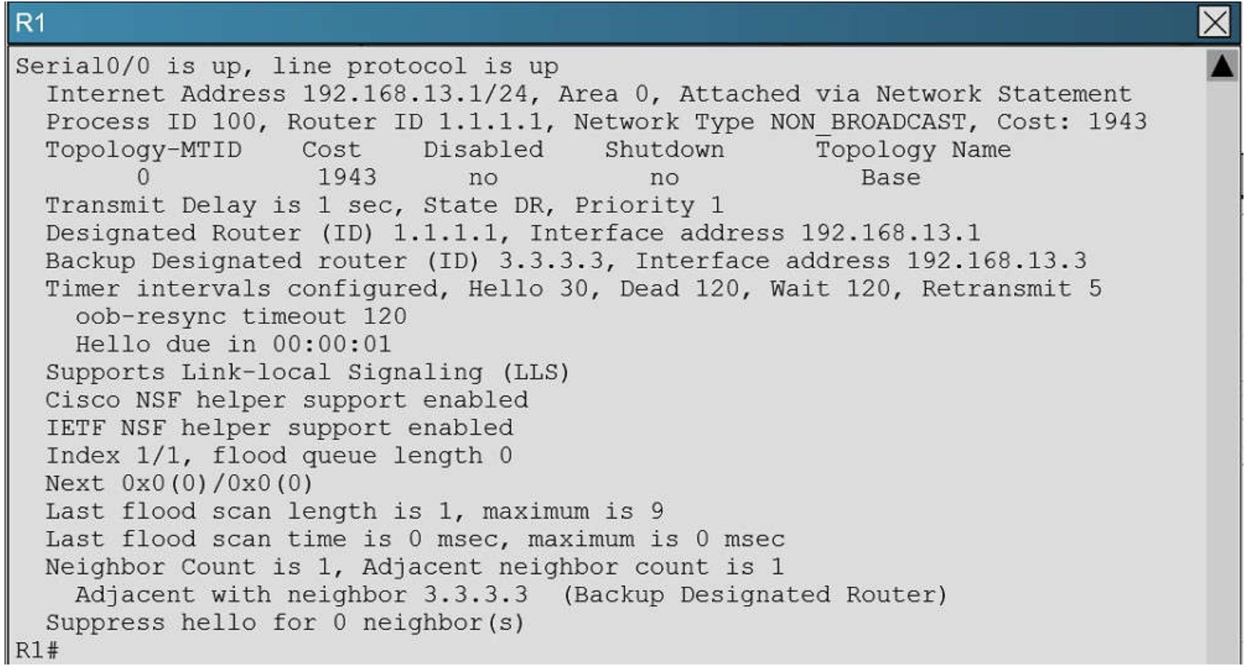


```
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Serial0/0
 ip address 192.168.13.1 255.255.255.0
 ip ospf network non-broadcast
 no fair-queue
 serial restart-delay 0
!
```

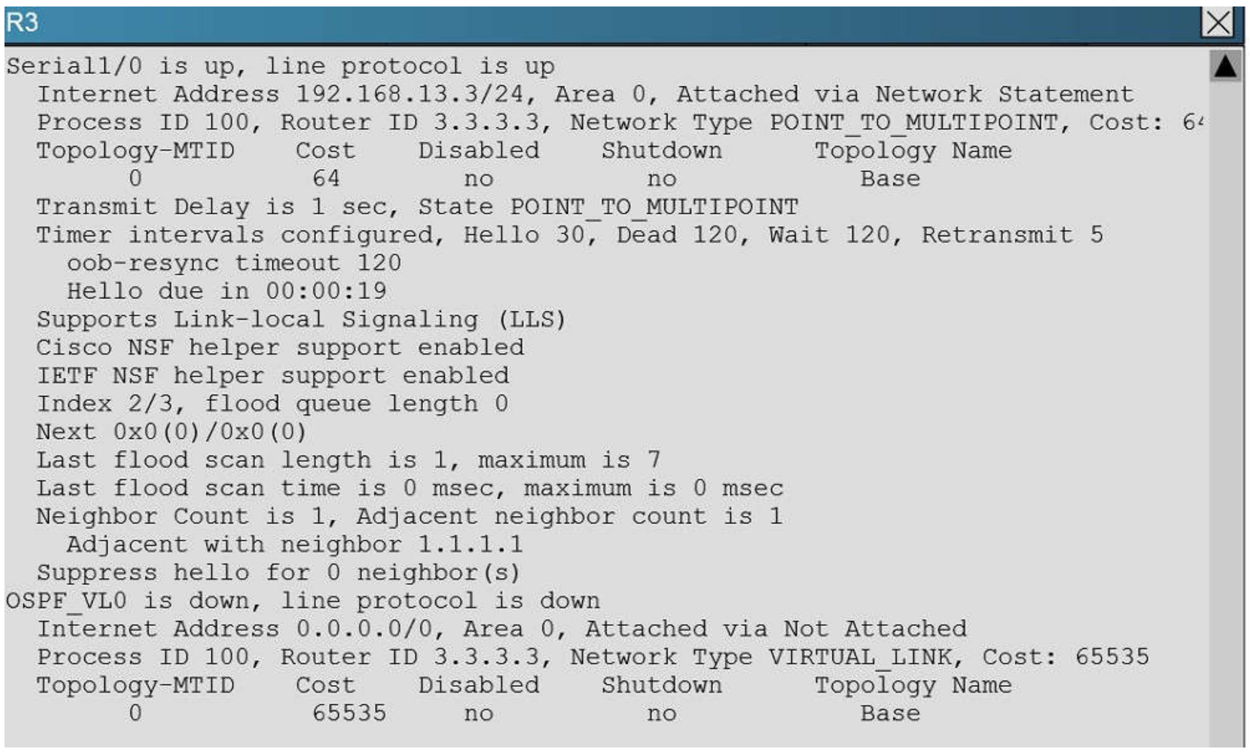


```
!
interface Serial1/0
 ip address 192.168.13.3 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
 no fair-queue
 serial restart-delay 0
!
```

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



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

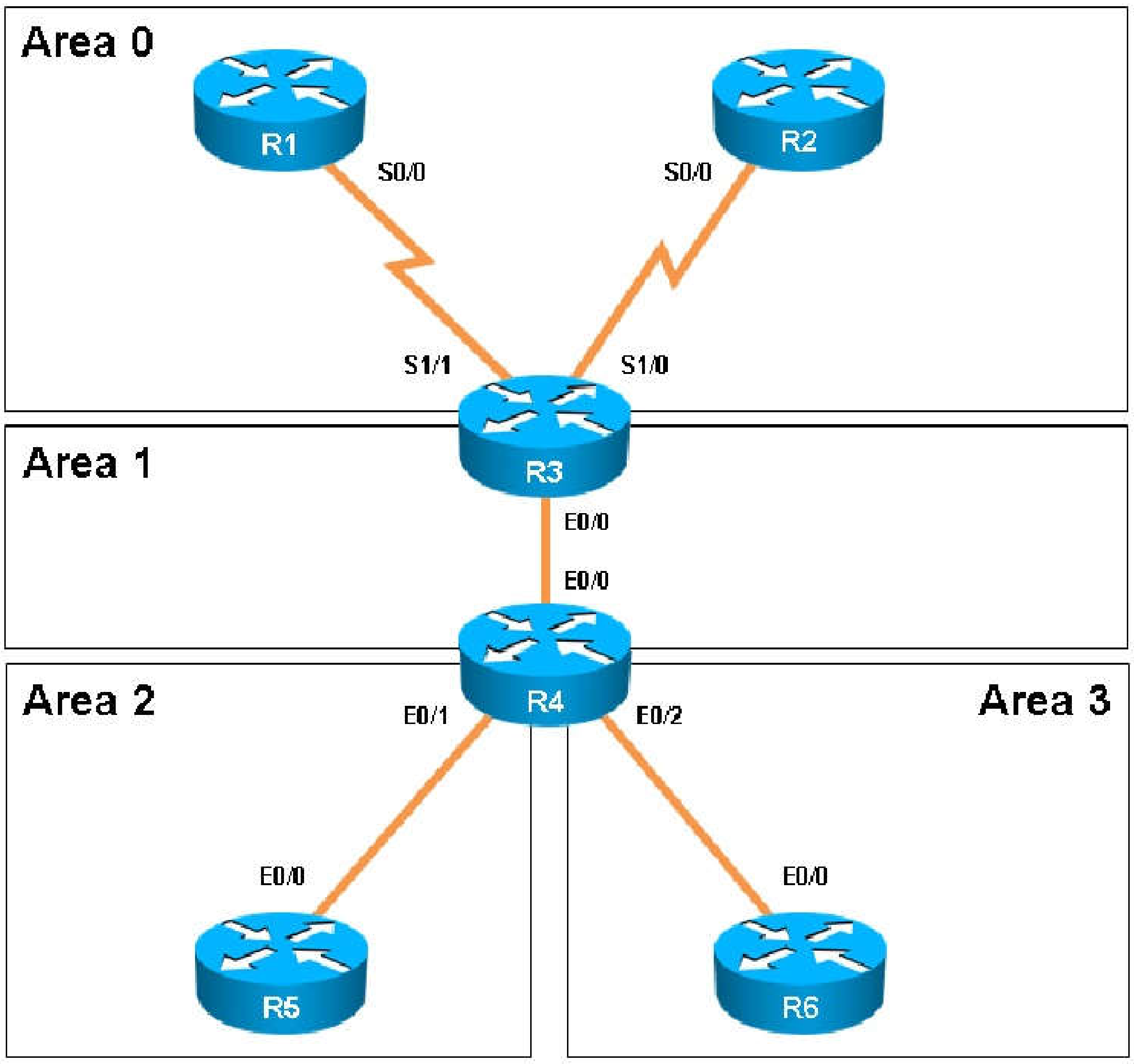


```
Serial1/0 is up, line protocol is up
  Internet Address 192.168.13.3/24, Area 0, Attached via Network Statement
  Process ID 100, Router ID 3.3.3.3, Network Type POINT_TO_MULTIPOINT, Cost: 6
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:19
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 7
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
OSPF_VL0 is down, line protocol is down
  Internet Address 0.0.0.0/0, Area 0, Attached via Not Attached
  Process ID 100, Router ID 3.3.3.3, Network Type VIRTUAL_LINK, Cost: 65535
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           65535     no          no            Base
```

QUESTION 2

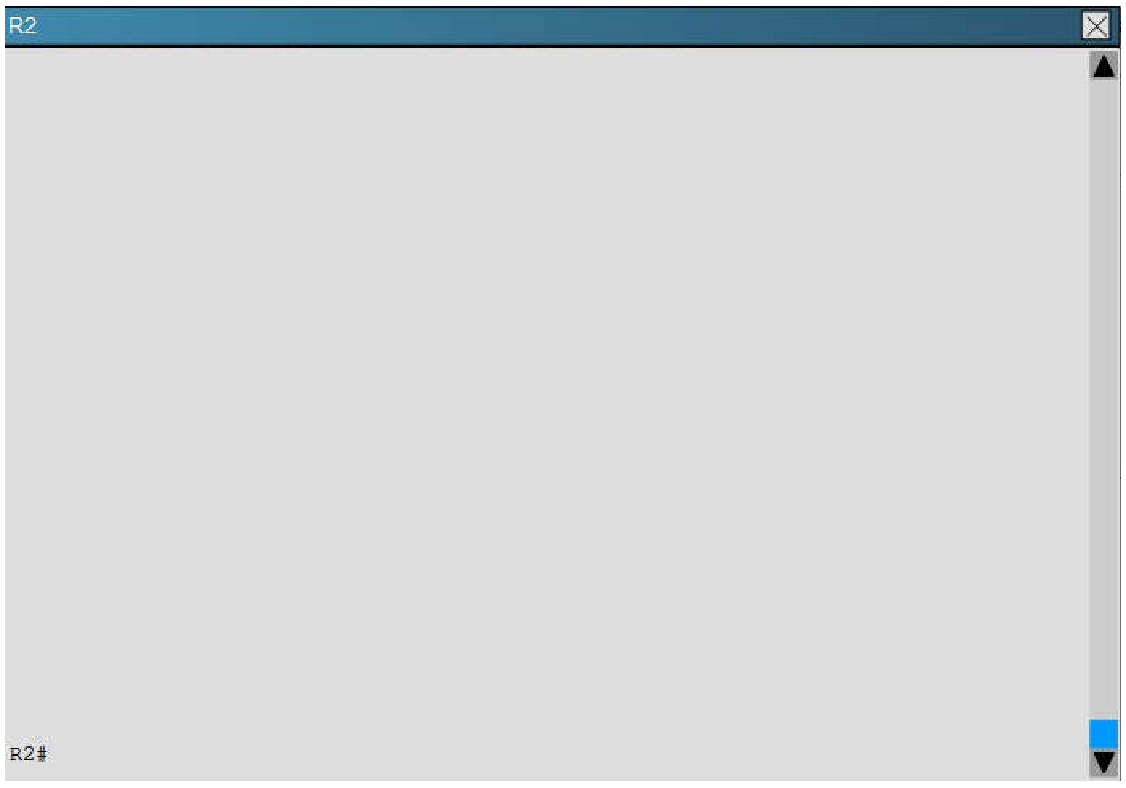
Scenario:

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

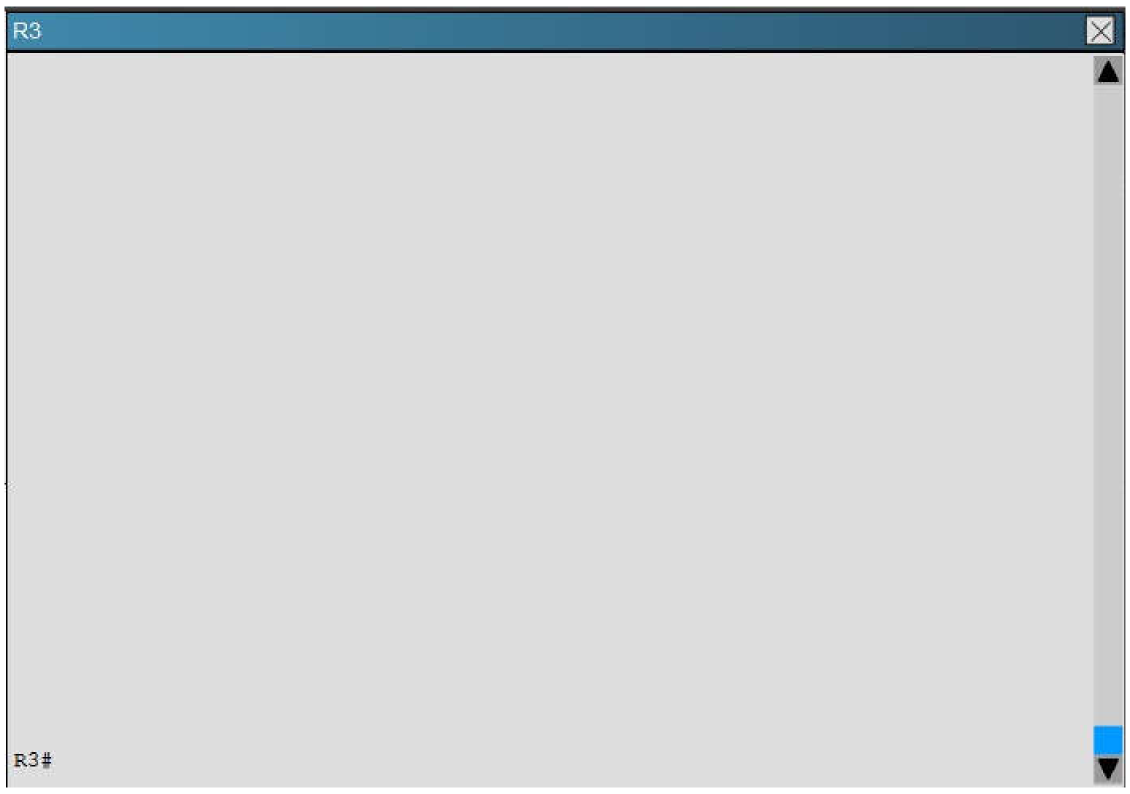

Area 0
R1
S0/0
R2
S0/0
S1/1
S1/0
Area 1
R3
E0/0
E0/0
Area 2
E0/1
R4
E0/2
Area 3
E0/0
E0/0
R5
R6

R1

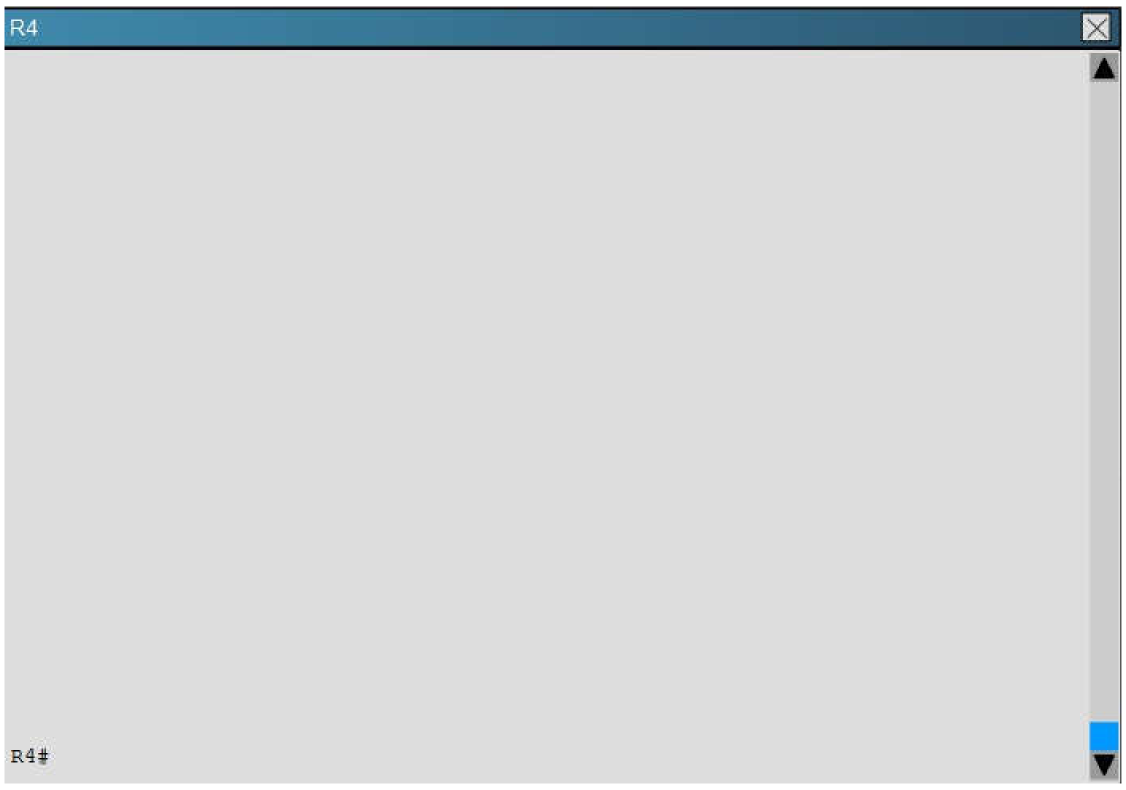
```
R1#
```


R2

```
R2#
```



```
R3#
```



```
R4#
```

```
R5#
```

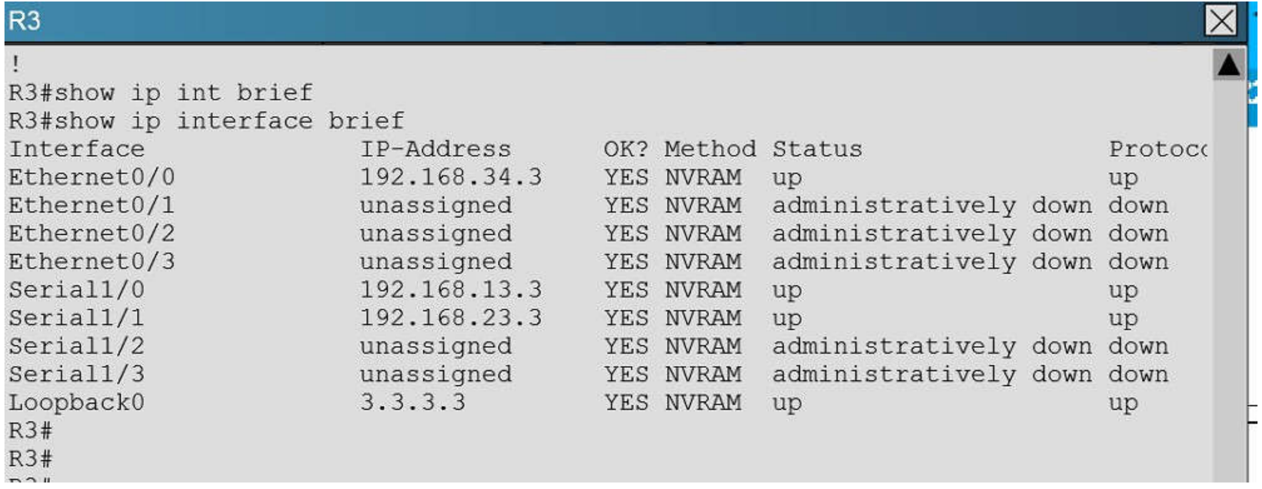
```
R6#
```

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

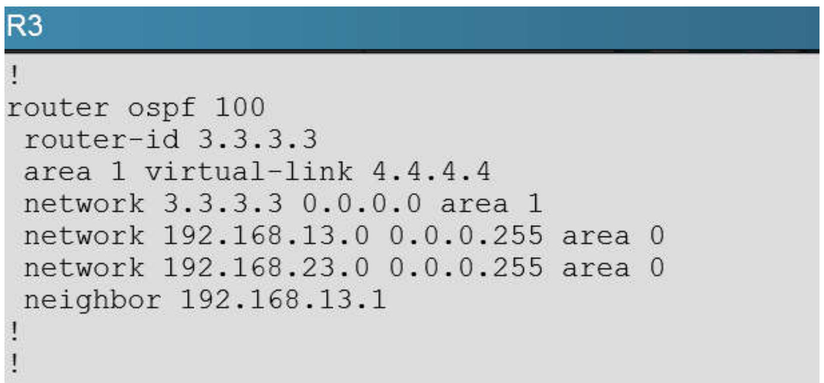
A. Configure R4 with a virtual link to 192.168.13.2
B. Change the R3 and R4 hello-interval and retransmit-interface timers to zero so the link won't go down.
C. Add an OSPF network statement for 4.4.4.4 0.0.0.0 area 1 in R3
D. Add an OSPF network statement for 192.168.34.3 0.0.0.255 area 2 in R3
E. Add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

Correct Answer: E
Section: [none]
Explanation

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



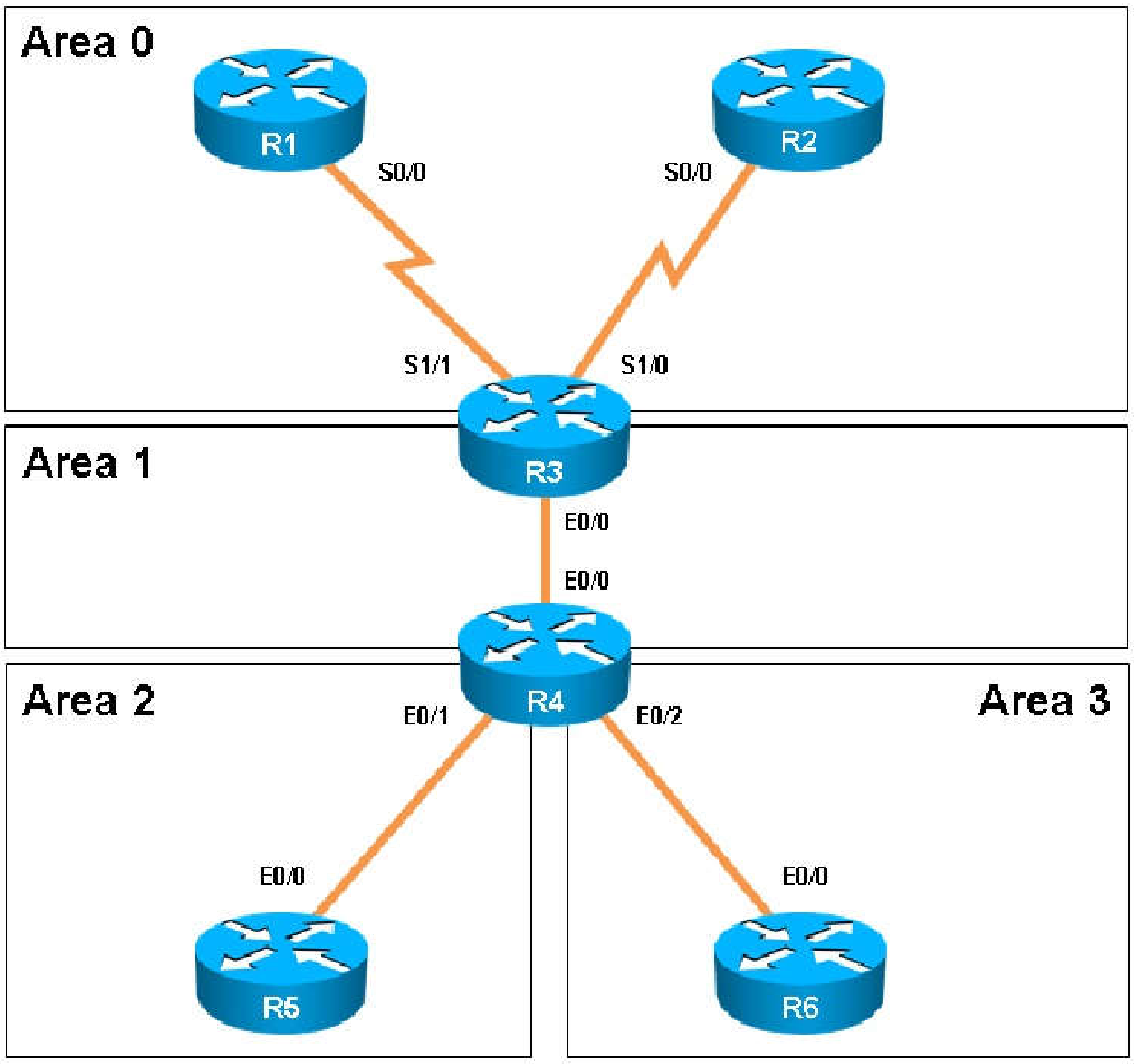
```
!
R3#show ip int brief
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protoco
Ethernet0/0            192.168.34.3    YES NVRAM  up                    up
Ethernet0/1            unassigned      YES NVRAM  administratively down down
Ethernet0/2   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



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

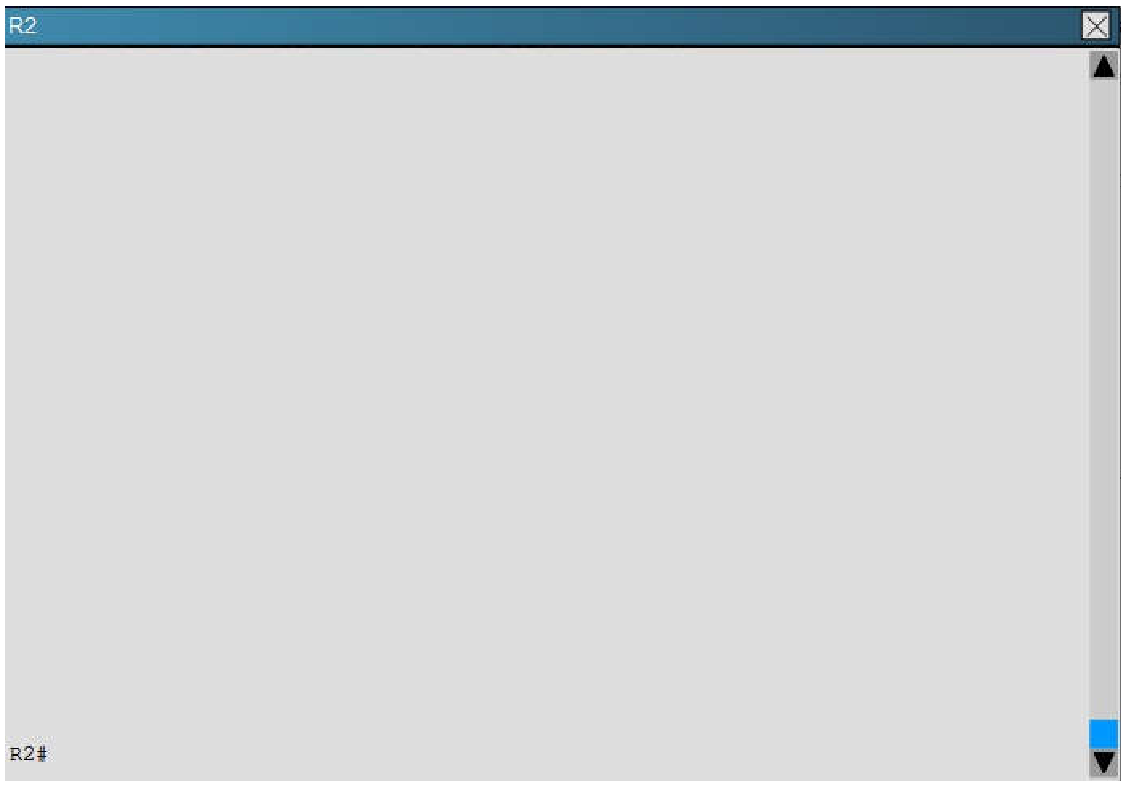
Based on the network diagram, this link should be added to Area 1, not Area 2.

QUESTION 3
Scenario:
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.

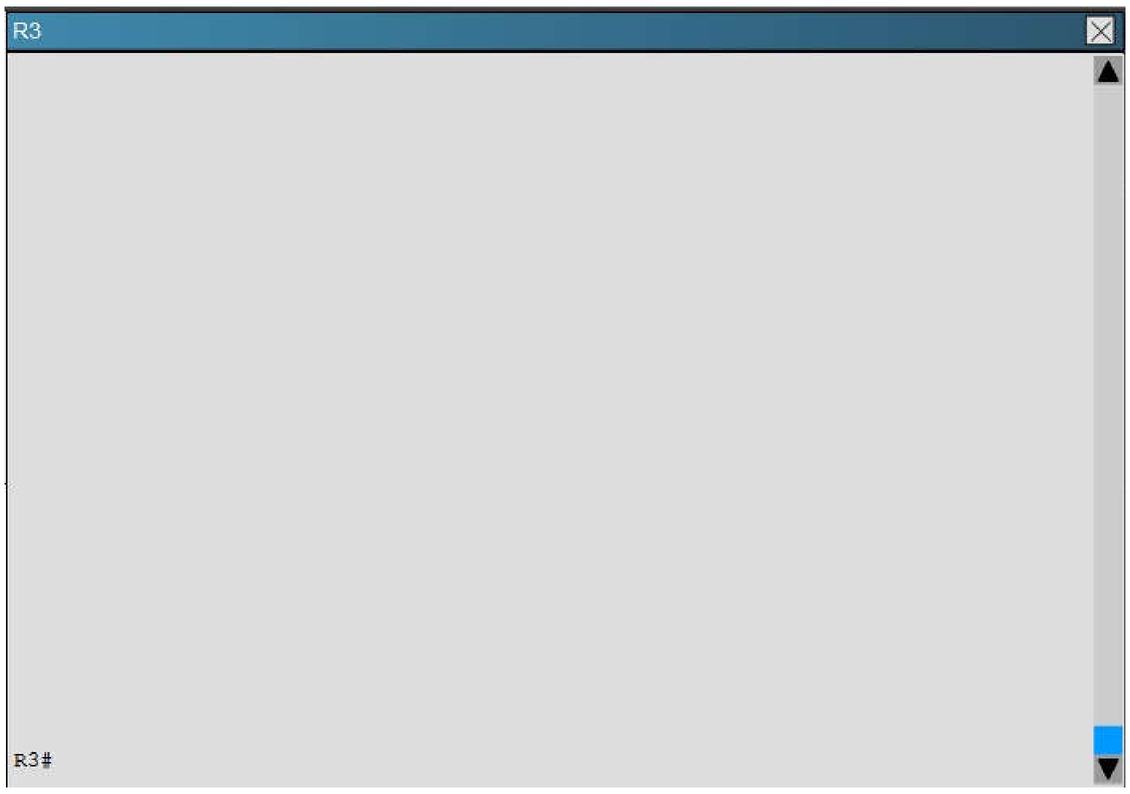

Area 0
R1
R2
S0/0
S0/0
S1/1
S1/0
Area 1
R3
E0/0
E0/0
Area 2
R4
E0/1
E0/2
Area 3
E0/0
E0/0
R5
R6

R1

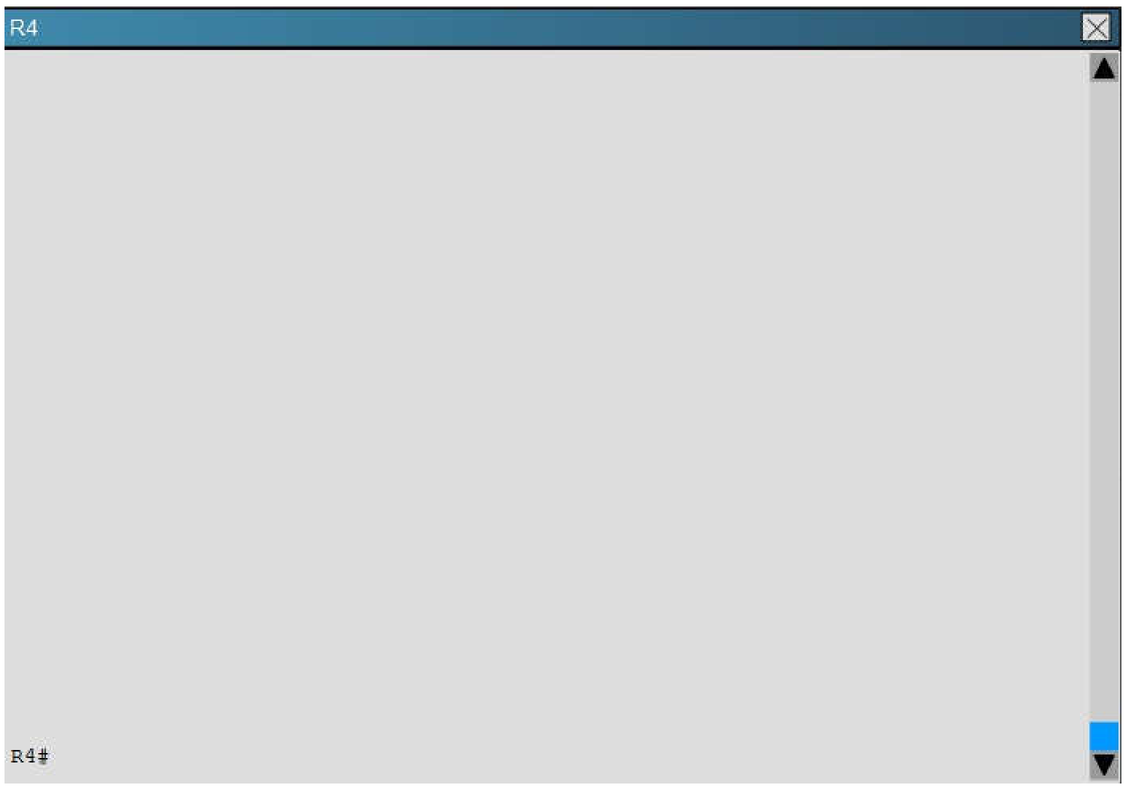
```
R1#
```


R2

```
R2#
```



```
R3#
```



```
R4#
```

```
R5#
```

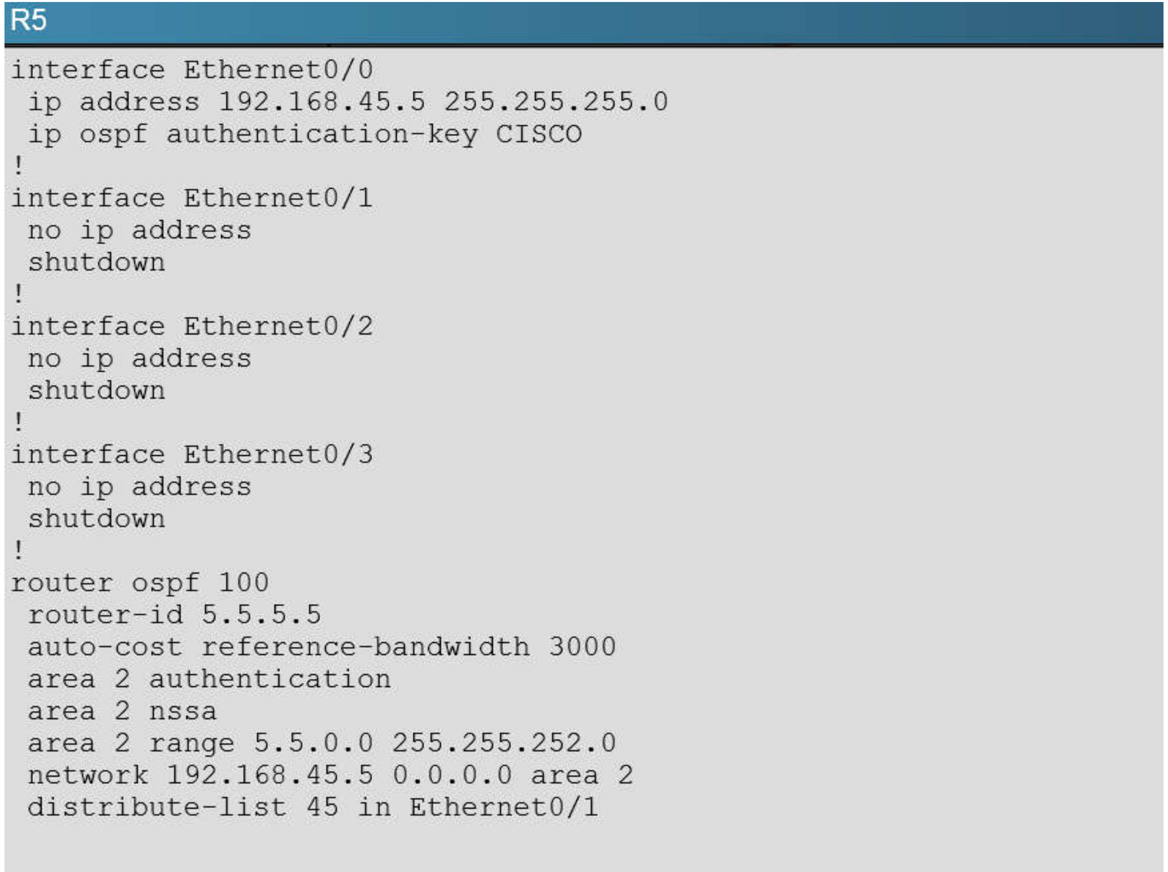
```
R6#
```

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

A. Configure R4 and R5 to use MD5 authentication on the Ethernet interfaces that connect to the common subnet.
B. Configure Area 1 in both R4 and R5 to use MD5 authentication.
C. Add 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.

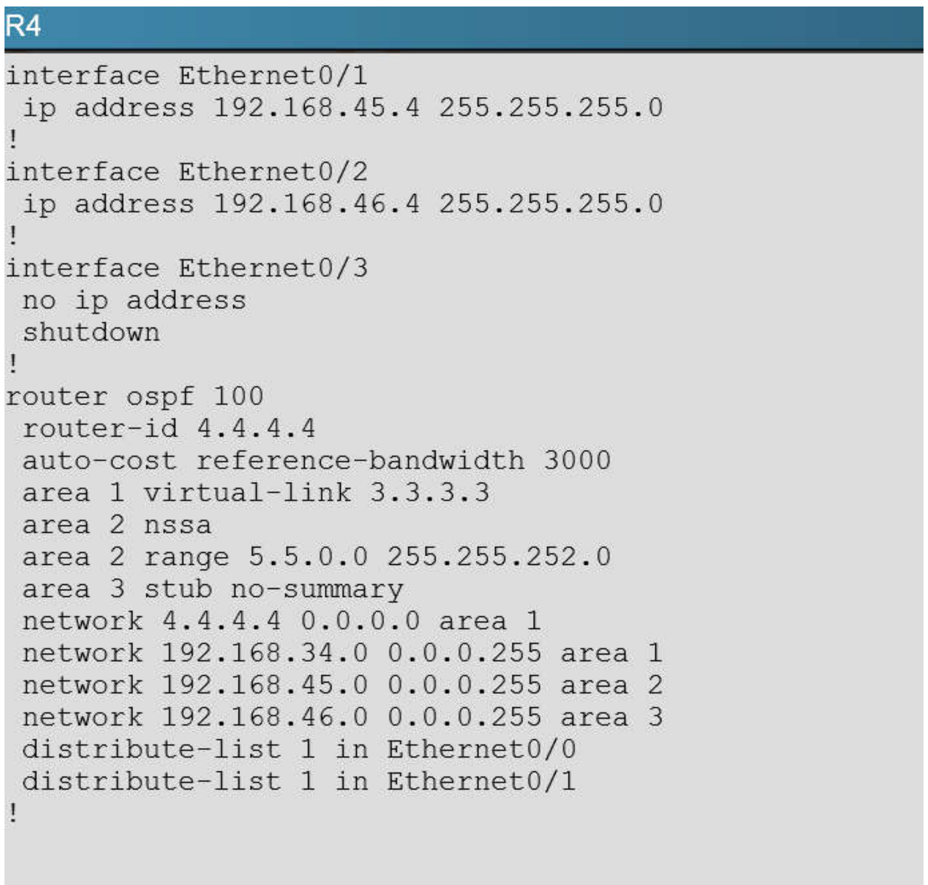
Correct Answer: D
Section: [none]
Explanation

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



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

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



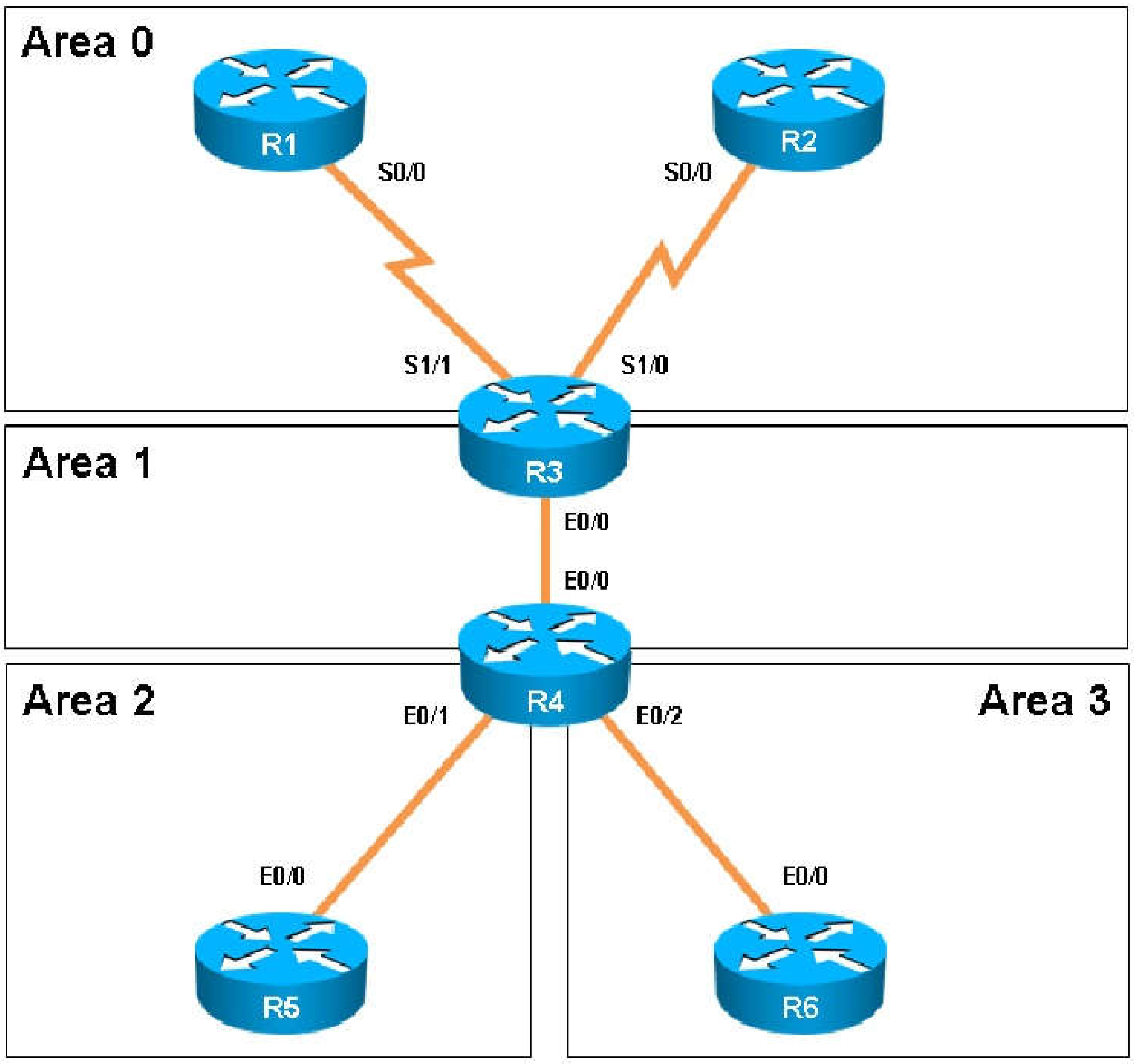
R4

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

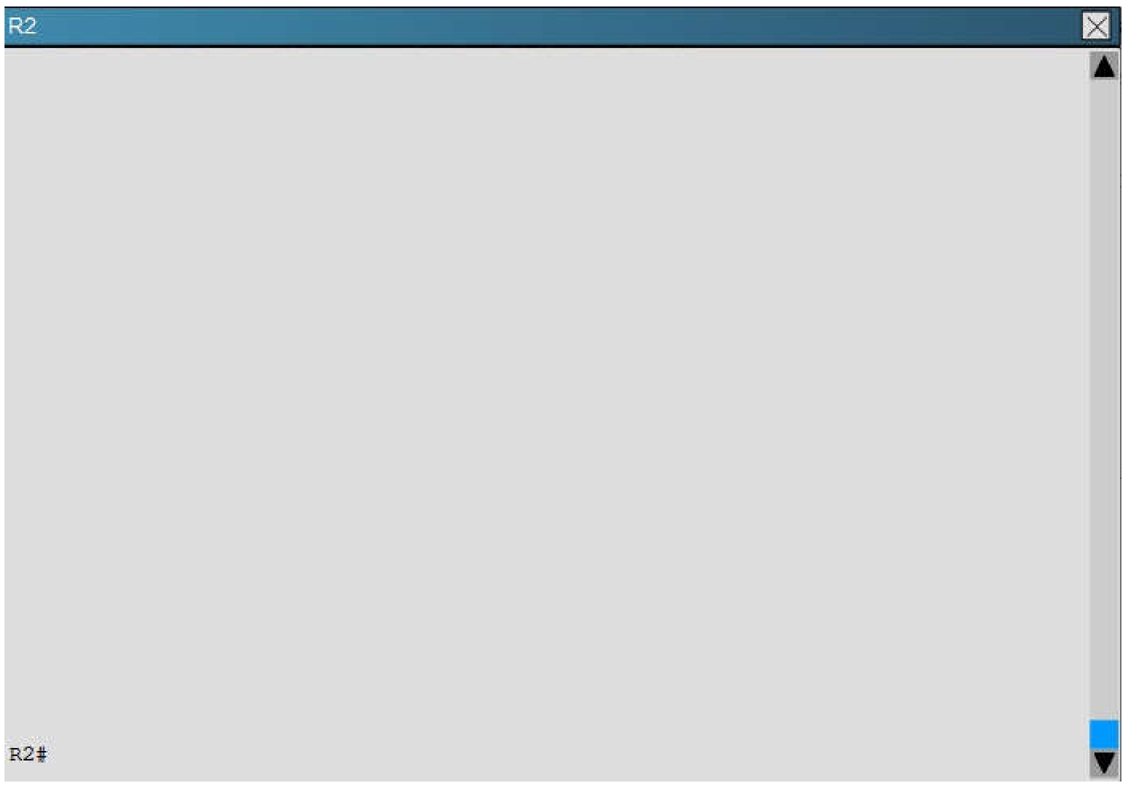
QUESTION 4

Scenario:

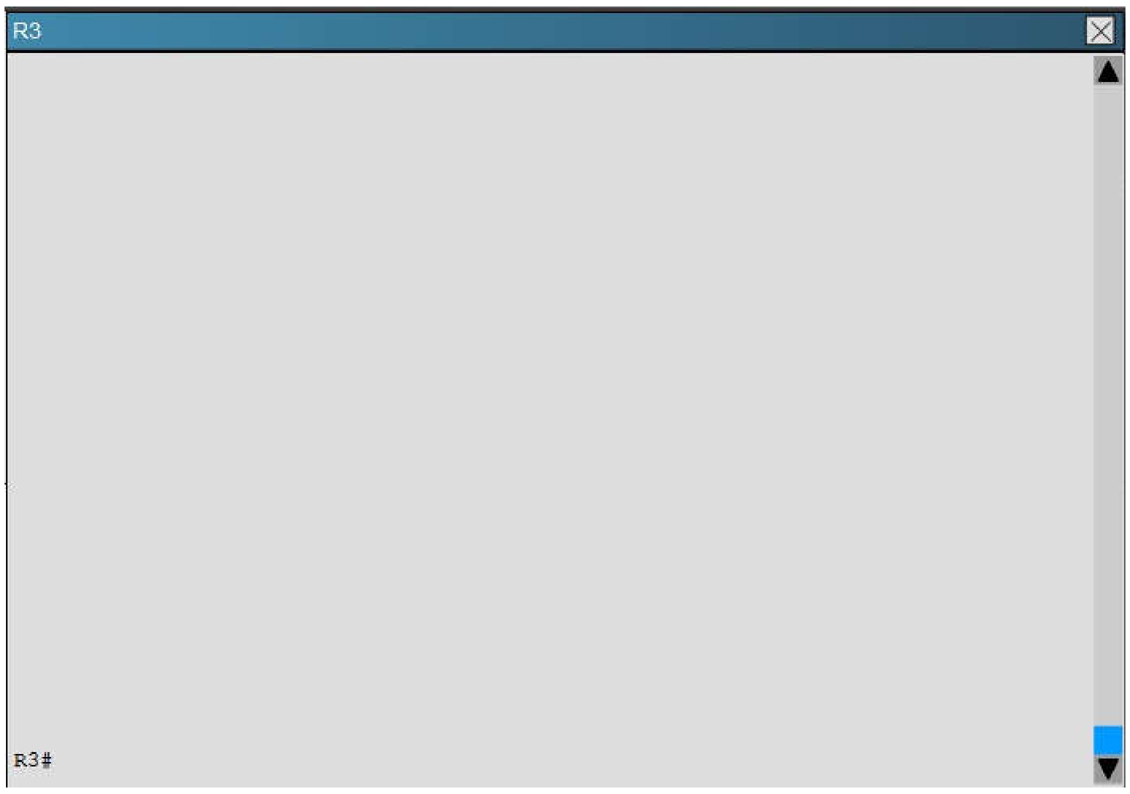
A customer network engineer has edited their OSPF network configuration and now your customer is experiencing network issues. They have contacted you to resolve the issues and return the network to full functionality.



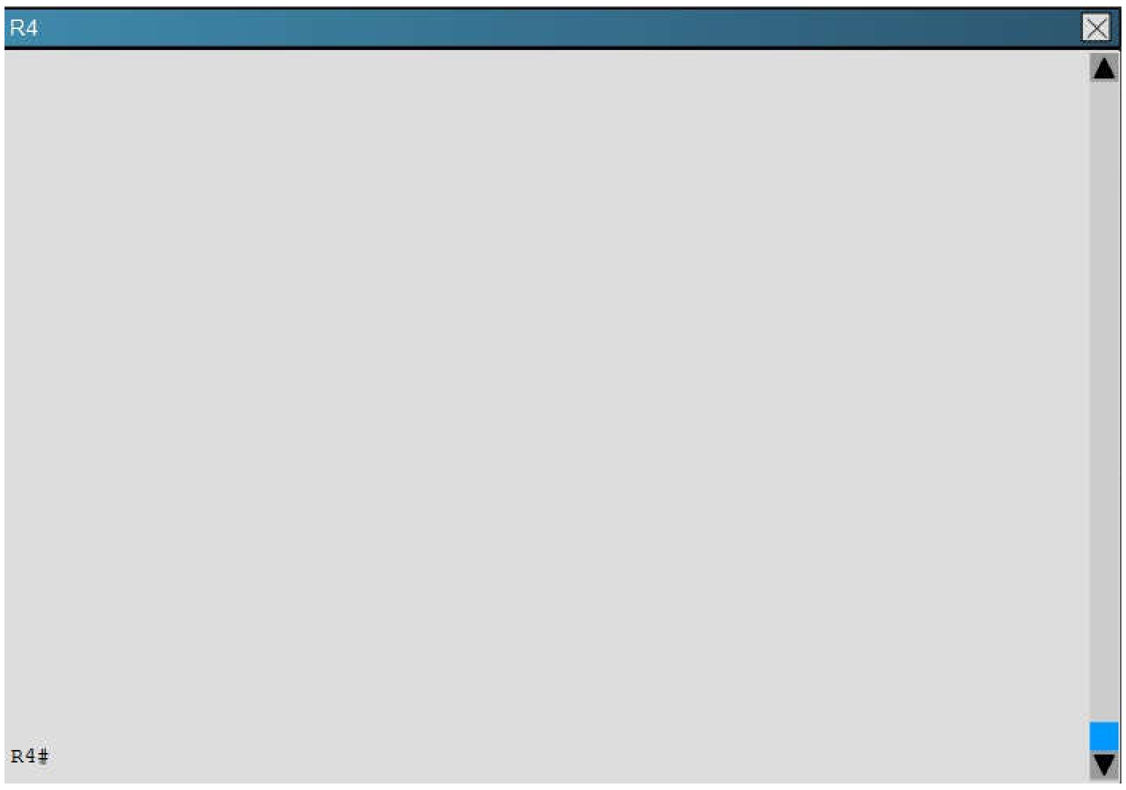
```
R1#
```



```
R2#
```



```
R3#
```



```
R4#
```

```
R5#
```

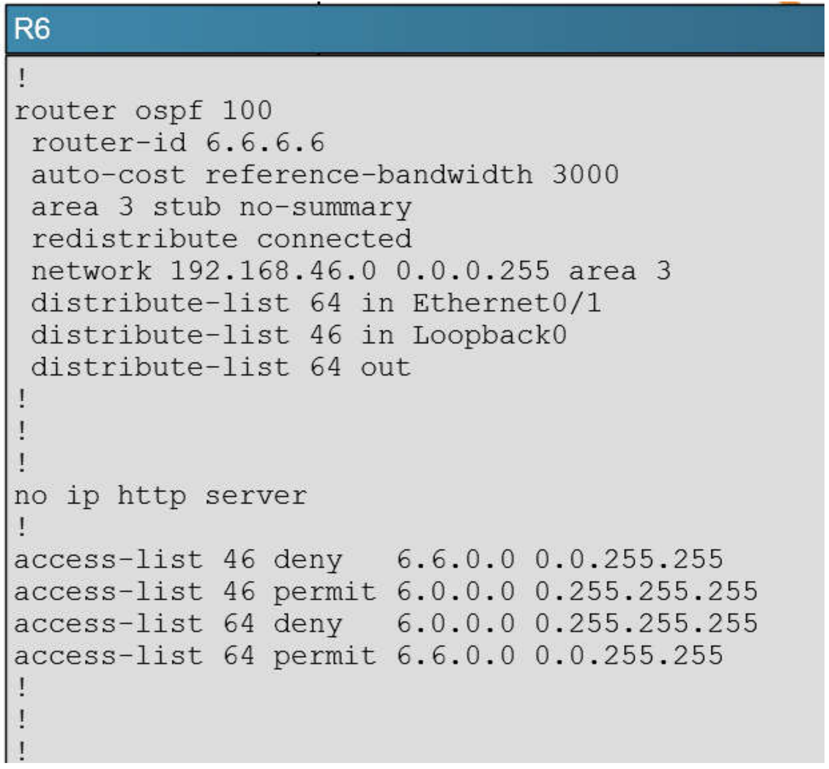
```
R6#
```

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

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

Correct Answer: D
Section: [none]
Explanation

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



R6

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

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

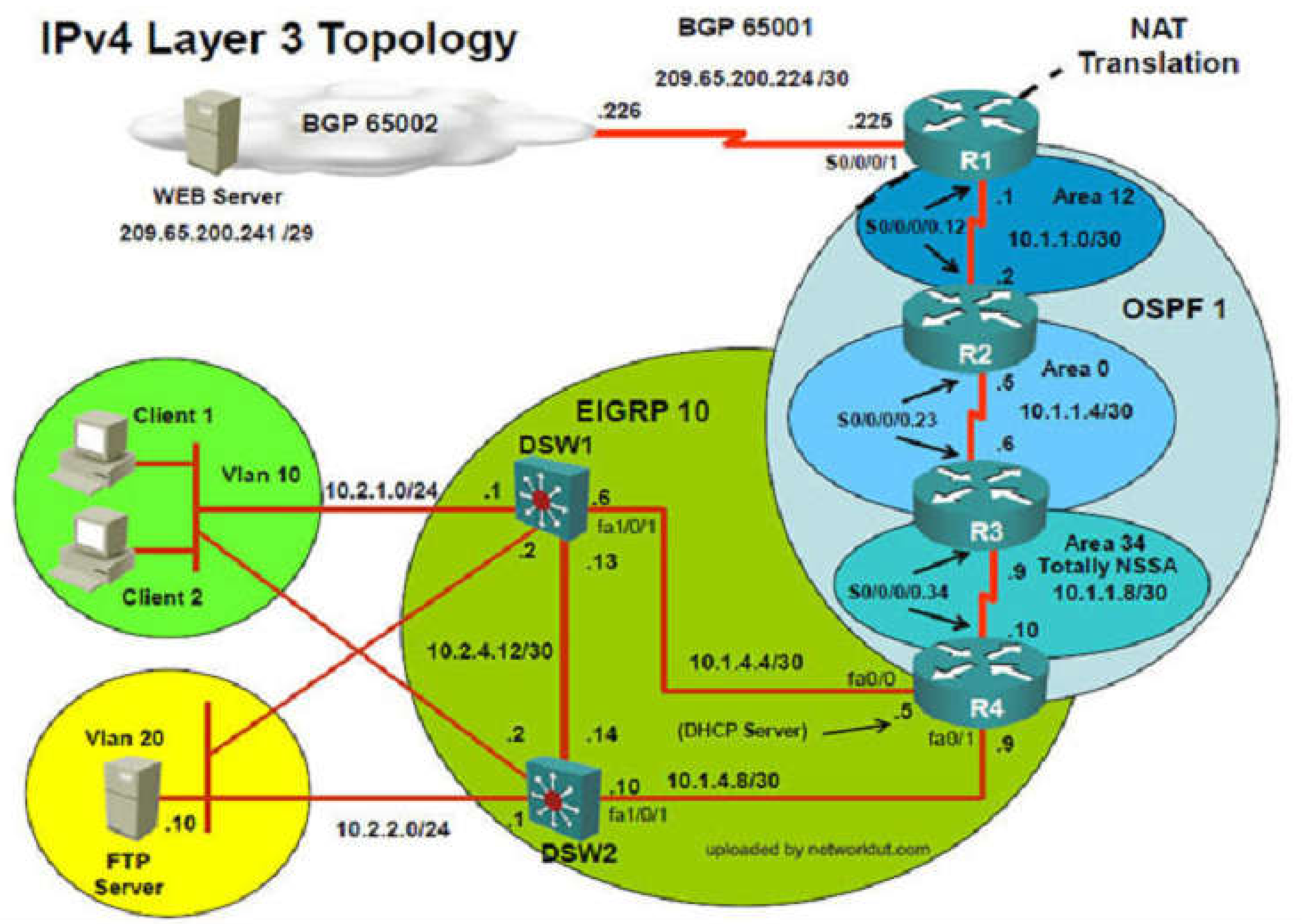
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

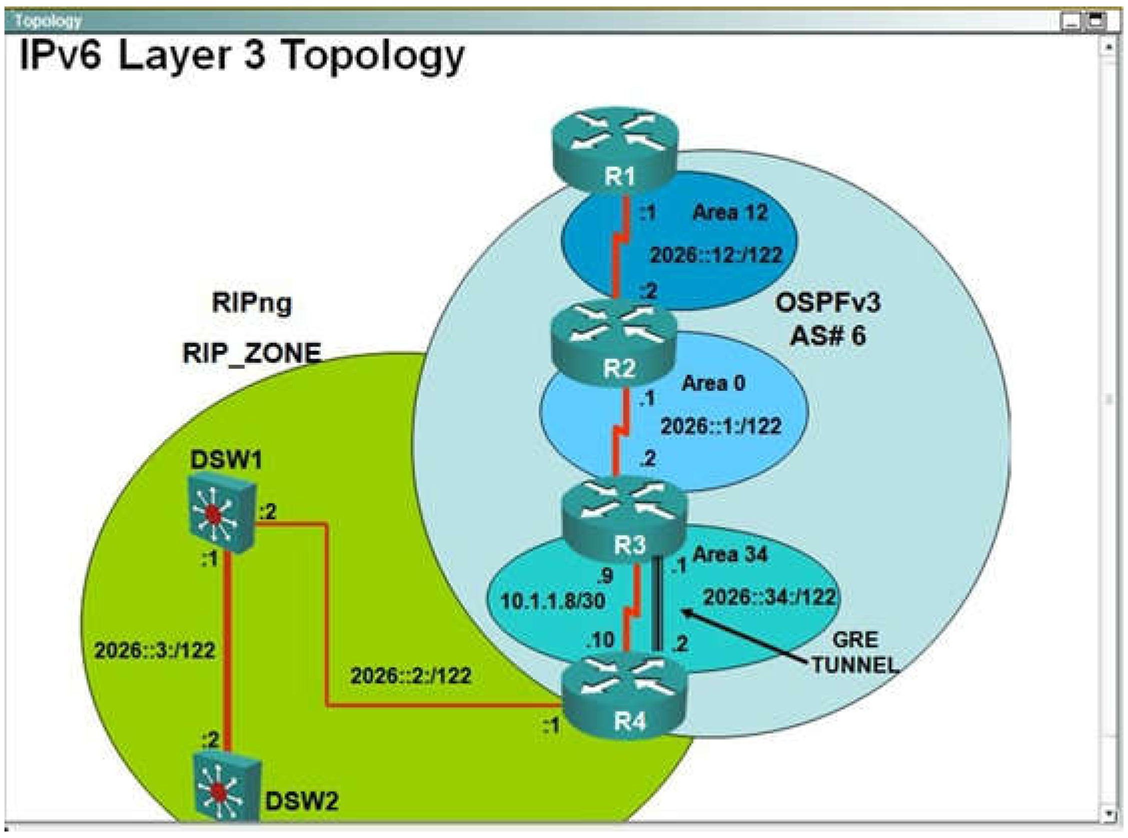
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

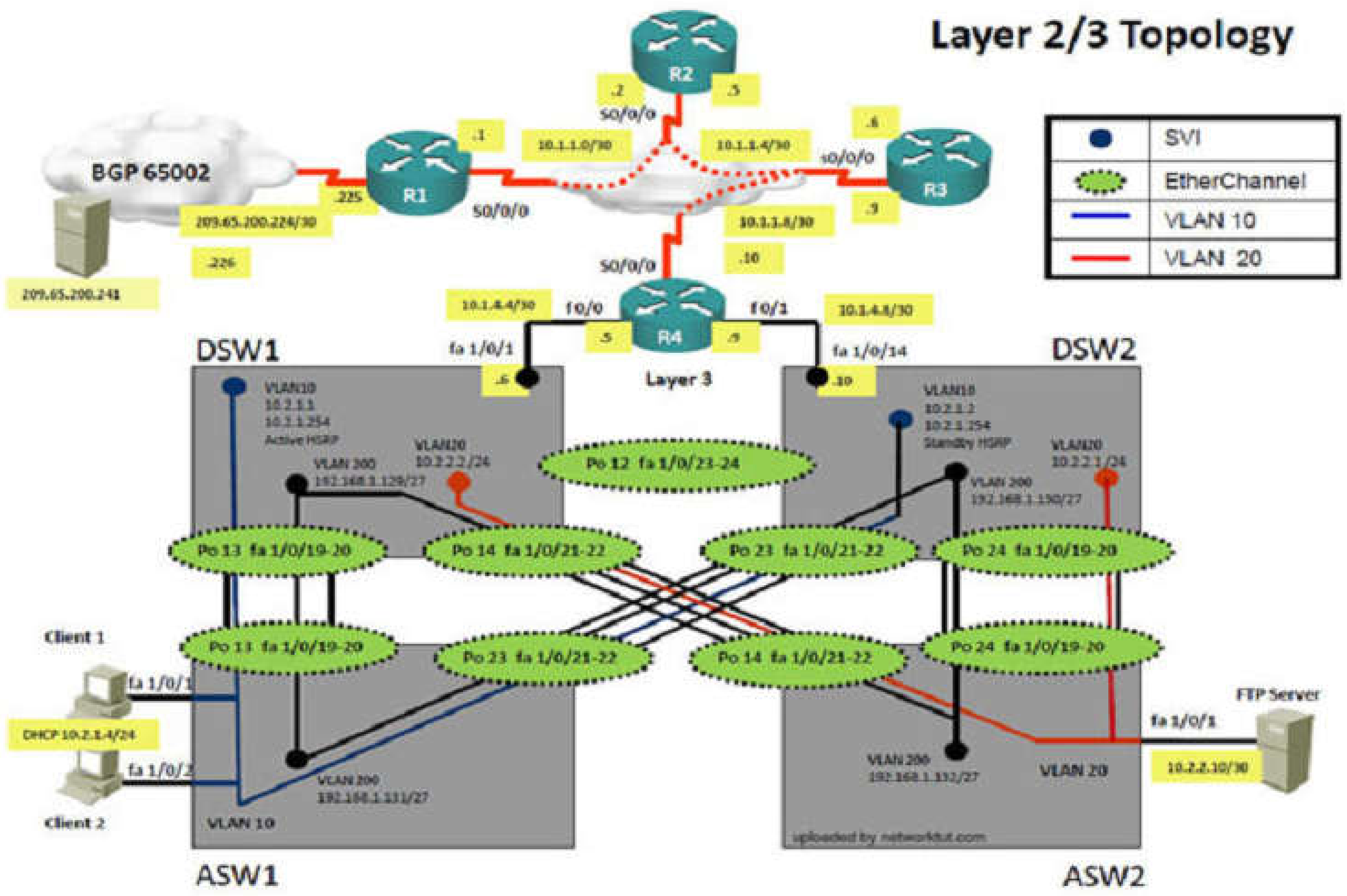
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

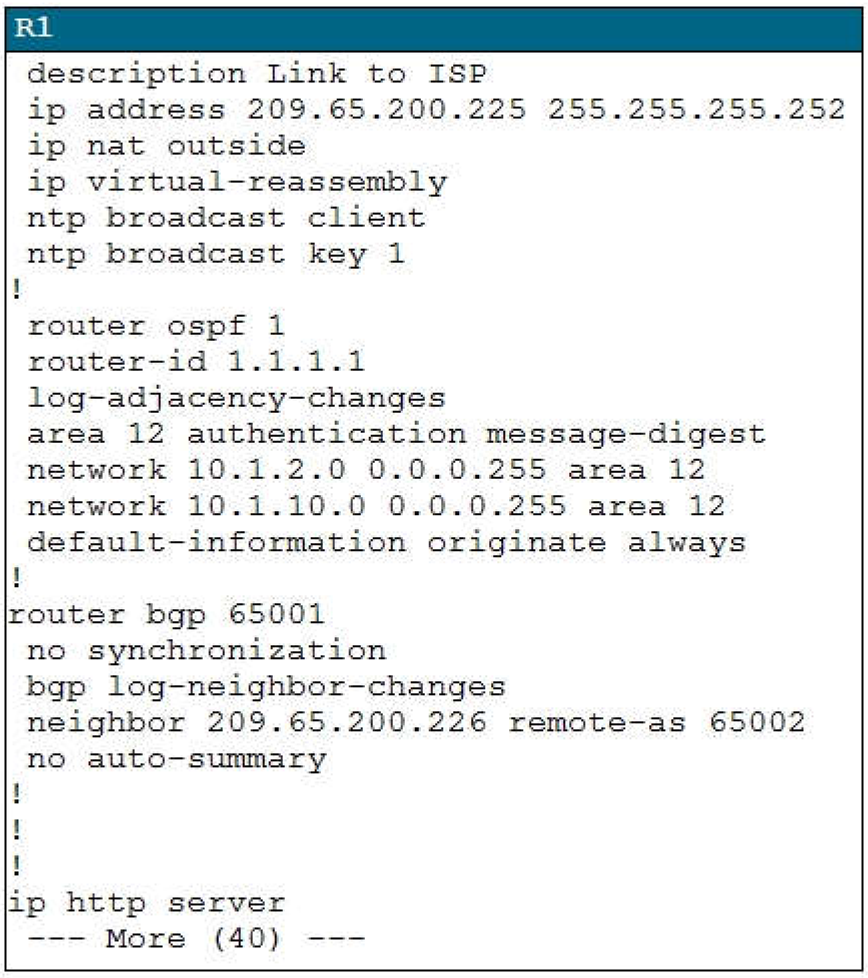
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution


IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT
Translation
BGP 65002
WEB Server
209.65.200.241 /29
.226
.225
S0/0/0/1
R1
.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
Client 1
Vlan 10
10.2.1.0/24
Client 2
EIGRP 10
DSW1
.1
.6
fa1/0/1
.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
fa1/0/1
.1
FTP
Server
10.2.2.0/24
DSW2
uploaded by networldut.com

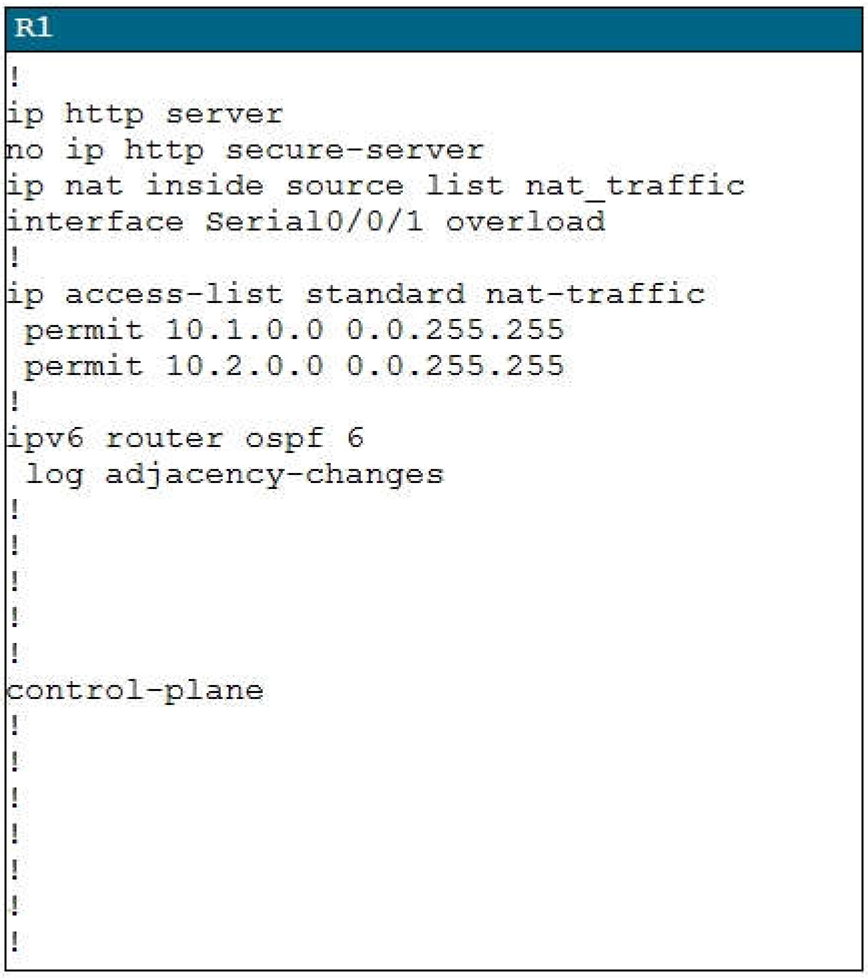

Topology
IPv6 Layer 3 Topology
R1
:1
Area 12
2026::12:/122
:2
OSPFv3
AS# 6
RIPng
RIP_ZONE
R2
Area 0
.1
2026::1:/122
.2
DSW1
:2
R3
:1
Area 34
.9
.1
10.1.1.8/30
2026::34:/122
2026::3:/122
.10
.2
GRE
TUNNEL
2026::2:/122
:1
R4
:2
DSW2





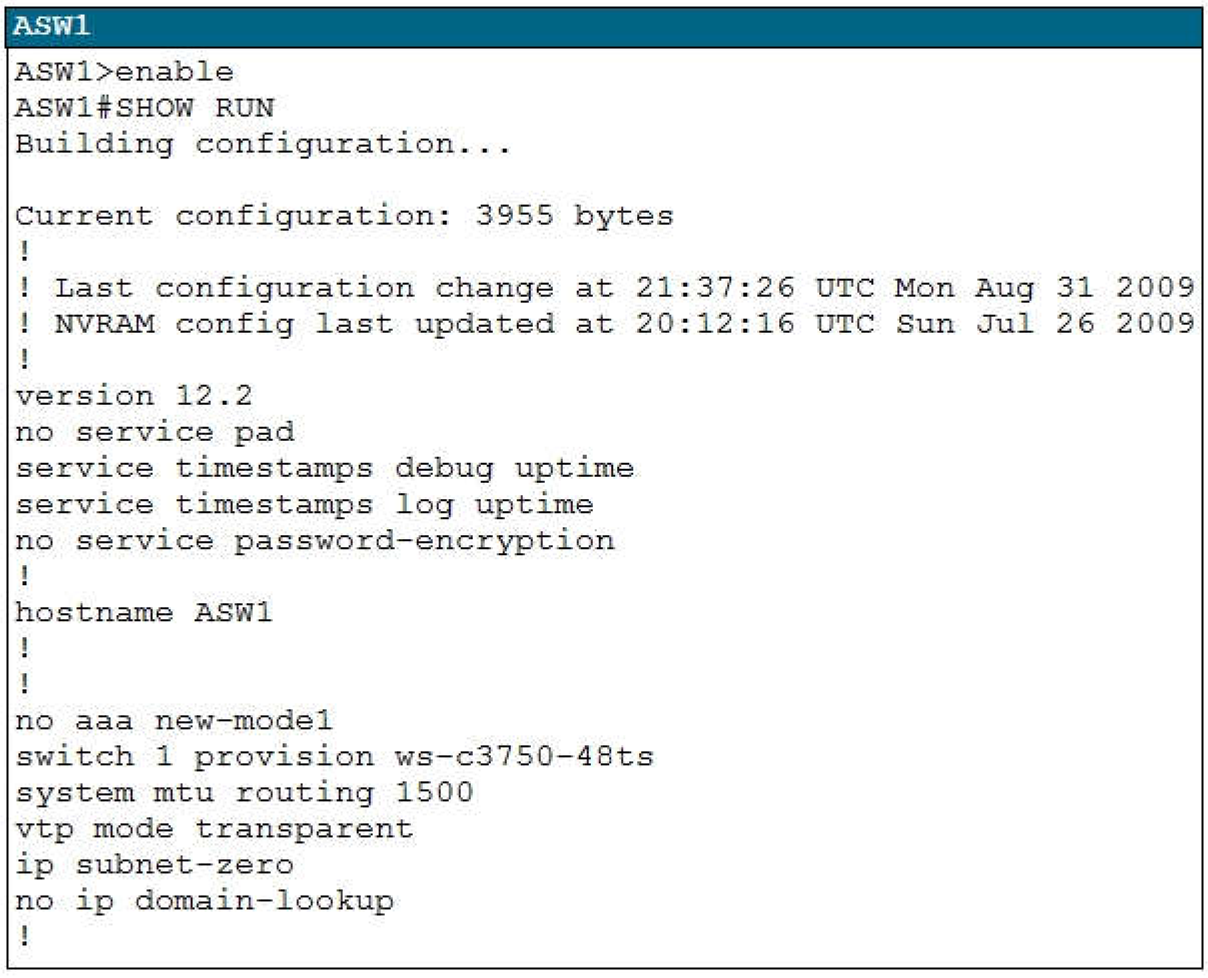
R1

```
 description Link to ISP
 ip address 209.65.200.225 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 ntp broadcast client
 ntp broadcast key 1
!
 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 area 12 authentication message-digest
 network 10.1.2.0 0.0.0.255 area 12
 network 10.1.10.0 0.0.0.255 area 12
 default-information originate always
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 neighbor 209.65.200.226 remote-as 65002
 no auto-summary
!
!
!
ip http server
 --- More (40) ---
```



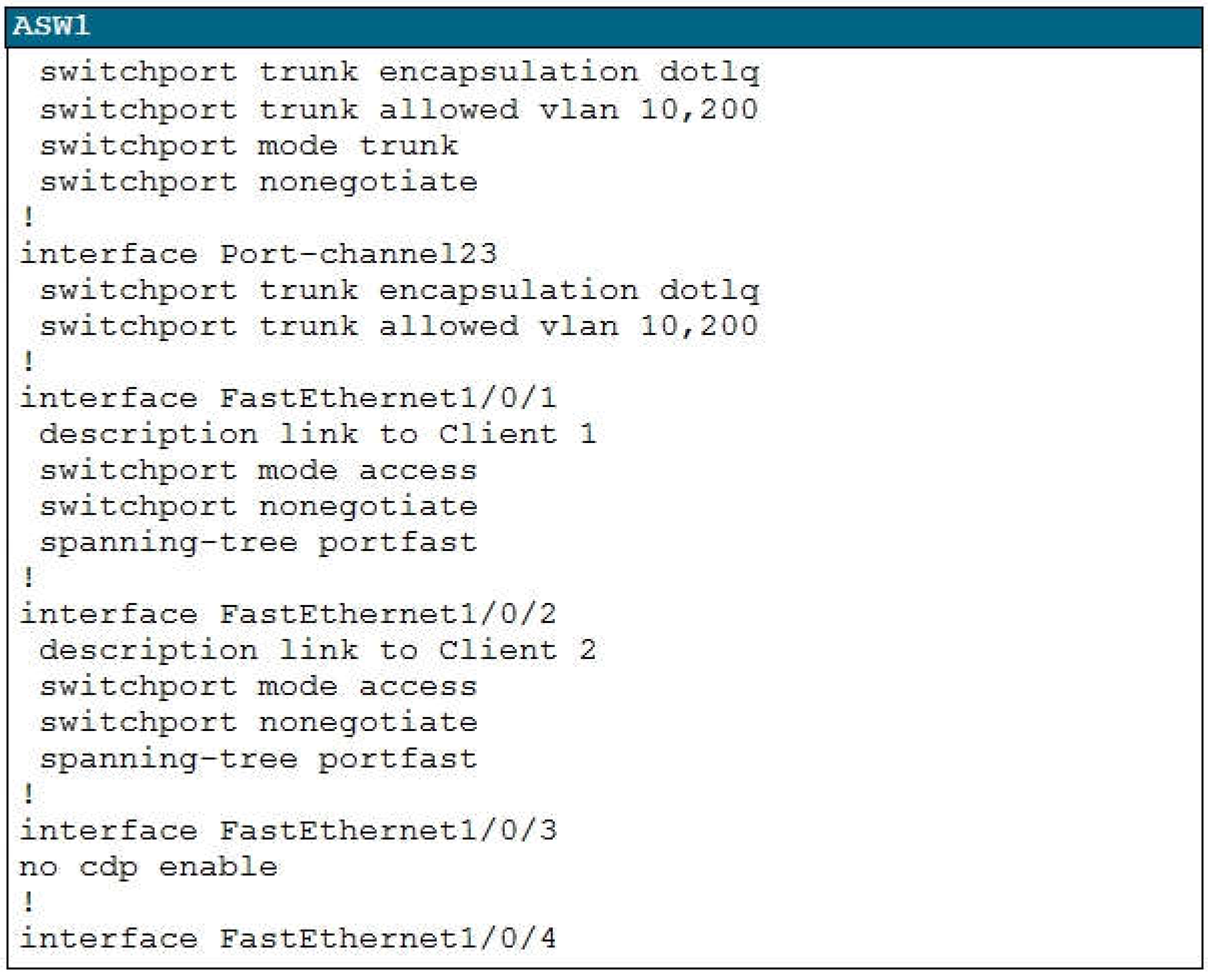
R1

```
!
ip http server
no ip http secure-server
ip nat inside source list nat_traffic
interface Serial0/0/1 overload
!
ip access-list standard nat-traffic
 permit 10.1.0.0 0.0.255.255
 permit 10.2.0.0 0.0.255.255
!
ipv6 router ospf 6
 log adjacency-changes
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
```

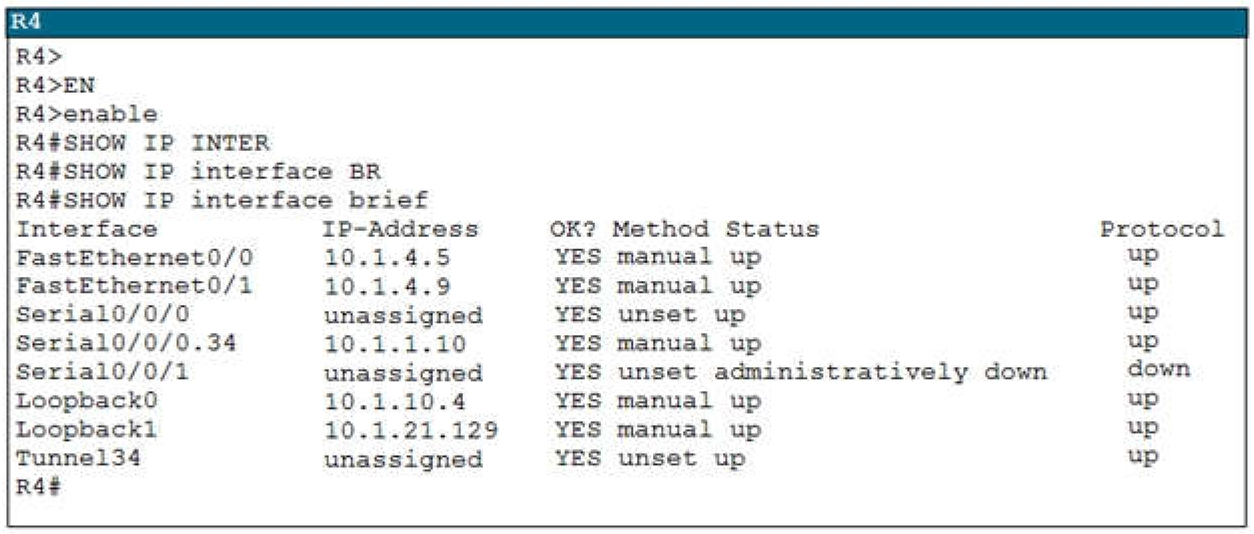


ASW1

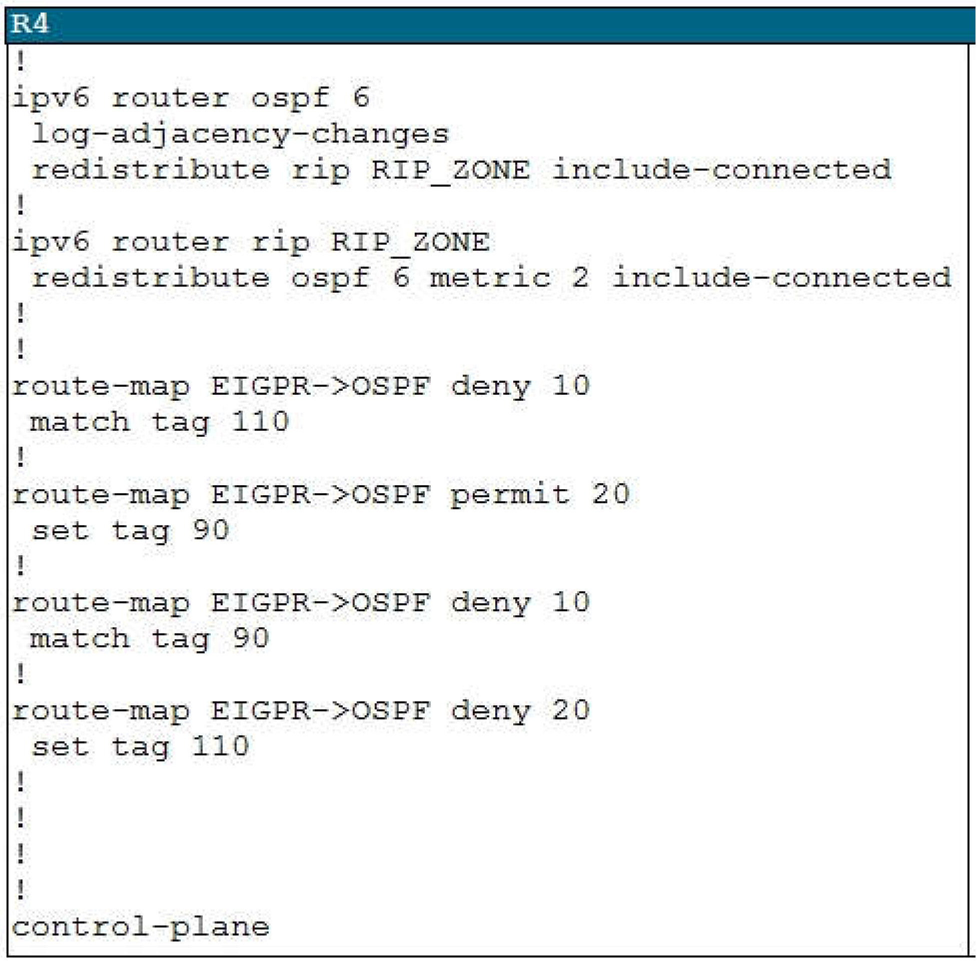
```
ASW1>enable
ASW1#SHOW RUN
Building configuration...

Current configuration: 3955 bytes
!
! Last configuration change at 21:37:26 UTC Mon Aug 31 2009
! NVRAM config last updated at 20:12:16 UTC Sun Jul 26 2009
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ASW1
!
!
no aaa new-mode1
switch 1 provision ws-c3750-48ts
system mtu routing 1500
vtp mode transparent
ip subnet-zero
no ip domain-lookup
!
```



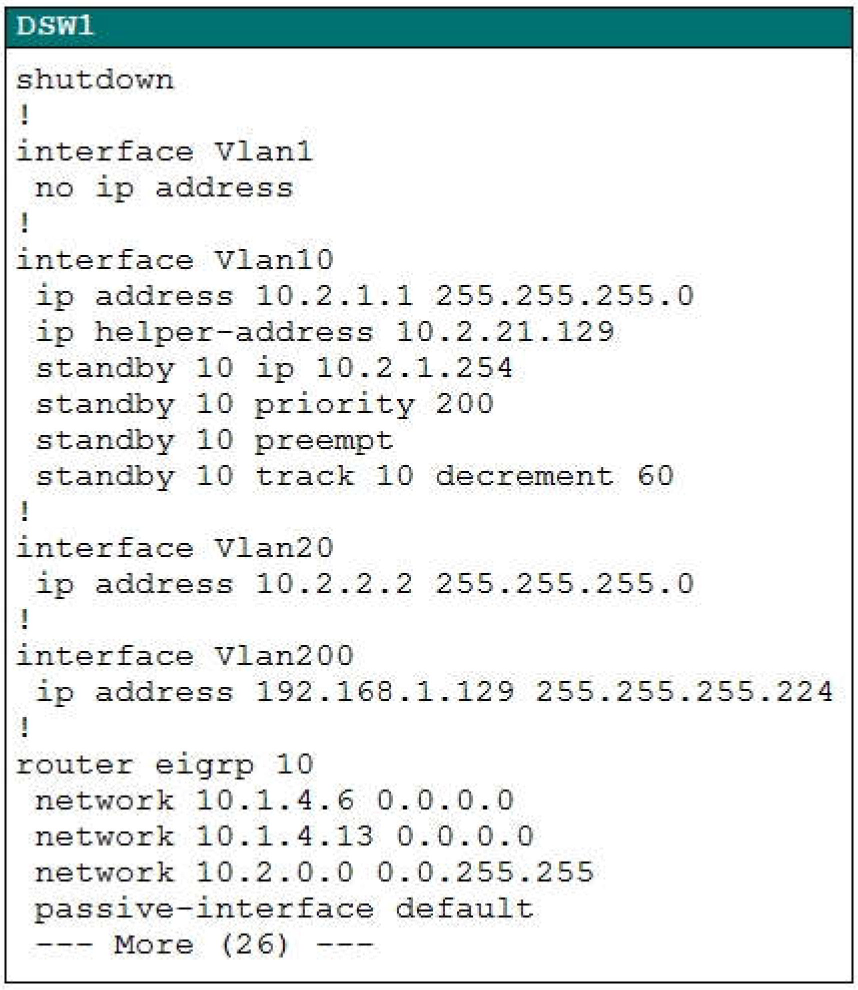
```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,200
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel23
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,200
!
interface FastEthernet1/0/1
 description link to Client 1
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description link to Client 2
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
!
interface FastEthernet1/0/3
no cdp enable
!
interface FastEthernet1/0/4
```



```
R4>
R4>EN
R4>enable
R4#SHOW IP INTER
R4#SHOW IP interface BR
R4#SHOW IP interface brief
Interface          IP-Address     OK? Method Status                  Protocol
FastEthernet0/0    10.1.4.5       YES manual up                        up
FastEthernet0/1    10.1.4.9       YES manual up                        up
Serial0/0/0        unassigned     YES unset up                         up
Serial0/0/0.34     10.1.1.10      YES manual up                        up
Serial0/0/1        unassigned     YES unset administratively down      down
Loopback0          10.1.10.4      YES manual up                        up
Loopback1          10.1.21.129    YES manual up                        up
Tunnel34           unassigned     YES unset up                         up
R4#
```



```
!
ipv6 router ospf 6
 log-adjacency-changes
 redistribute rip RIP_ZONE include-connected
!
ipv6 router rip RIP_ZONE
 redistribute ospf 6 metric 2 include-connected
!
!
route-map EIGPR->OSPF deny 10
 match tag 110
!
route-map EIGPR->OSPF permit 20
 set tag 90
!
route-map EIGPR->OSPF deny 10
 match tag 90
!
route-map EIGPR->OSPF deny 20
 set tag 110
!
!
!
!
control-plane
```



```
DSW1
shutdown
!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 10.2.21.129
 standby 10 ip 10.2.1.254
 standby 10 priority 200
 standby 10 preempt
 standby 10 track 10 decrement 60
!
interface Vlan20
 ip address 10.2.2.2 255.255.255.0
!
interface Vlan200
 ip address 192.168.1.129 255.255.255.224
!
router eigrp 10
 network 10.1.4.6 0.0.0.0
 network 10.1.4.13 0.0.0.0
 network 10.2.0.0 0.0.255.255
 passive-interface default
 --- More (26) ---
```

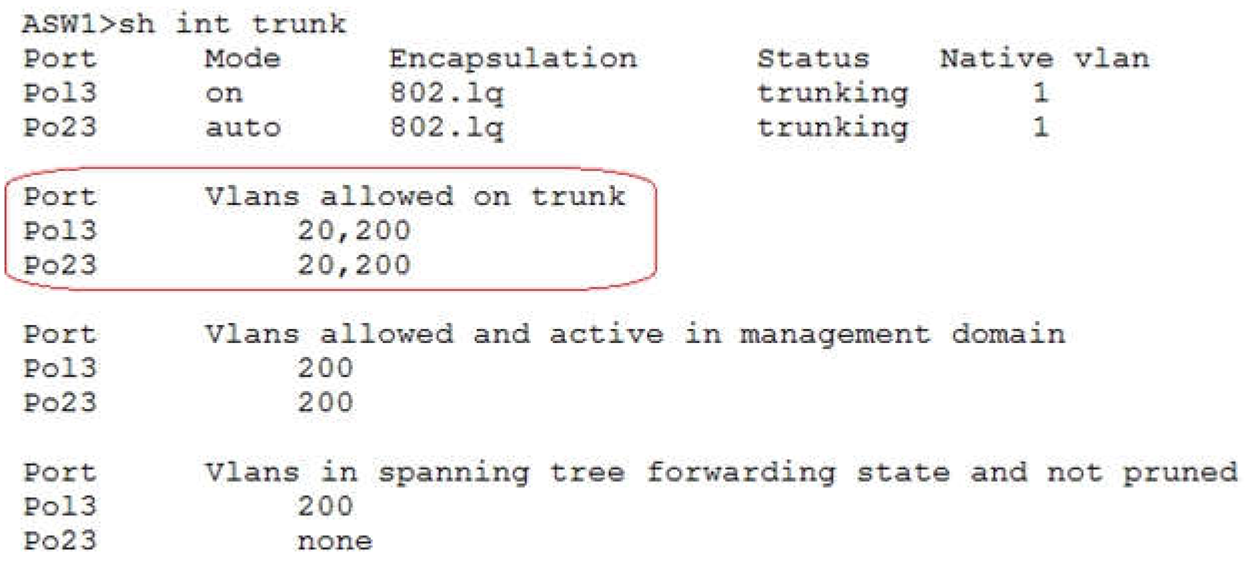
Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
Ipconfig ----- Client will be getting 169.X.X.X

2. On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24

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

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

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

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



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

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

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

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

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

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

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

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

On which device is the fault condition located?

A. R1
B. R2

C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Correct Answer: G
Section: [none]
Explanation

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

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

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

The fault condition is related to which technology?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, and FHRP services, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

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

Correct Answer: B
Section: [none]
Explanation

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

Testlet 1

Instructions

The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

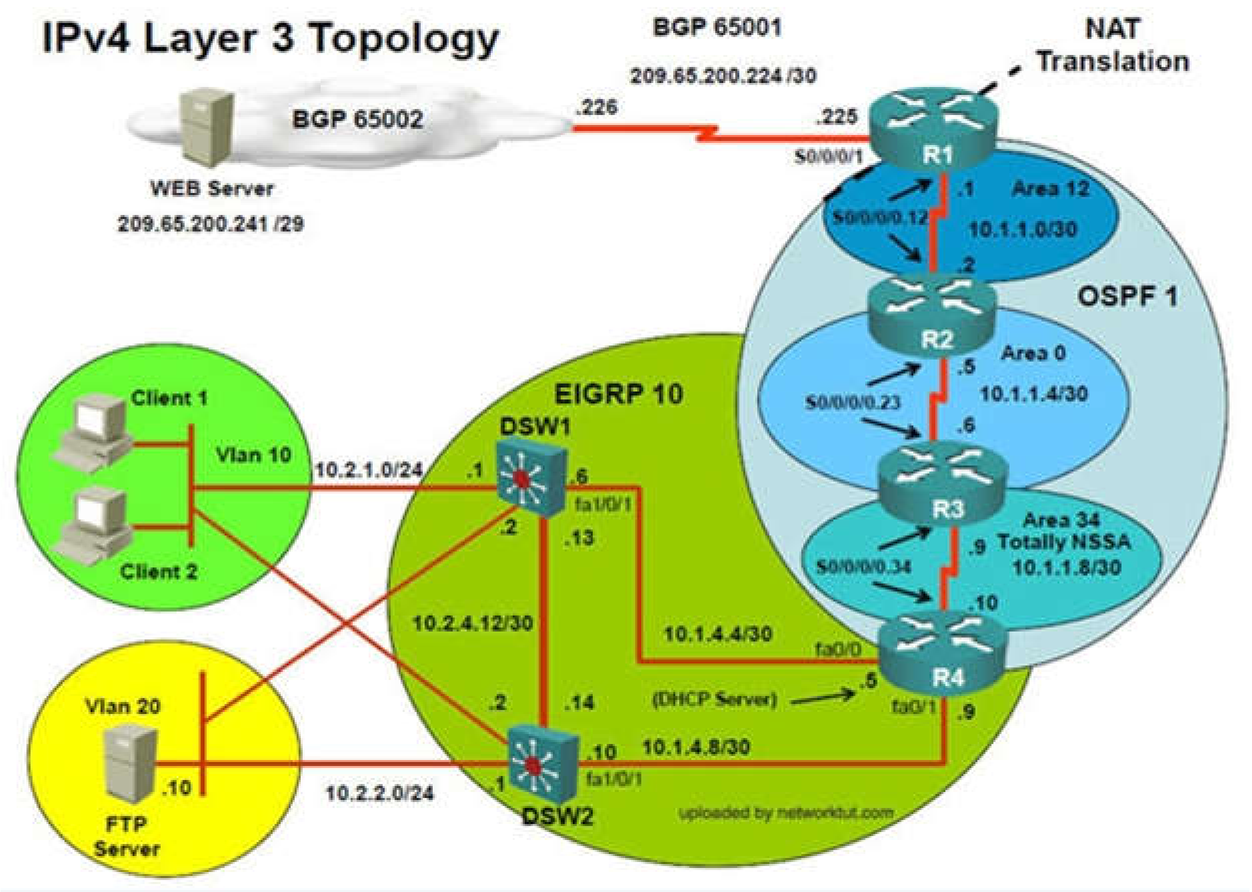
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

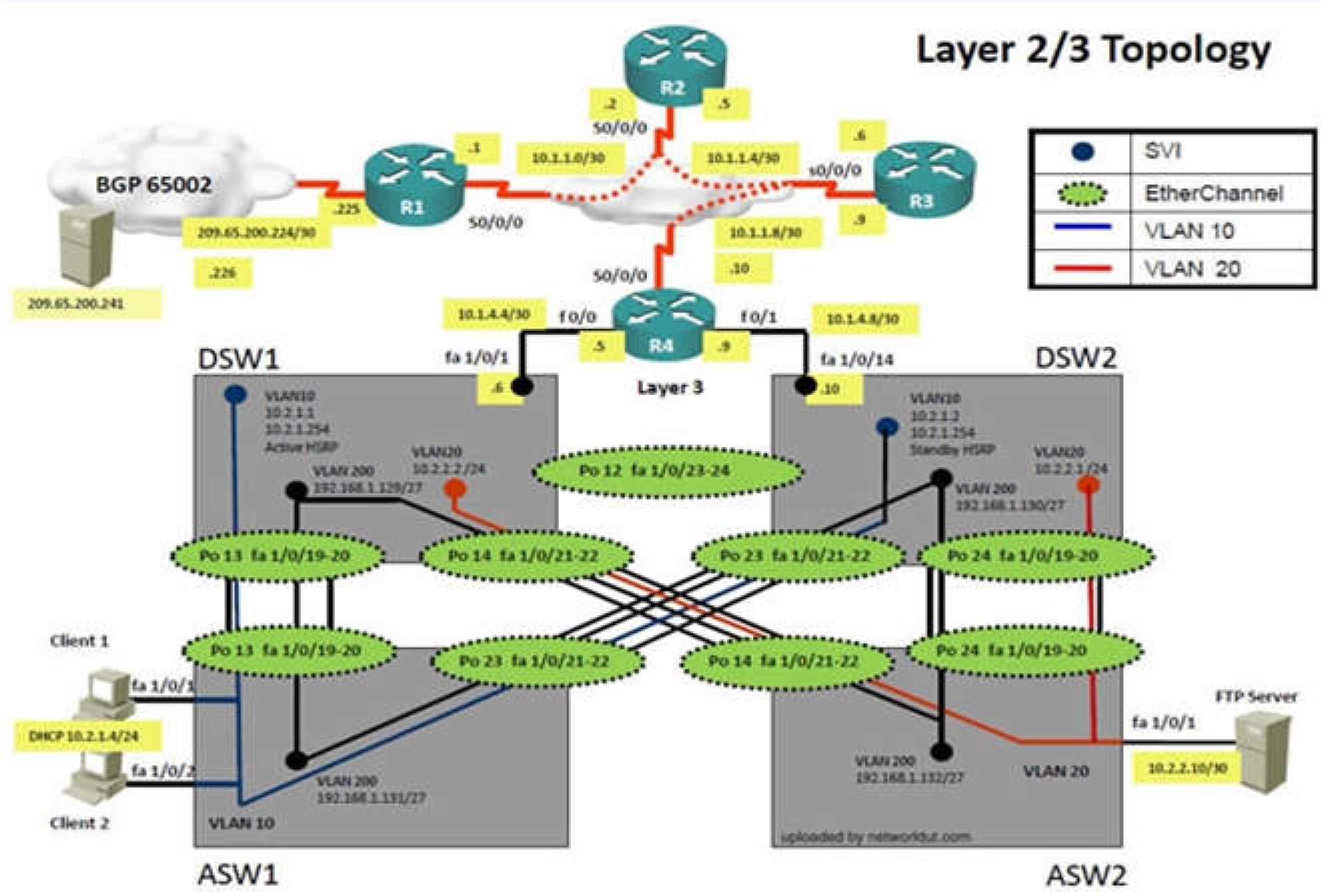
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

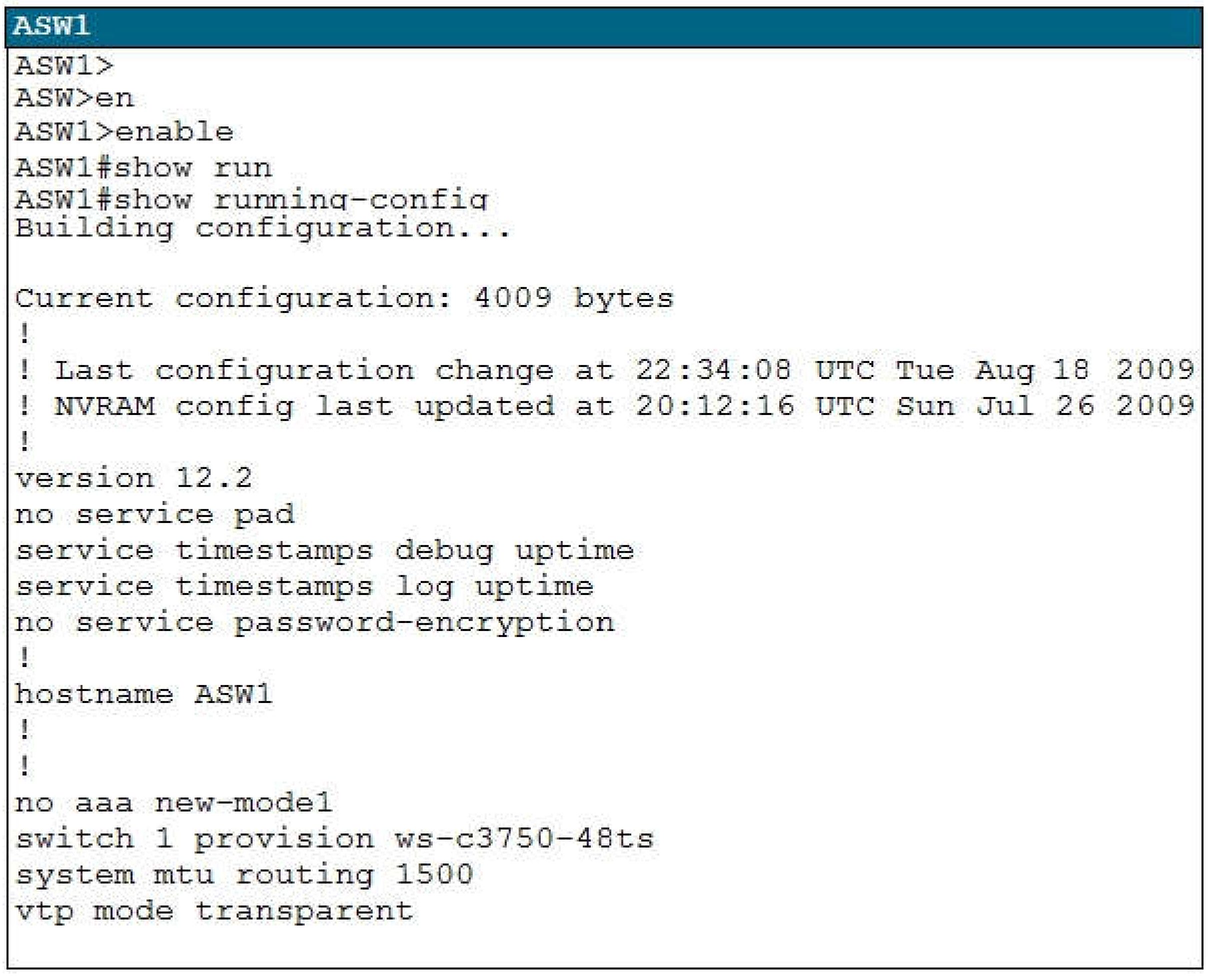
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

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

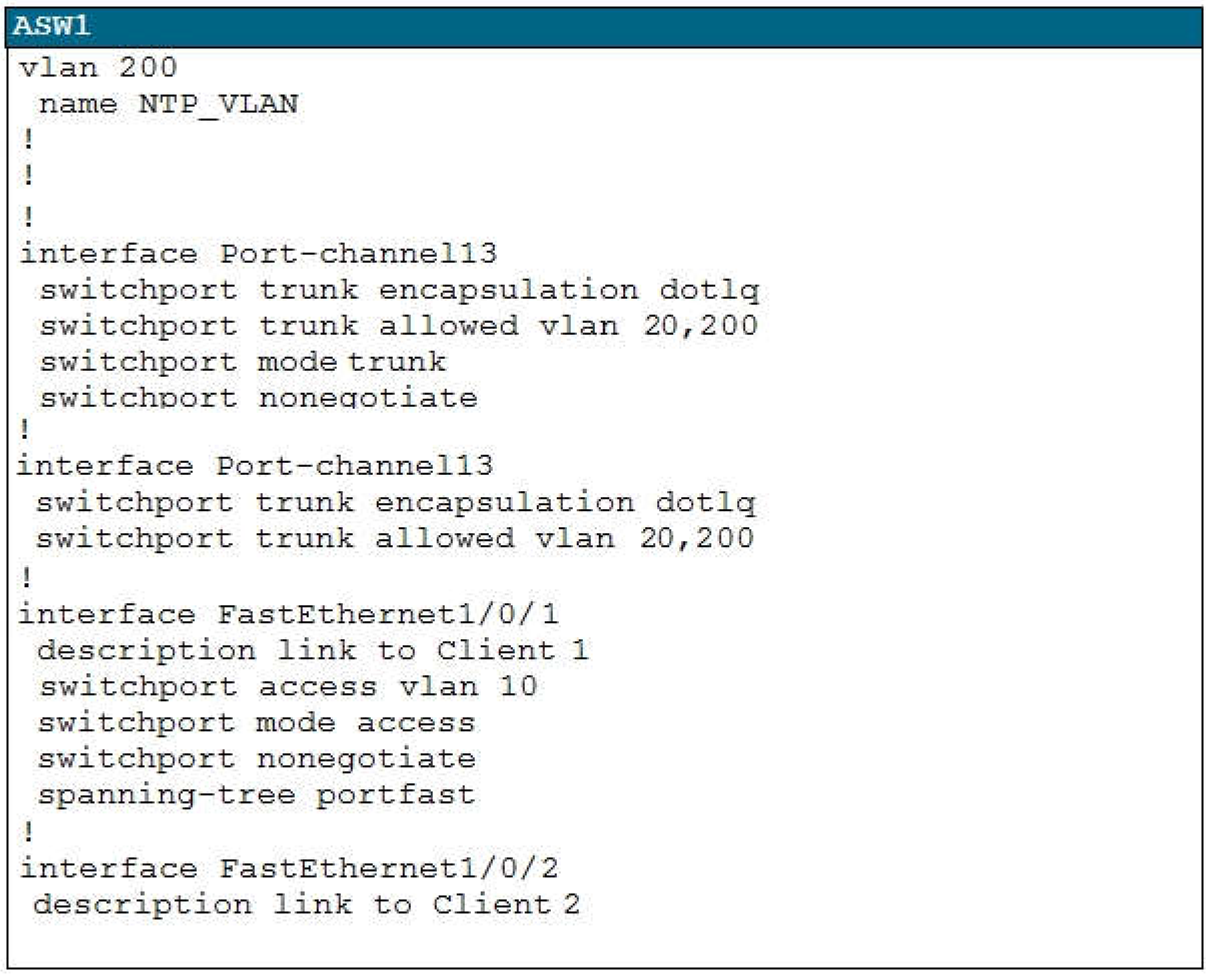
Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution


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

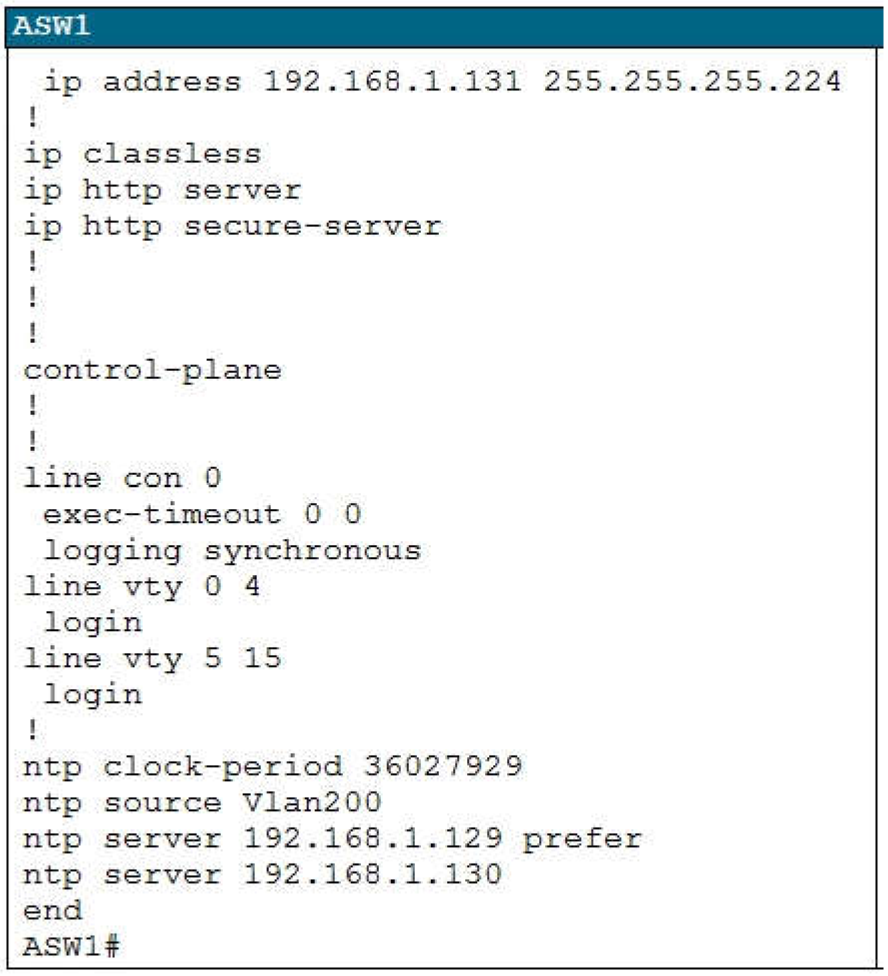

Layer 2/3 Topology
R2
.2
.5
S0/0/0
BGP 65002
.1
10.1.1.0/30
10.1.1.4/30
S0/0/0
.6
R3
R1
.225
S0/0/0
209.65.200.224/30
.226
10.1.1.8/30
.9
209.65.200.241
S0/0/0
.10
SVI
EtherChannel
VLAN 10
VLAN 20
10.1.4.4/30
f0/0
R4
f0/1
10.1.4.8/30
.5
.9
Layer 3
DSW1
fa 1/0/1
.6
fa 1/0/14
.10
DSW2
VLAN10
10.2.1.1
10.2.1.254
Active HSRP
VLAN20
10.2.2.2 /24
VLAN 200
192.168.1.129/27
Po 12 fa 1/0/23-24
VLAN10
10.2.1.2
10.2.1.254
Standby HSRP
VLAN 200
192.168.1.130/27
VLAN20
10.2.2.1 /24
Po 13 fa 1/0/19-20
Po 14 fa 1/0/21-22
Po 23 fa 1/0/21-22
Po 24 fa 1/0/19-20
Client 1
Po 13 fa 1/0/19-20
Po 23 fa 1/0/21-22
Po 14 fa 1/0/21-22
Po 24 fa 1/0/19-20
fa 1/0/1
DHCP 10.2.1.4/24
fa 1/0/2
Client 2
VLAN 200
192.168.1.131/27
VLAN 10
VLAN 200
192.168.1.132/27
VLAN 20
FTP Server
fa 1/0/1
10.2.2.10/30
uploaded by networktut.com
ASW1
ASW2



```
ASW1>
ASW>en
ASW1>enable
ASW1#show run
ASW1#show running-config
Building configuration...

Current configuration: 4009 bytes
!
! Last configuration change at 22:34:08 UTC Tue Aug 18 2009
! NVRAM config last updated at 20:12:16 UTC Sun Jul 26 2009
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ASW1
!
!
no aaa new-model
switch 1 provision ws-c3750-48ts
system mtu routing 1500
vtp mode transparent
```



```
vlan 200
 name NTP_VLAN
!
!
!
interface Port-channel13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,200
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,200
!
interface FastEthernet1/0/1
 description link to Client 1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description link to Client 2
```



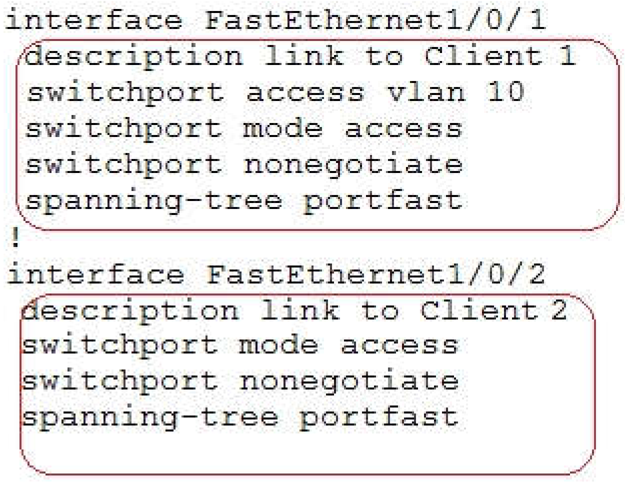
```
ASW1
 ip address 192.168.1.131 255.255.255.224
!
ip classless
ip http server
ip http secure-server
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
!
ntp clock-period 36027929
ntp source Vlan200
ntp server 192.168.1.129 prefer
ntp server 192.168.1.130
end
ASW1#
```

Client is unable to ping IP 209.65.200.241

Solution
Steps need to follow as below:-
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
Ipconfig ----- Client will be getting 169.X.X.X

2. On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24

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



```
interface FastEthernet1/0/1
 description link to Client 1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description link to Client 2
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
```

===

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

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

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

What is the solution to the fault condition?

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

Correct Answer: G
Section: [none]
Explanation

Explanation/Reference:
Explanation:

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

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

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

The fault condition is related to switch technology?

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

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

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

Correct Answer: D
Section: [none]
Explanation

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

Question Set 2

QUESTION 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

Scenario

The company has created the test bed network shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range, R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and the outside (209.65.200.0/24) network.

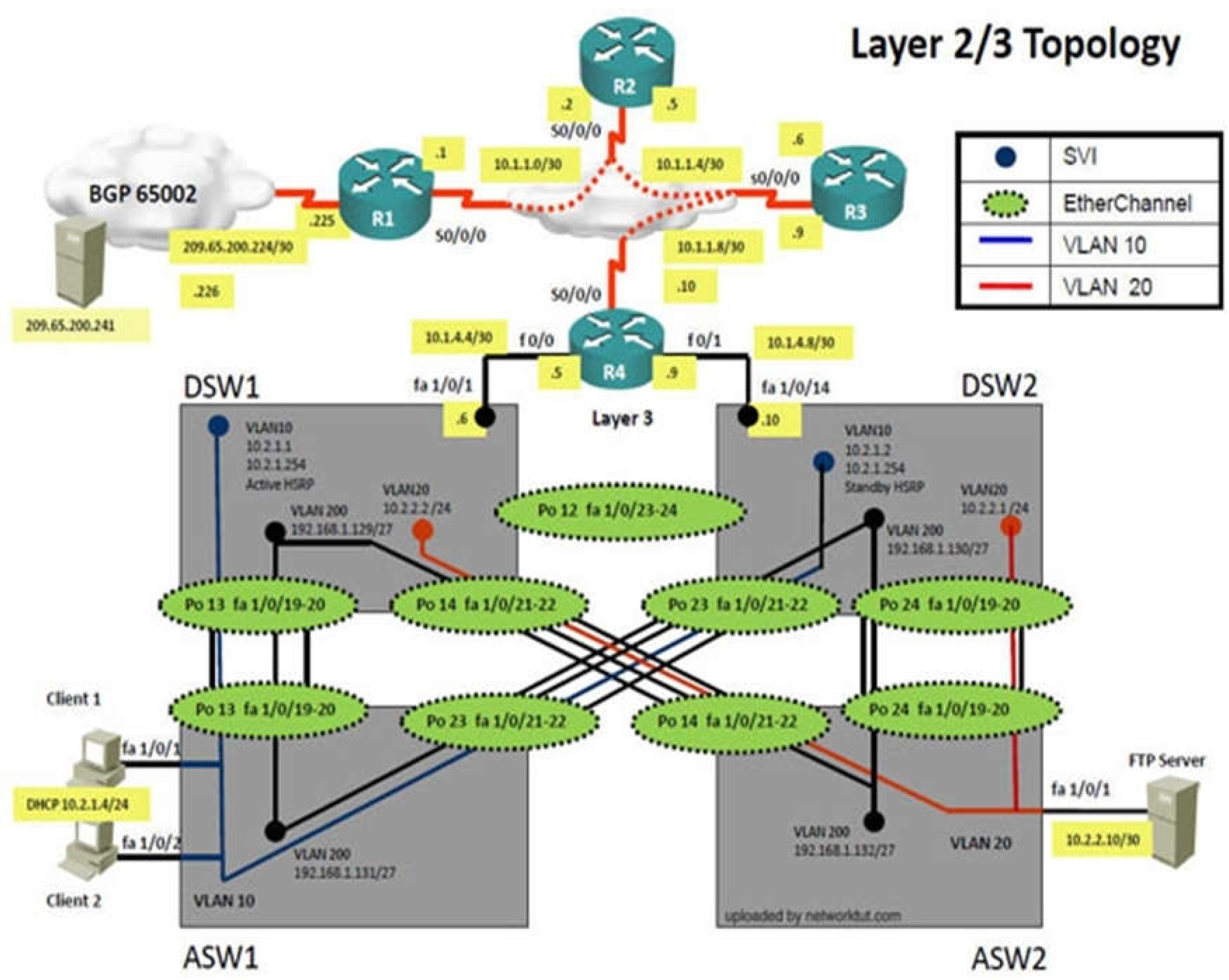
ASW1 and ASW2 are layer 2 switches.

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

The client workstations receive their IP address and default gateway via R4's DHCP server. The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary.

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



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

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

On which device is the fault condition located?

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

Correct Answer: G
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Steps need to follow as below:-1.When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4Ipconfig ----- Client will be getting 169.X.X.X2.On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IPaddress 10.2.1.0/24Sh 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===

3.We need to check on ASW 1 trunk port the trunk Po13 & Po23 were receiving VLAN 20 &200 but not VLAN 10 so that switch could not get DHCP IP address and was failing to reach IPaddress of Internet4.

Change required:
On ASW1 below change is required for switch-to-switch connectivity..int range portchannel13,portchannel23switchport trunk allowed vlan noneswitchport trunk allowed vlan 10,200

QUESTION 2

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.

To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

Scenario

The company has created the test bed network shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range, R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and the outside (209.65.200.0/24) network.

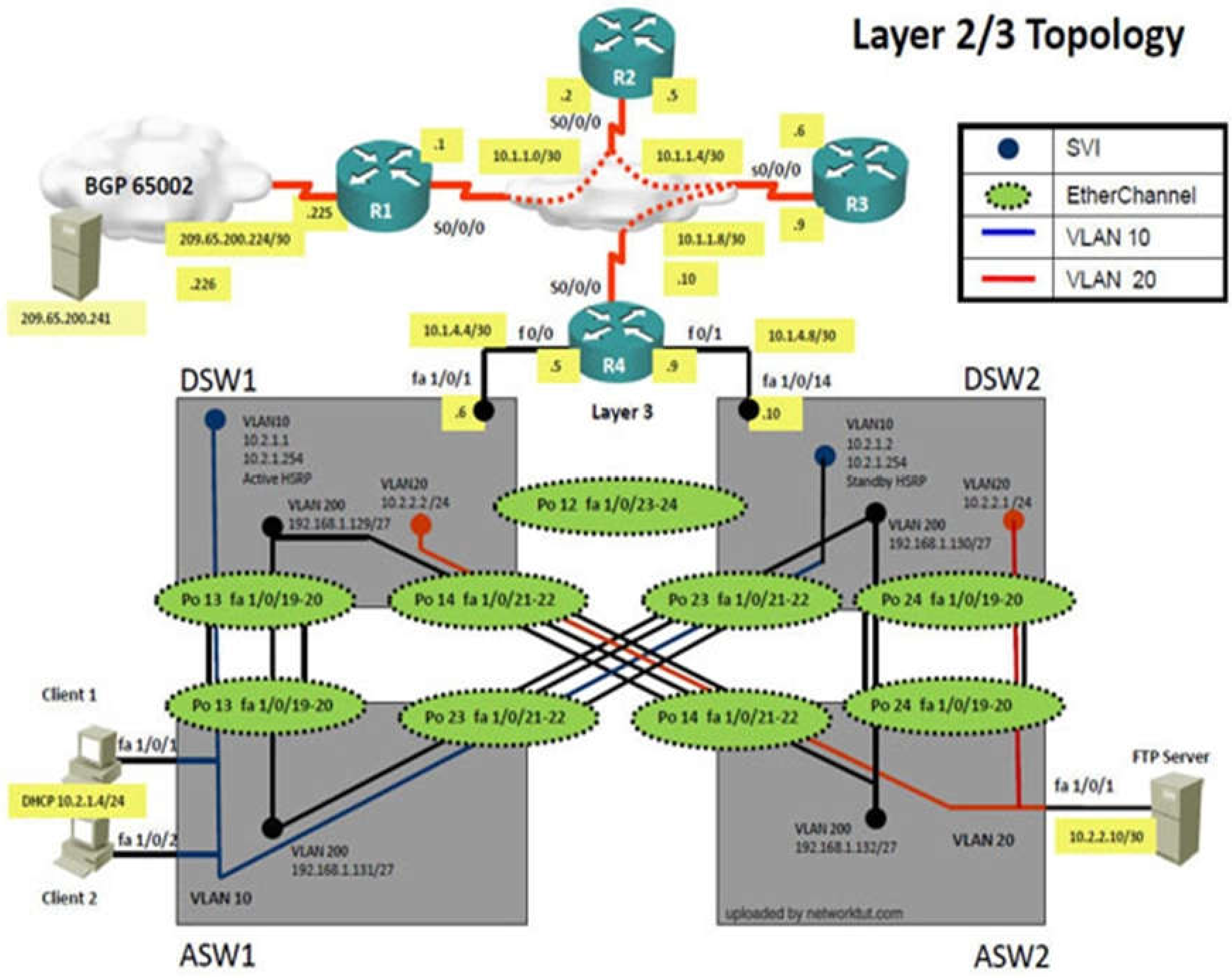
ASW1 and ASW2 are layer 2 switches.

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

The client workstations receive their IP address and default gateway via R4's DHCP server. The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary.

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



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

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

The fault condition is related to which technology?

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

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Steps need to follow as below:-1.When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4Ipconfig ----- Client will be getting 169.X.X.X2.On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IPaddress 10.2.1.0/24Sh 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==

3.We need to check on ASW 1 trunk port the trunk Po13 & Po23 were receiving VLAN 20 &200 but not VLAN 10 so that switch could not get DHCP IP address and was failing to reach IPaddress of Internet4.

Change required:
On ASW1 below change is required for switch-to-switch connectivity..int range portchannel13,portchannel23switchport trunk allowed vlan noneswitchport trunk allowed vlan 10,200

QUESTION 3

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket

scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

Scenario

The company has created the test bed network shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range, R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and the outside (209.65.200.0/24) network.

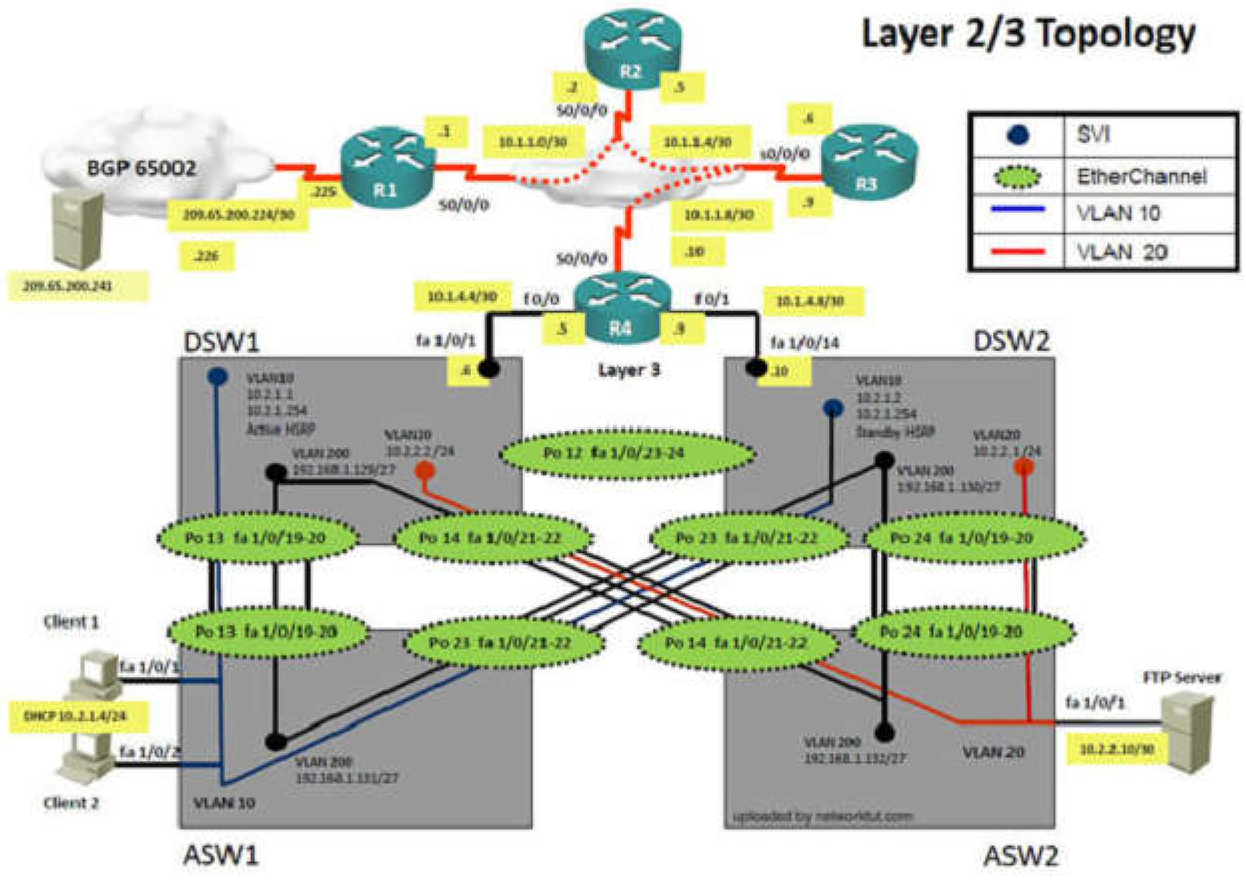
ASW1 and ASW2 are layer 2 switches.

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

The client workstations receive their IP address and default gateway via R4's DHCP server. The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary.

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



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 scheme, DHCP services, NTP services, and FHRP services, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

A. In configuration mode, using the **interface range port-channel 23, port-channel 24**, then configure **switchport trunk allowed vlan none** followed by **switchport trunk allowed vlan 10,20,200** commands.

B. In configuration mode, using the **interface range port-channel 13, port-channel 23,** then configure **switchport trunk allowed vlan none** followed by **switchport trunk allowed vlan 10,200** commands.

C. In configuration mode, using the **interface range port-channel 23, port-channel 24,** then configure **switchport trunk allowed vlan none** followed by **switchport trunk allowed vlan 10,20,** commands.

D. In configuration mode, using the **interface range port-channel 13, port-channel 23,** then configure **switchport trunk allowed vlan 10,200** followed by **interface Fastethernet 1/0/1,** then **no shutdown** commands.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Solution
Steps need to follow as below:-1.When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4Ipconfig ----- Client will be getting 169.X.X.X2.On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IPaddress 10.2.1.0/24Sh 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==

3.We need to check on ASW 1 trunk port the trunk Po13 & Po23 were receiving VLAN 20 &200 but not VLAN 10 so that switch could not get DHCP IP address and was failing to reach IPaddress of Internet4.

Change required:
On ASW1 below change is required for switch-to-switch connectivity..int range portchannel13,portchannel23switchport trunk allowed vlan noneswitchport trunk allowed vlan 10,200

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

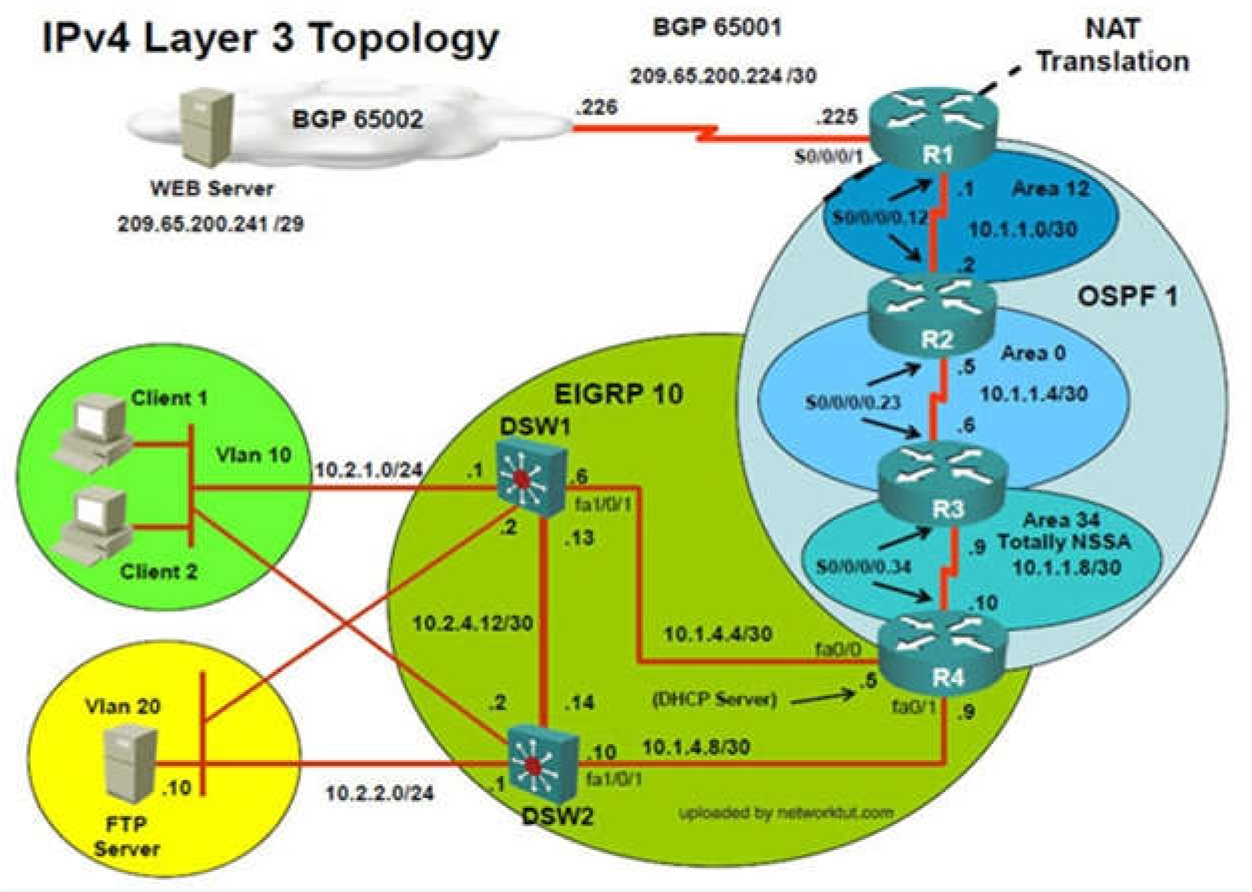
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary.

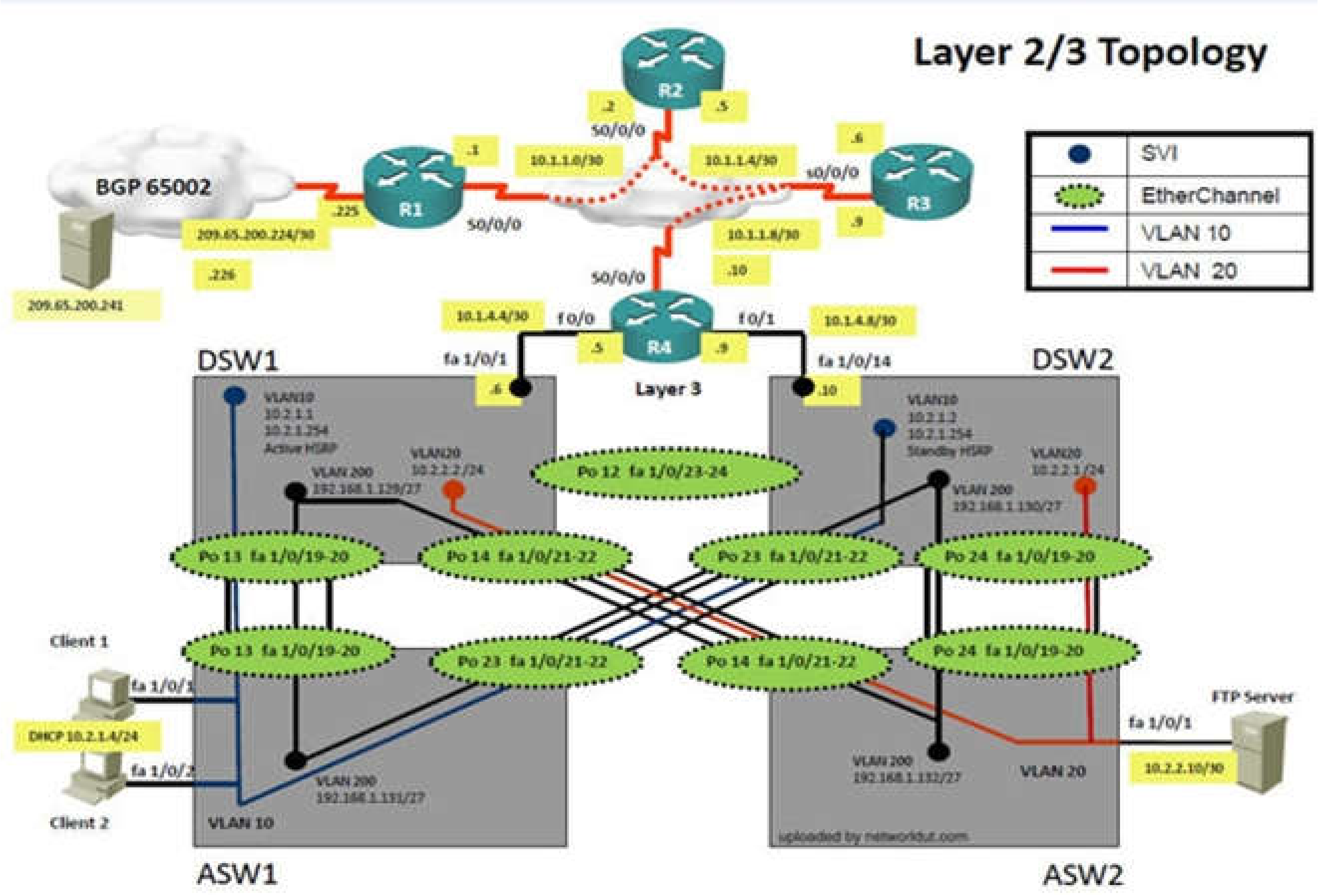
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

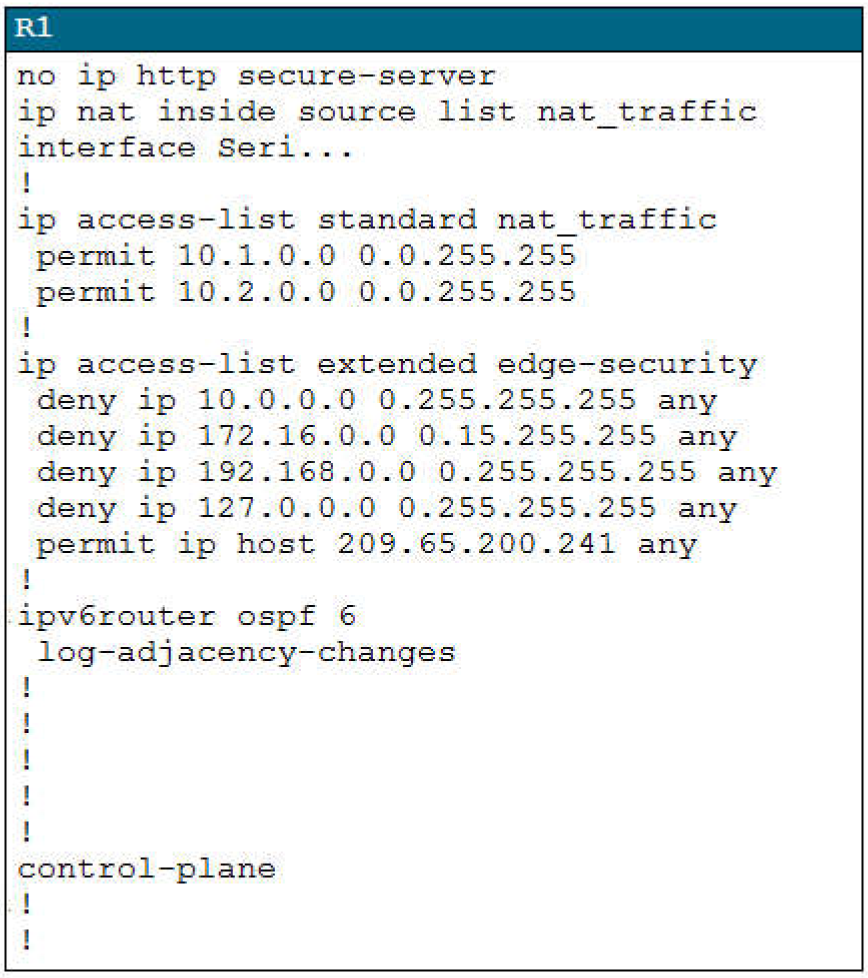
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution

==

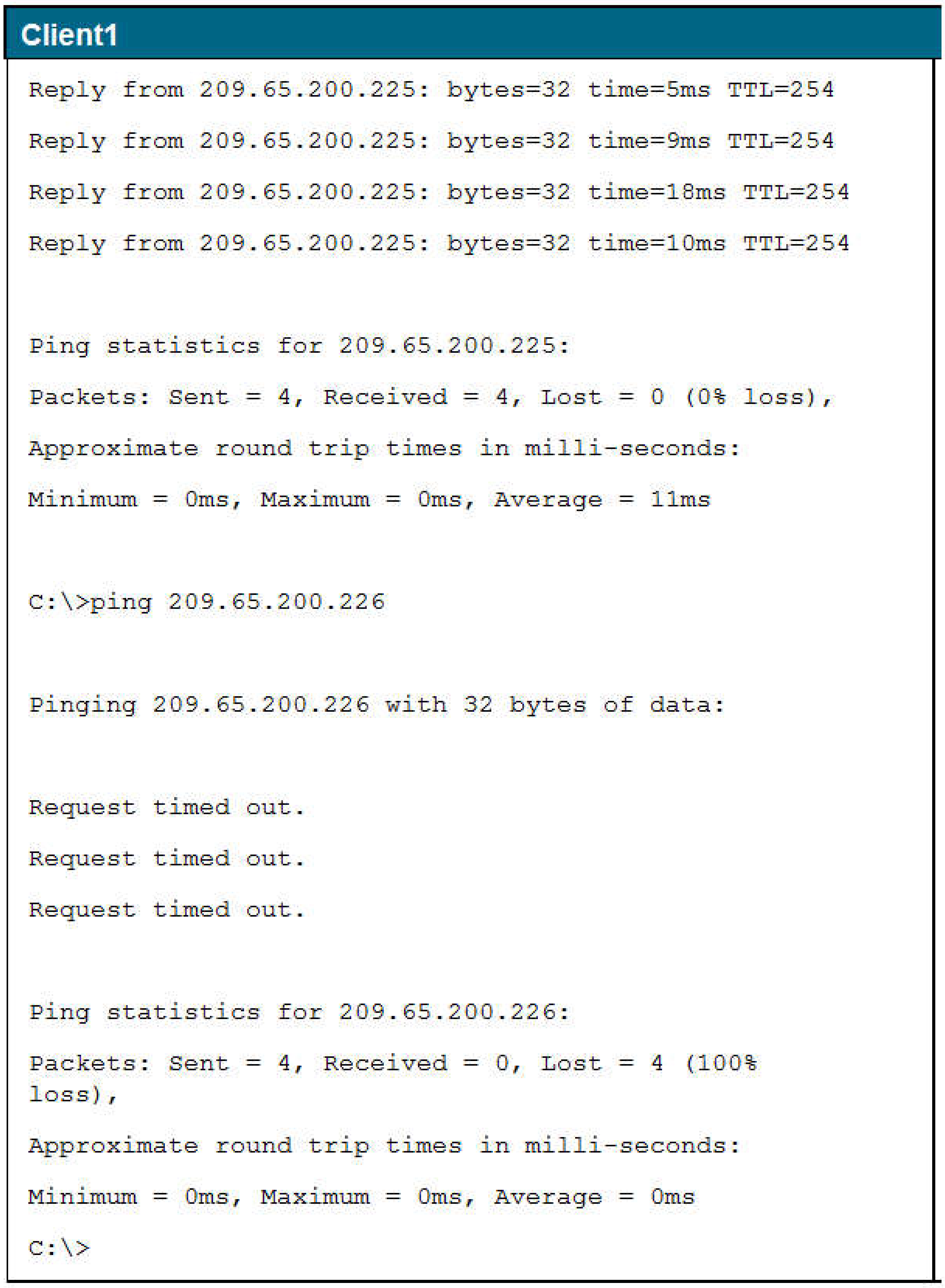

IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT
Translation
BGP 65002
WEB Server
209.65.200.241 /29
.226
.225
S0/0/0/1
R1
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
R2
OSPF 1
Area 0
.5
S0/0/0/0.23
10.1.1.4/30
.6
R3
Area 34
Totally NSSA
S0/0/0/0.34
.9
10.1.1.8/30
.10
R4
fa0/0
.5
(DHCP Server)
fa0/1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


Layer 2/3 Topology
R2
.2
.5
S0/0/0
BGP 65002
.1
R1
10.1.1.0/30
10.1.1.4/30
.6
s0/0/0
R3
.225
S0/0/0
10.1.1.8/30
.9
209.65.200.224/30
.226
209.65.200.241
S0/0/0
.10
10.1.4.4/30
f 0/0
R4
f 0/1
10.1.4.8/30
.5
.9
DSW1
fa 1/0/1
.6
Layer 3
fa 1/0/14
.10
DSW2
VLAN10
10.2.1.1
10.2.1.254
Active HSRP
VLAN20
10.2.2.2 /24
VLAN 200
192.168.1.129/27
Po 12 fa 1/0/23-24
VLAN10
10.2.1.2
10.2.1.254
Standby HSRP
VLAN20
10.2.2.1 /24
VLAN 200
192.168.1.130/27
Po 13 fa 1/0/19-20
Po 14 fa 1/0/21-22
Po 23 fa 1/0/21-22
Po 24 fa 1/0/19-20
Client 1
Po 13 fa 1/0/19-20
Po 23 fa 1/0/21-22
Po 14 fa 1/0/21-22
Po 24 fa 1/0/19-20
fa 1/0/1
DHCP 10.2.1.4/24
fa 1/0/2
Client 2
VLAN 200
192.168.1.131/27
VLAN 10
VLAN 200
192.168.1.132/27
VLAN 20
FTP Server
fa 1/0/1
10.2.2.10/30
uploaded by networktut.com
ASW1
ASW2
SVI
EtherChannel
VLAN 10
VLAN 20



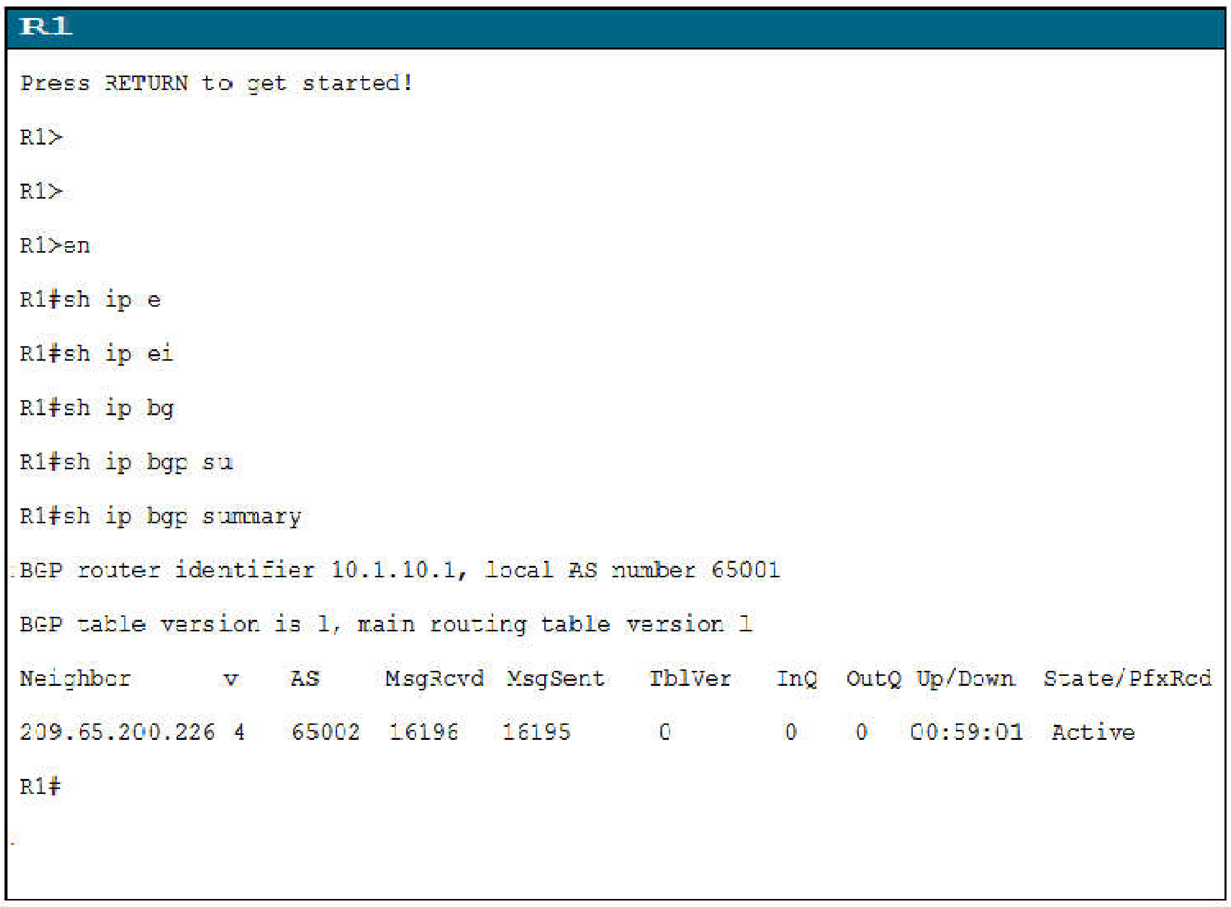
R1

```
no ip http secure-server
ip nat inside source list nat_traffic
interface Seri...
!
ip access-list standard nat_traffic
 permit 10.1.0.0 0.0.255.255
 permit 10.2.0.0 0.0.255.255
!
ip access-list extended edge-security
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.255.255.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 permit ip host 209.65.200.241 any
!
ipv6router ospf 6
 log-adjacency-changes
!
!
!
!
!
control-plane
!
!
```



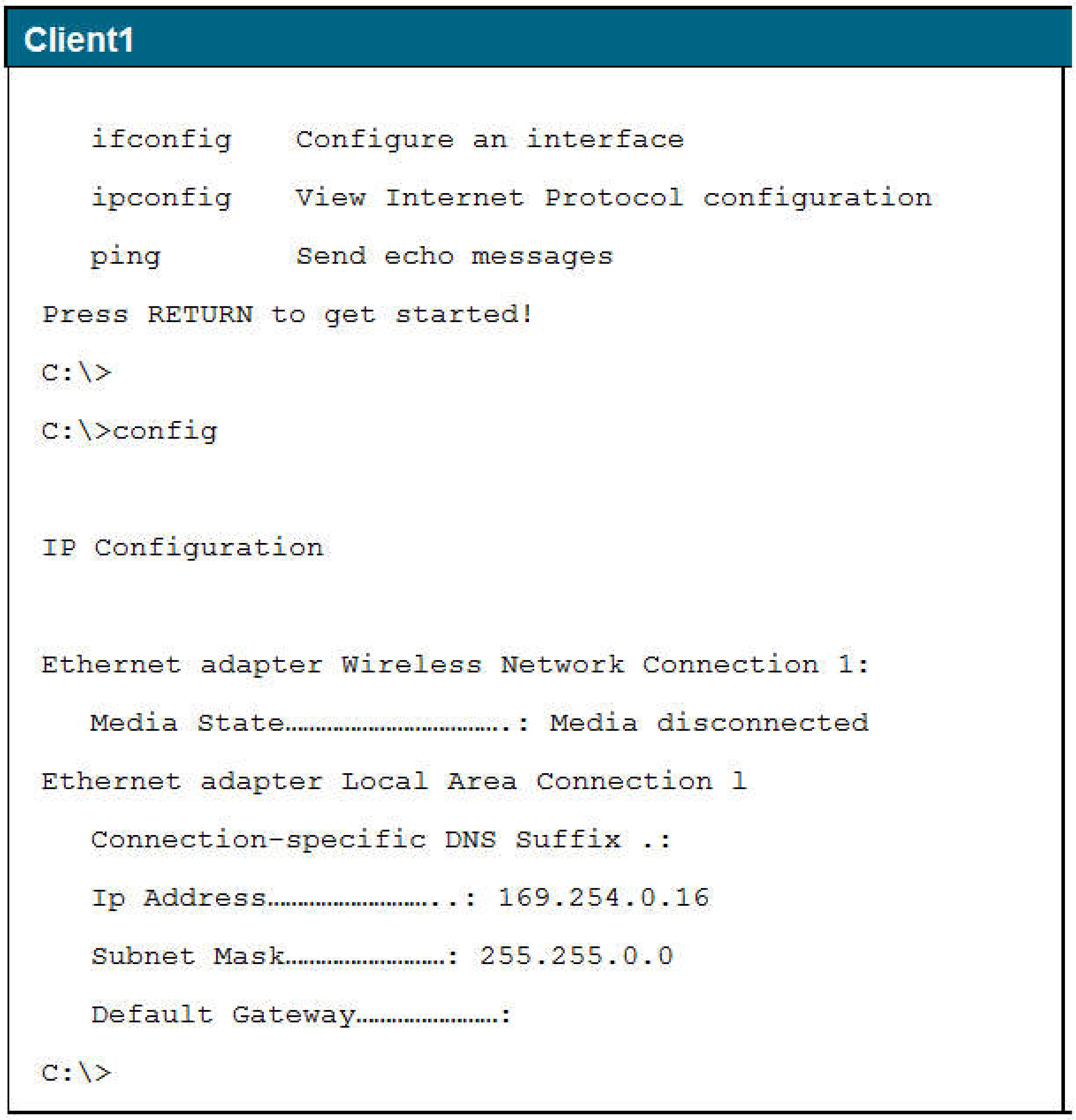
Client1

```
Reply from 209.65.200.225: bytes=32 time=5ms TTL=254

Reply from 209.65.200.225: bytes=32 time=9ms TTL=254

Reply from 209.65.200.225: bytes=32 time=18ms TTL=254

Reply from 209.65.200.225: bytes=32 time=10ms TTL=254


Ping statistics for 209.65.200.225:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 11ms


C:\>ping 209.65.200.226


Pinging 209.65.200.226 with 32 bytes of data:


Request timed out.

Request timed out.

Request timed out.


Ping statistics for 209.65.200.226:

Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



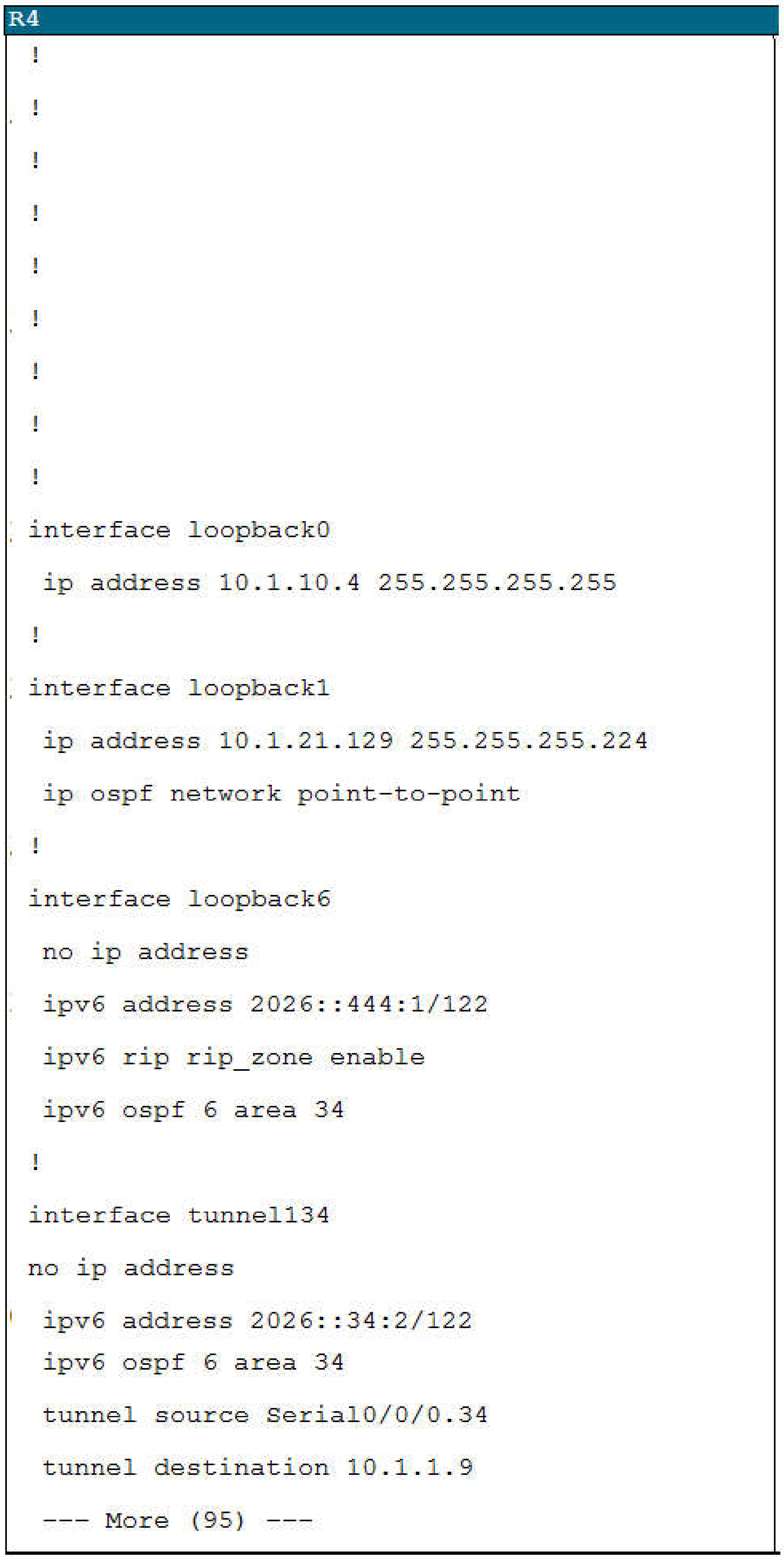
R1

```
Press RETURN to get started!
R1>
R1>
R1>en
R1#sh ip e
R1#sh ip ei
R1#sh ip bg
R1#sh ip bgp su
R1#sh ip bgp summary
BGP router identifier 10.1.10.1, local AS number 65001
BGP table version is 1, main routing table version 1
Neighbor        V    AS      MsgRcvd  MsgSent   TblVer   InQ  OutQ  Up/Down   State/PfxRcd
209.65.200.226  4    65002   16196    16195     0        0    0     00:59:01  Active
R1#
```



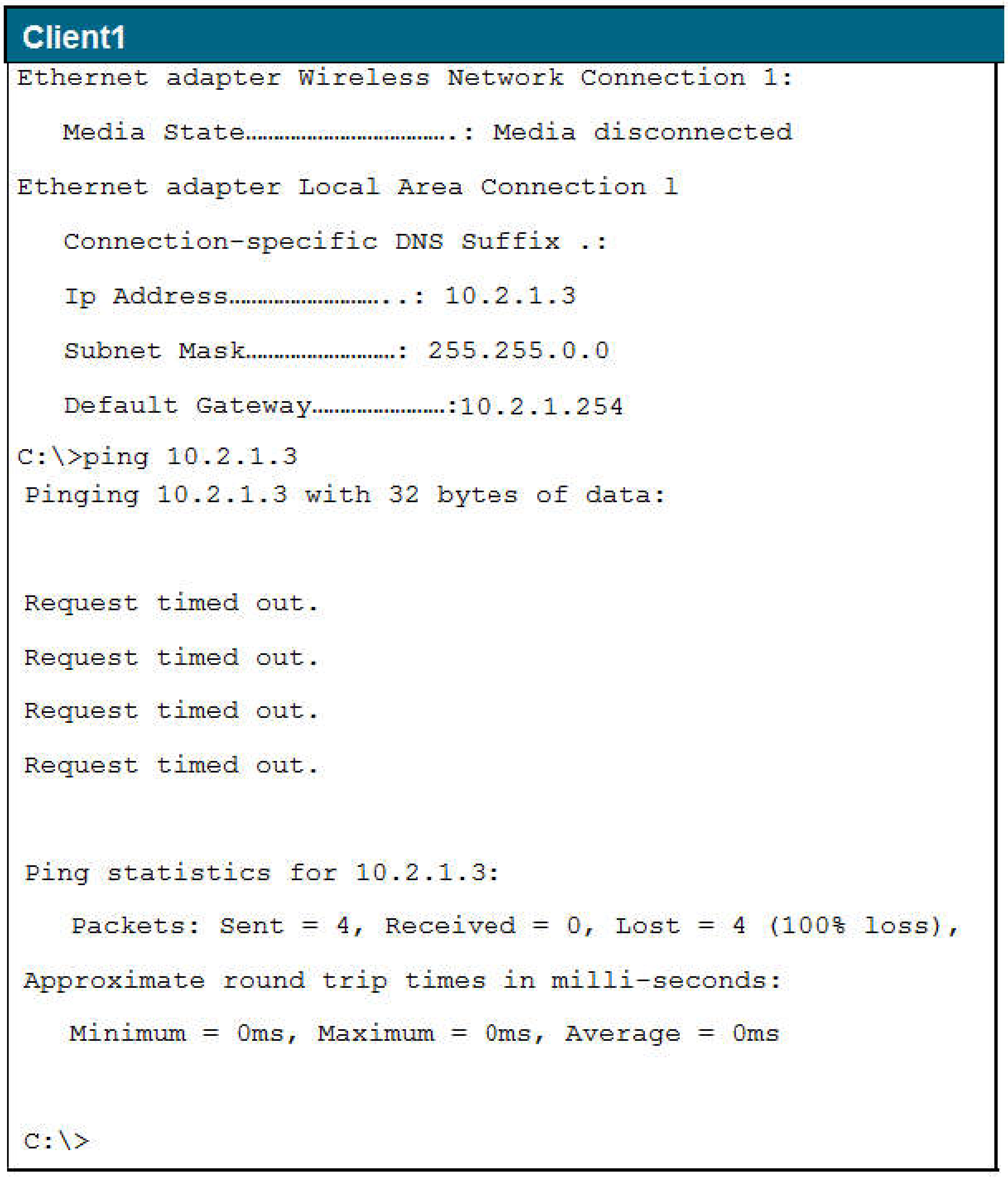
Client1

```
    ifconfig     Configure an interface
    ipconfig     View Internet Protocol configuration
    ping         Send echo messages
 Press RETURN to get started!
 C:\>
 C:\>config


 IP Configuration


 Ethernet adapter Wireless Network Connection 1:
    Media State.................................: Media disconnected
 Ethernet adapter Local Area Connection 1
    Connection-specific DNS Suffix .:
    Ip Address.........................: 169.254.0.16
    Subnet Mask.......................: 255.255.0.0
    Default Gateway.....................:
 C:\>
```



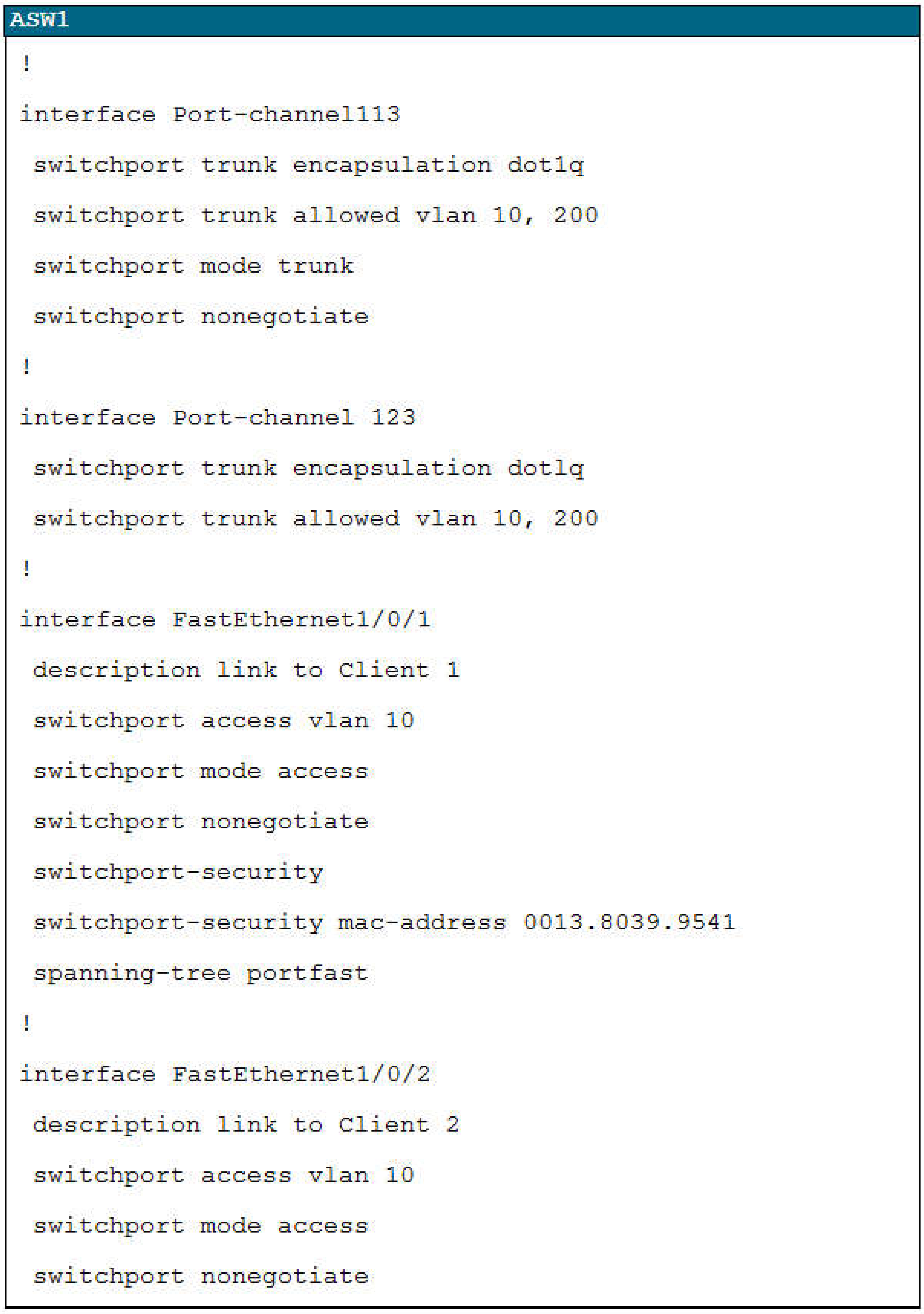
R4

```
!
!
!
!
!
!
!
!
!
interface loopback0
 ip address 10.1.10.4 255.255.255.255
!
interface loopback1
 ip address 10.1.21.129 255.255.255.224
 ip ospf network point-to-point
!
interface loopback6
 no ip address
 ipv6 address 2026::444:1/122
 ipv6 rip rip_zone enable
 ipv6 ospf 6 area 34
!
interface tunnel134
no ip address
 ipv6 address 2026::34:2/122
 ipv6 ospf 6 area 34
 tunnel source Serial0/0/0.34
 tunnel destination 10.1.1.9
 --- More (95) ---
```



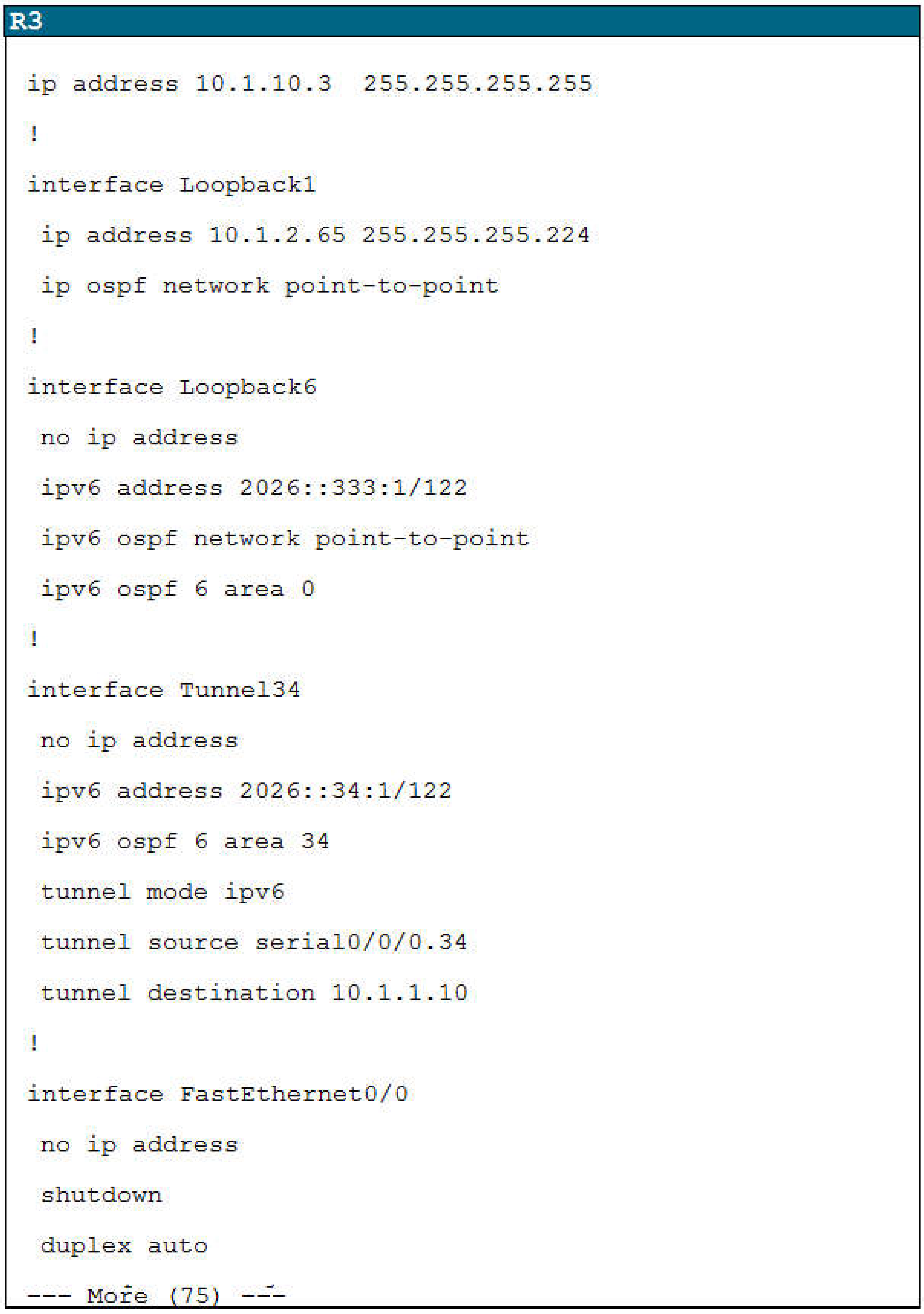
Client1

```
Ethernet adapter Wireless Network Connection 1:

   Media State.................................: Media disconnected

Ethernet adapter Local Area Connection 1

   Connection-specific DNS Suffix .:

   Ip Address........................ . .: 10.2.1.3

   Subnet Mask........................: 255.255.0.0

   Default Gateway......................:10.2.1.254

C:\>ping 10.2.1.3
 Pinging 10.2.1.3 with 32 bytes of data:


 Request timed out.

 Request timed out.

 Request timed out.

 Request timed out.


 Ping statistics for 10.2.1.3:

    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

 Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 0ms, Average = 0ms


 C:\>
```



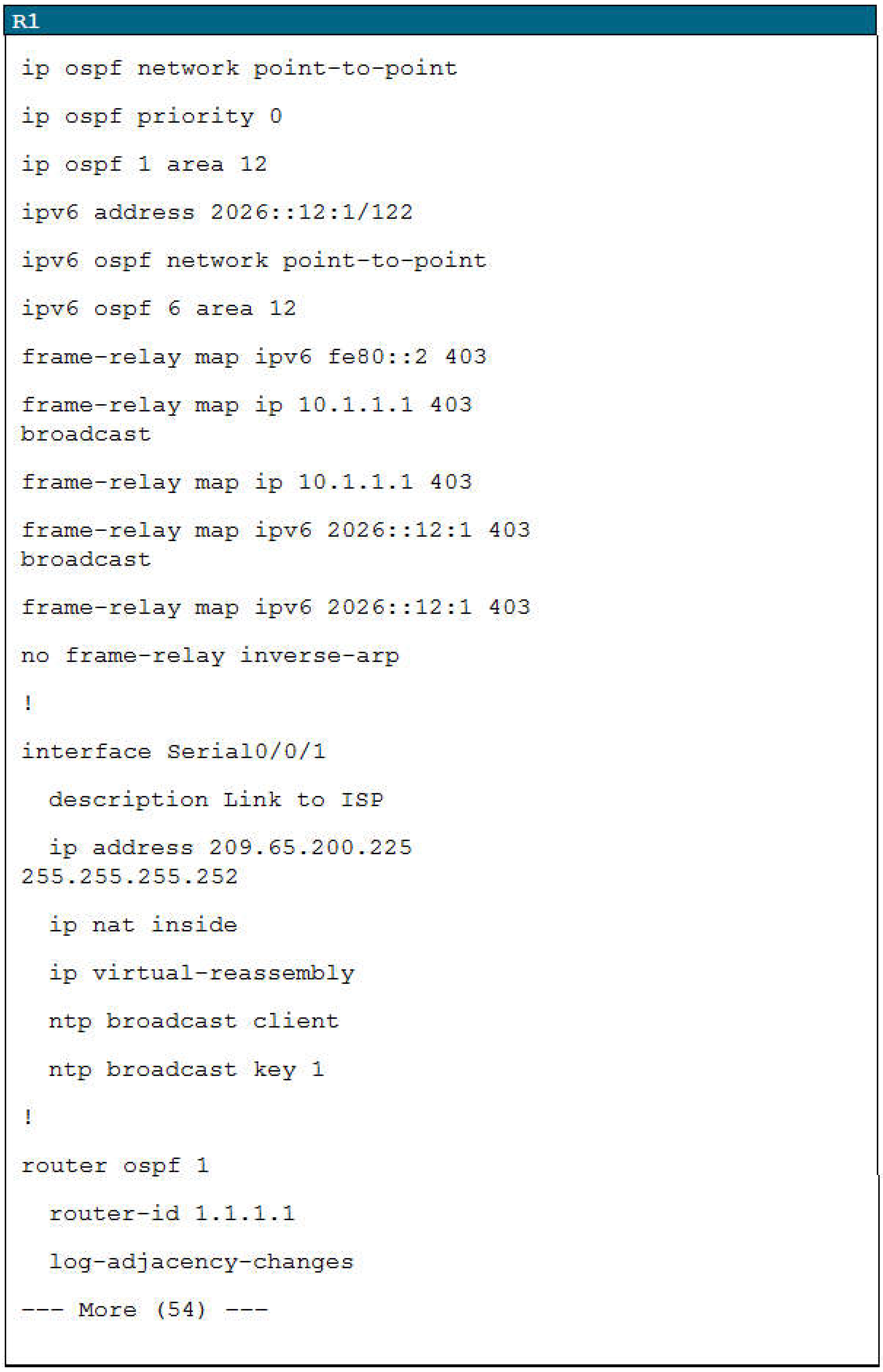
ASW1

```
!
interface Port-channel113
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10, 200
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel 123
 switchport trunk encapsulation dotlq
 switchport trunk allowed vlan 10, 200
!
interface FastEthernet1/0/1
 description link to Client 1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport-security
 switchport-security mac-address 0013.8039.9541
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description link to Client 2
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
```

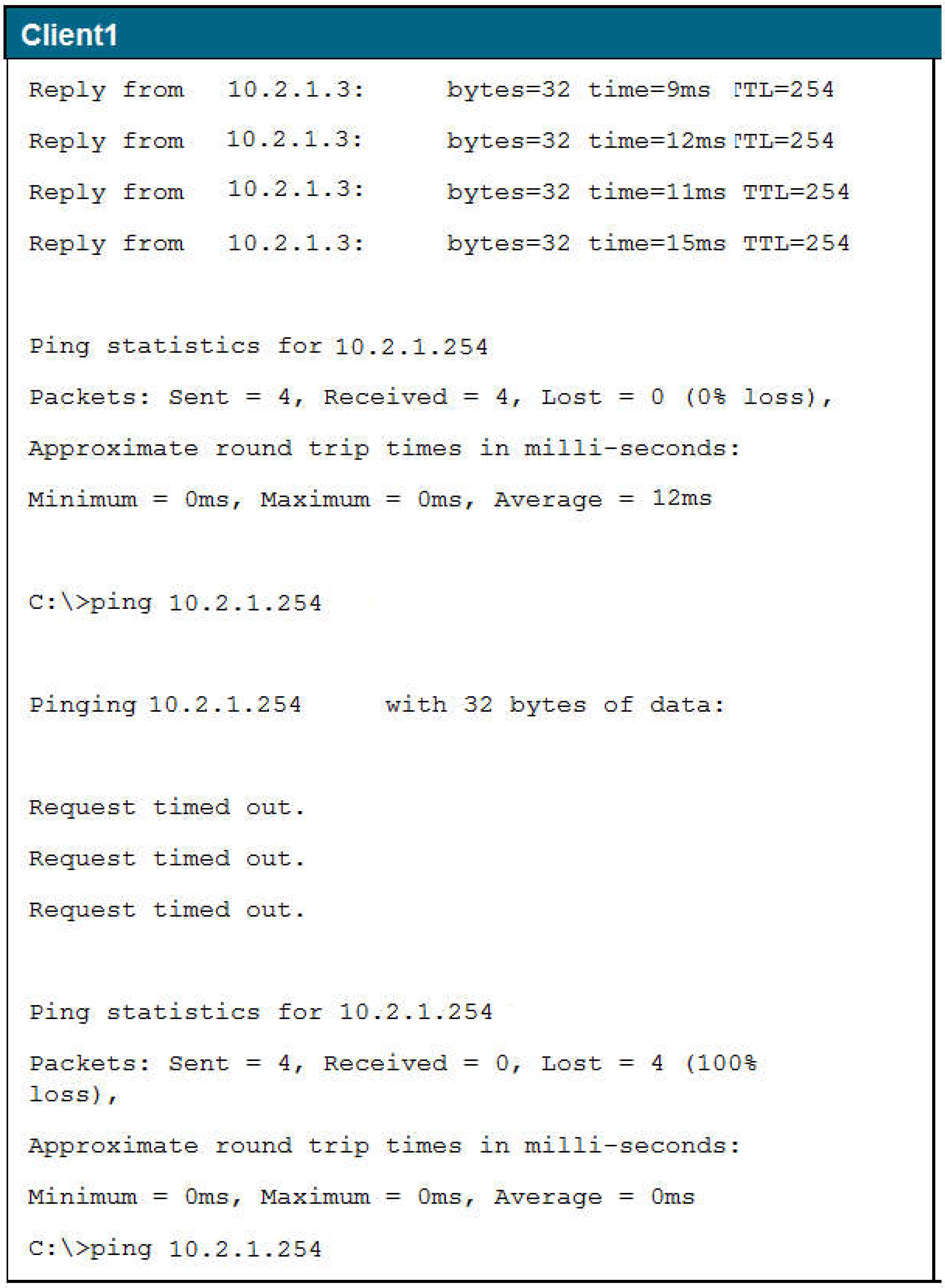


R3

```
ip address 10.1.10.3  255.255.255.255
!
interface Loopback1
 ip address 10.1.2.65 255.255.255.224
 ip ospf network point-to-point
!
interface Loopback6
 no ip address
 ipv6 address 2026::333:1/122
 ipv6 ospf network point-to-point
 ipv6 ospf 6 area 0
!
interface Tunnel34
 no ip address
 ipv6 address 2026::34:1/122
 ipv6 ospf 6 area 34
 tunnel mode ipv6
 tunnel source serial0/0/0.34
 tunnel destination 10.1.1.10
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
--- More (75) ---
```

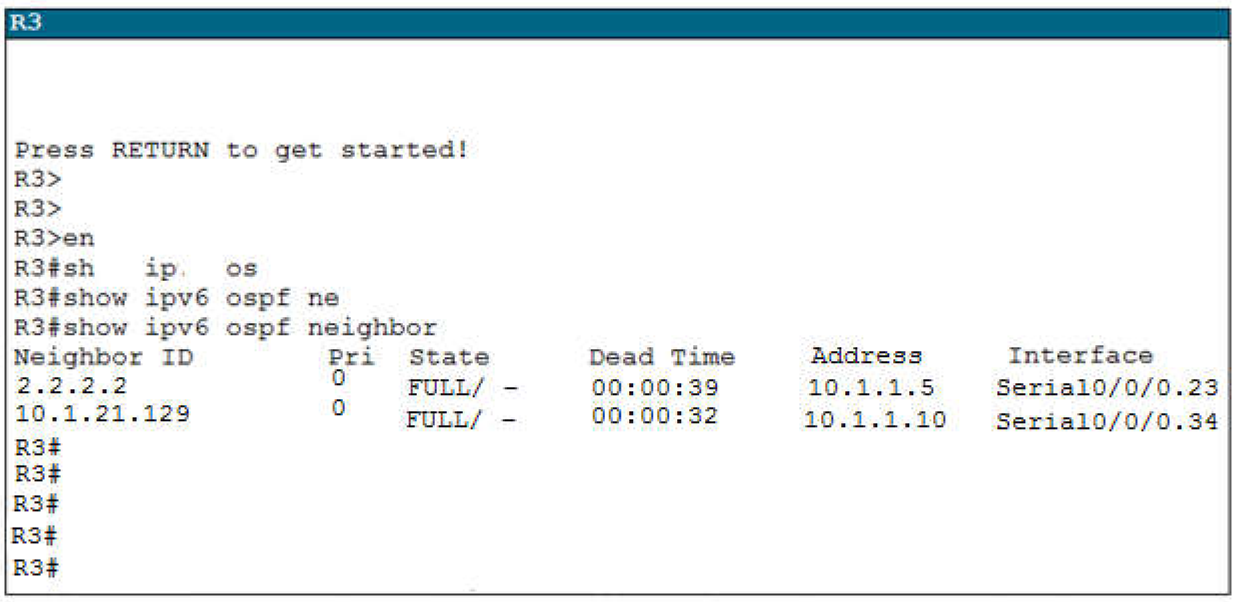


```
ip ospf network point-to-point

ip ospf priority 0

ip ospf 1 area 12

ipv6 address 2026::12:1/122

ipv6 ospf network point-to-point

ipv6 ospf 6 area 12

frame-relay map ipv6 fe80::2 403

frame-relay map ip 10.1.1.1 403
broadcast

frame-relay map ip 10.1.1.1 403

frame-relay map ipv6 2026::12:1 403
broadcast

frame-relay map ipv6 2026::12:1 403

no frame-relay inverse-arp

!

interface Serial0/0/1

  description Link to ISP

  ip address 209.65.200.225
255.255.255.252

  ip nat inside

  ip virtual-reassembly

  ntp broadcast client

  ntp broadcast key 1

!

router ospf 1

  router-id 1.1.1.1

  log-adjacency-changes

--- More (54) ---
```



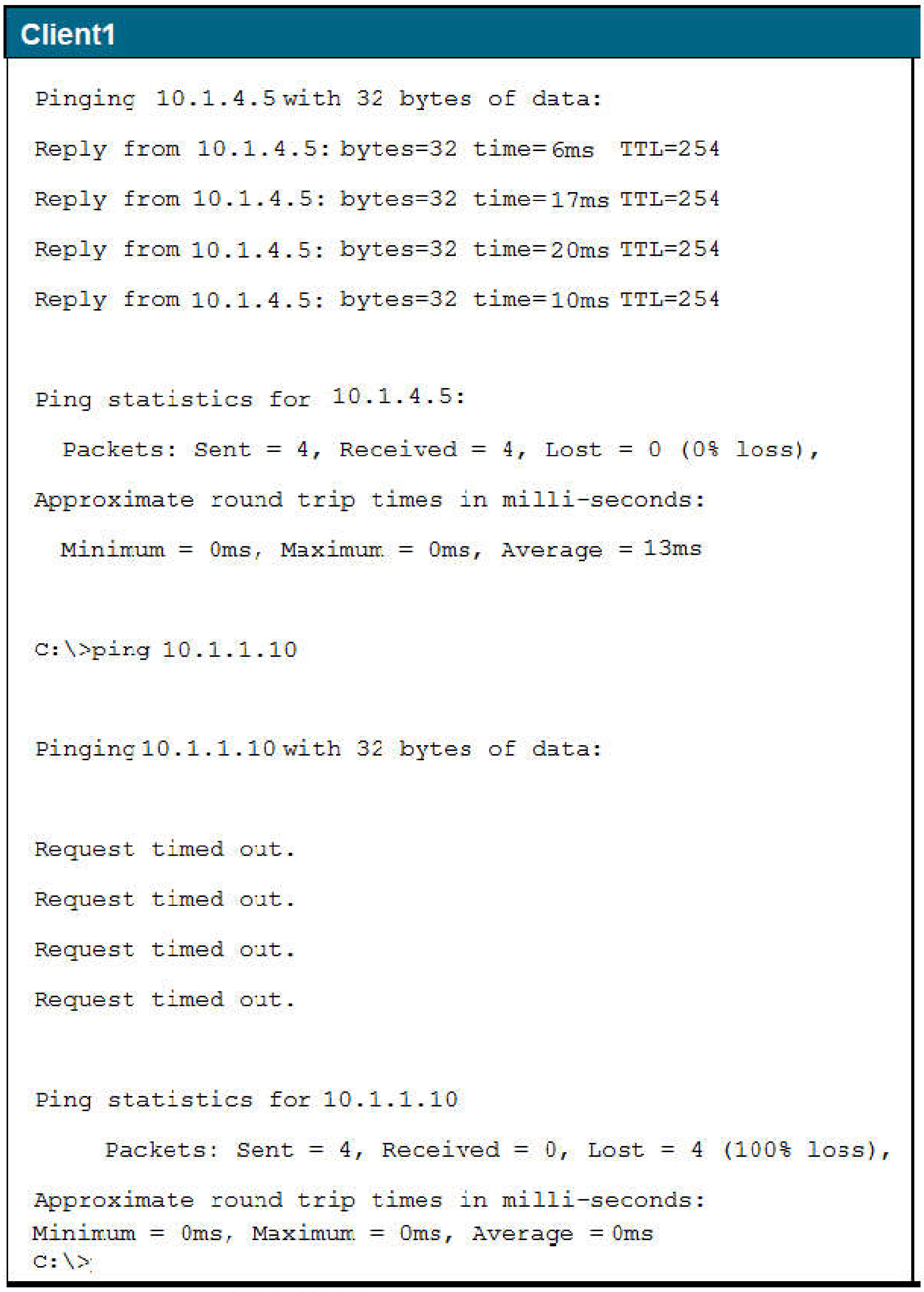
Client1

```
Reply from   10.2.1.3:     bytes=32 time=9ms  TTL=254
Reply from   10.2.1.3:     bytes=32 time=12ms TTL=254
Reply from   10.2.1.3:     bytes=32 time=11ms TTL=254
Reply from   10.2.1.3:     bytes=32 time=15ms TTL=254

Ping statistics for 10.2.1.254
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 12ms

C:\>ping 10.2.1.254

Pinging 10.2.1.254     with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.2.1.254
Packets: Sent = 4, Received = 0, Lost = 4 (100%
loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.2.1.254
```



R3

```
Press RETURN to get started!
R3>
R3>
R3>en
R3#sh   ip   os
R3#show ipv6 ospf ne
R3#show ipv6 ospf neighbor
Neighbor ID          Pri  State       Dead Time     Address       Interface
2.2.2.2               0   FULL/ -     00:00:39     10.1.1.5     Serial0/0/0.23
10.1.21.129           0   FULL/ -     00:00:32     10.1.1.10    Serial0/0/0.34
R3#
R3#
R3#
R3#
R3#
```



```
Pinging 10.1.4.5 with 32 bytes of data:

Reply from 10.1.4.5: bytes=32 time=6ms  TTL=254

Reply from 10.1.4.5: bytes=32 time=17ms TTL=254

Reply from 10.1.4.5: bytes=32 time=20ms TTL=254

Reply from 10.1.4.5: bytes=32 time=10ms TTL=254


Ping statistics for 10.1.4.5:

  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

  Minimum = 0ms, Maximum = 0ms, Average = 13ms


C:\>ping 10.1.1.10


Pinging 10.1.1.10 with 32 bytes of data:


Request timed out.

Request timed out.

Request timed out.

Request timed out.


Ping statistics for 10.1.1.10

     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

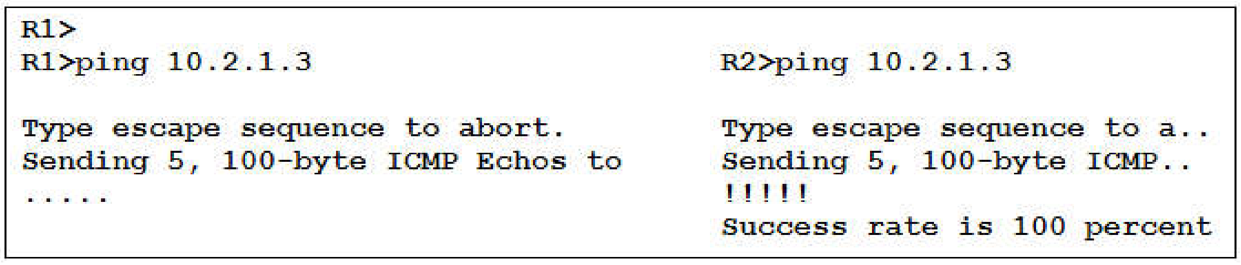
Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

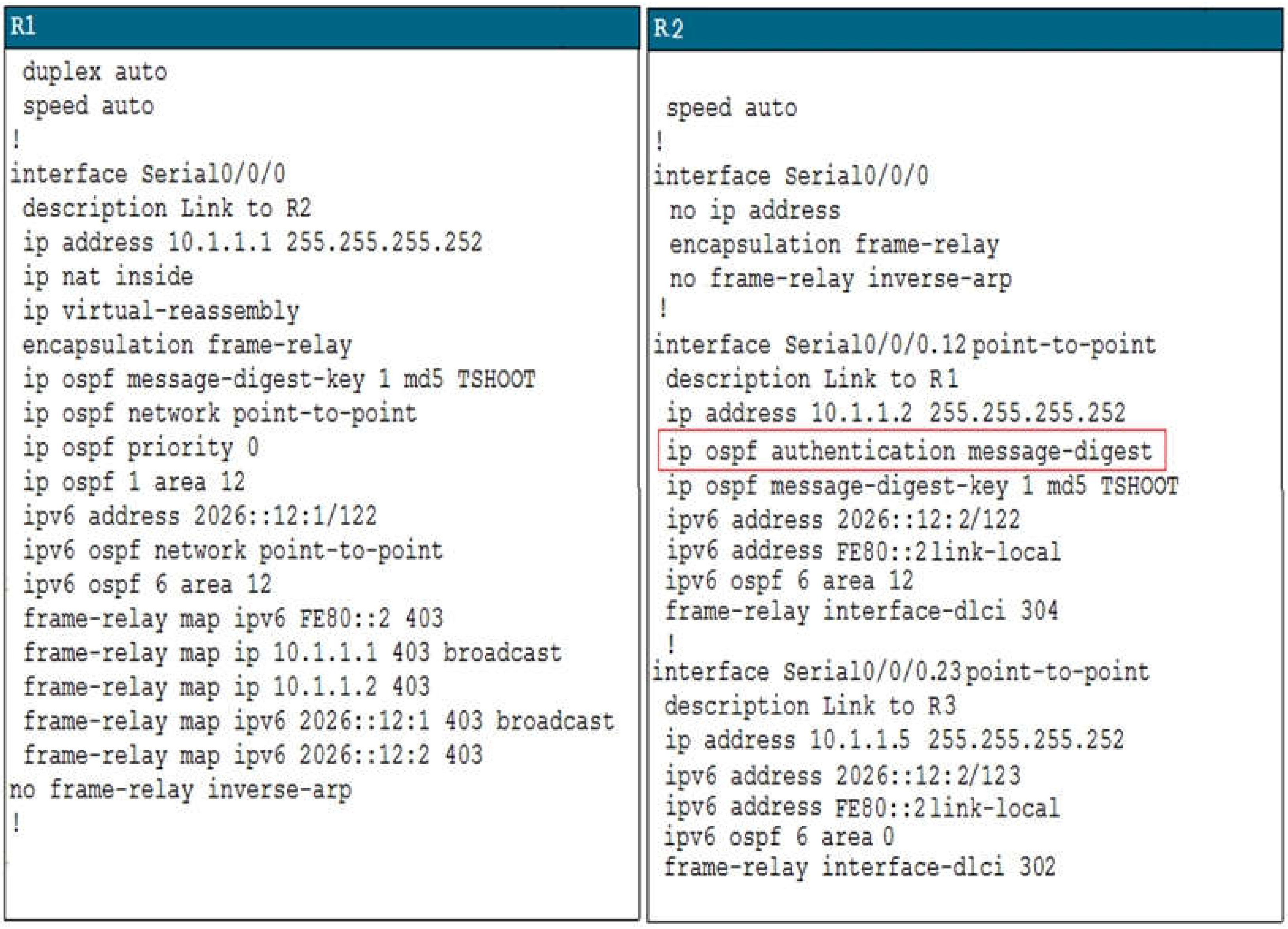
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
Ipconfig ----- Client will be receiving IP address 10.2.1.3

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



```
R1>
R1>ping 10.2.1.3                      R2>ping 10.2.1.3

Type escape sequence to abort.        Type escape sequence to a..
Sending 5, 100-byte ICMP Echos to     Sending 5, 100-byte ICMP..
.....                                 !!!!!
                                      Success rate is 100 percent
```

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



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

```
R2

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

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

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

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

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

On which device is the fault condition located?

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

Correct Answer: A
Section: [none]
Explanation

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

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

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

The fault condition is related to which technology?

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

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

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

Correct Answer: A
Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

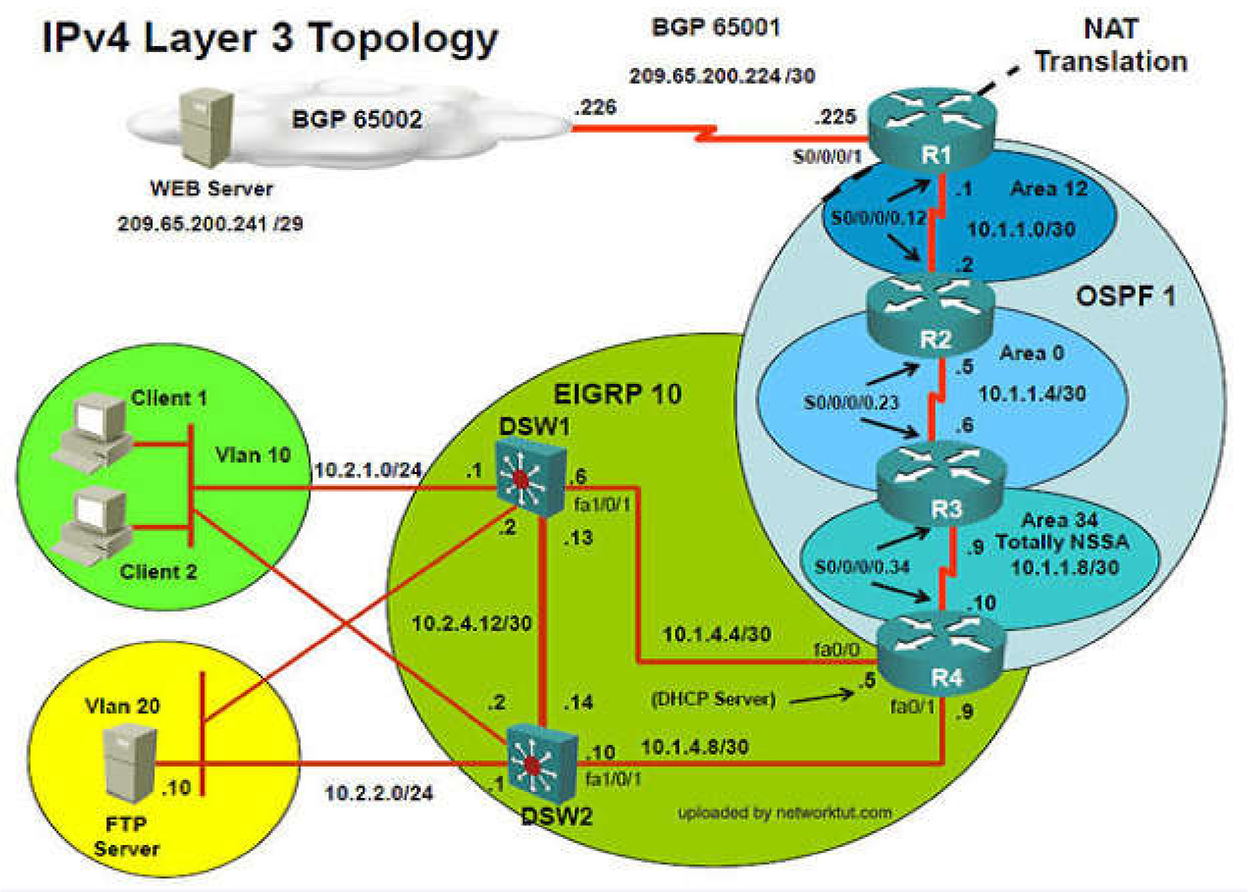
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

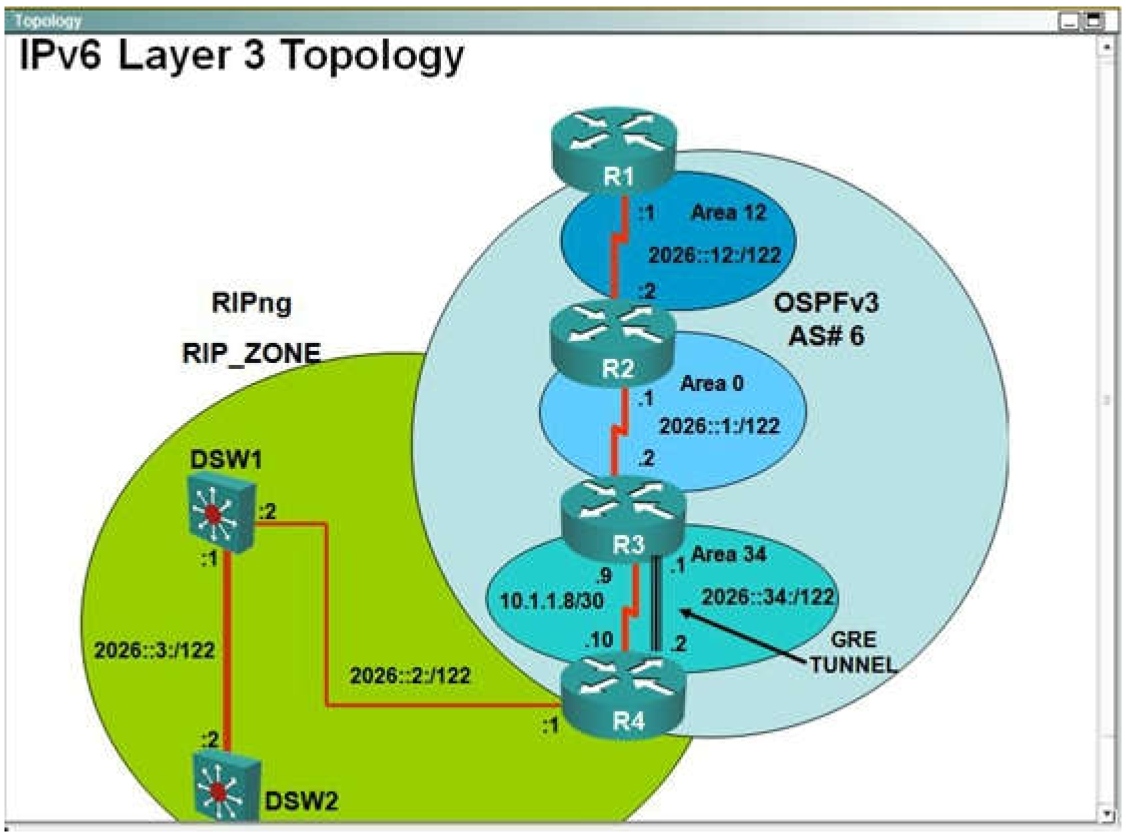
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

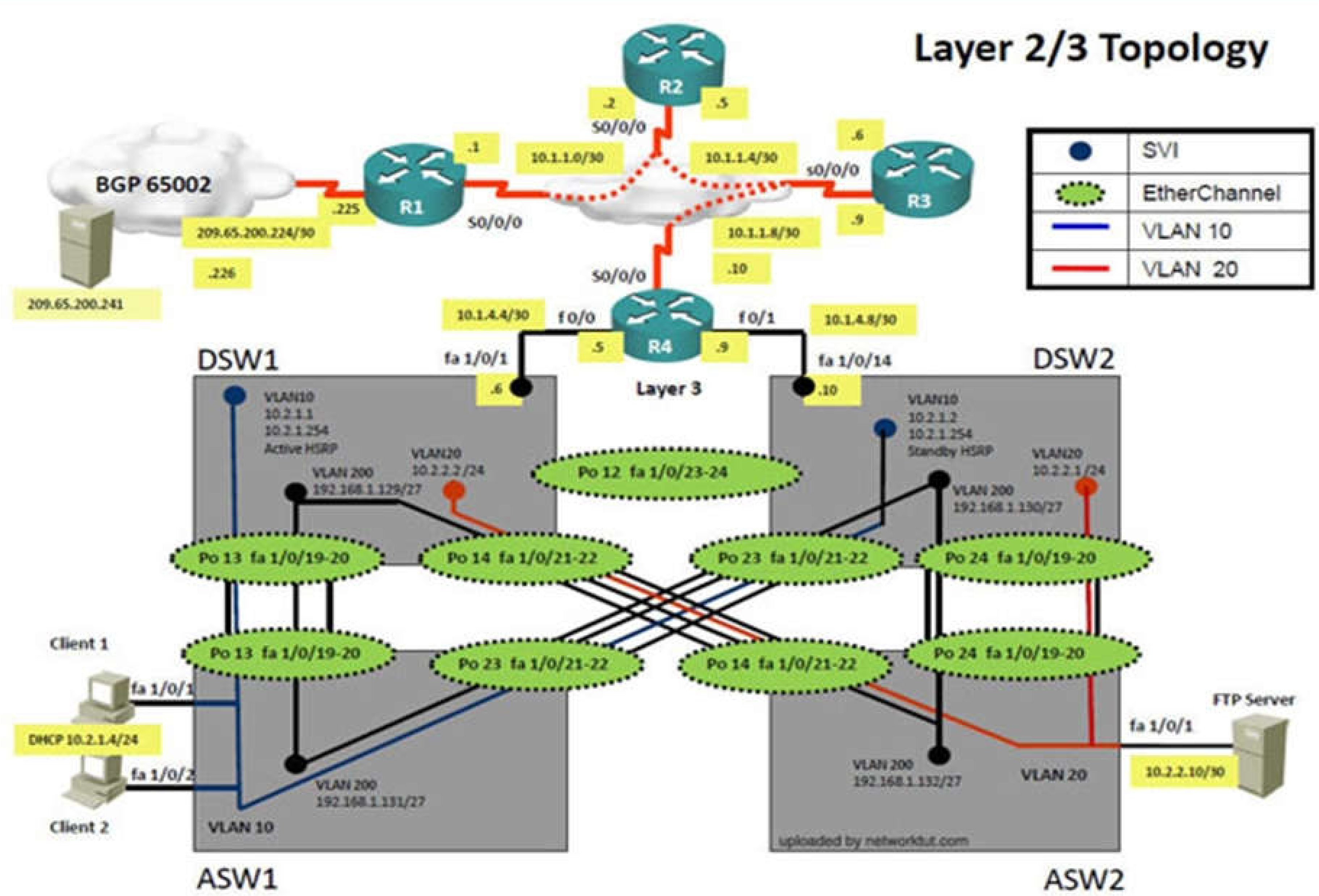
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

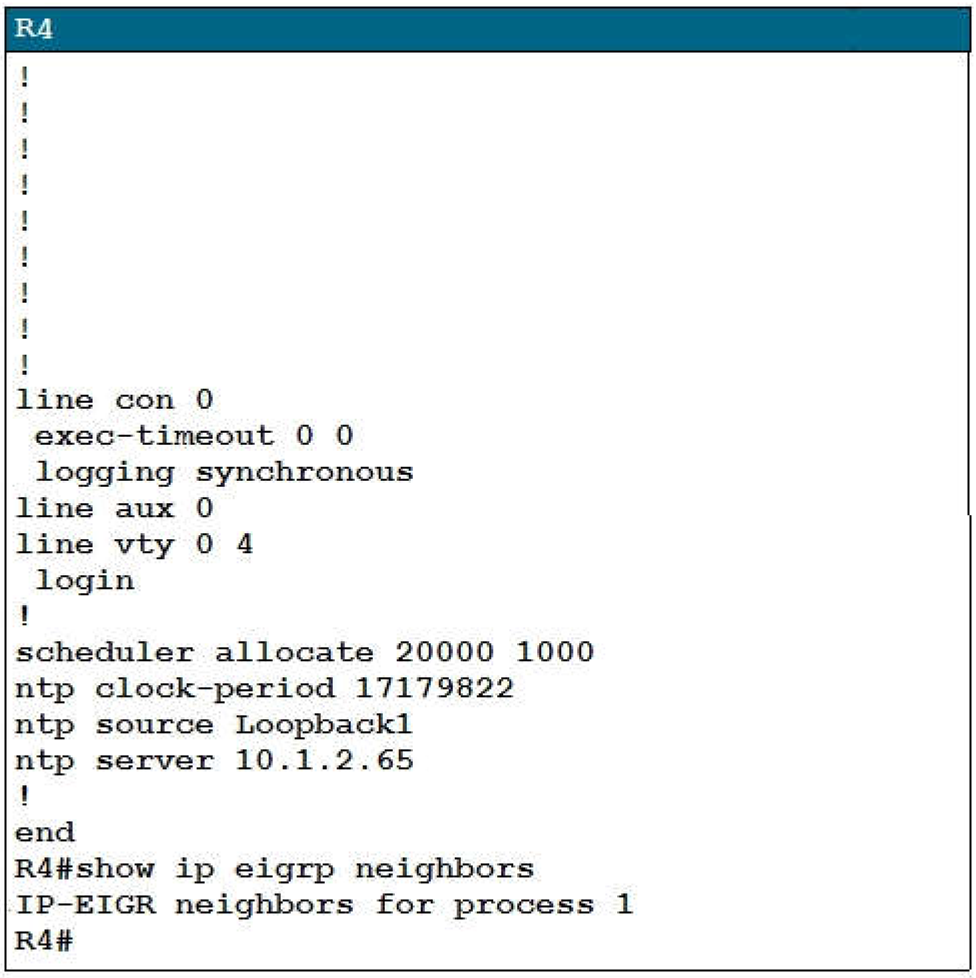
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution


IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT
Translation
BGP 65002
.226
.225
WEB Server
209.65.200.241 /29
S0/0/0/1
R1
.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
fa0/0
.5
fa0/1
.9
(DHCP Server)
EIGRP 10
DSW1
Client 1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
.2
.13
Client 2
10.2.4.12/30
10.1.4.4/30
Vlan 20
.2
.14
.10
10.1.4.8/30
.10
10.2.2.0/24
.1
fa1/0/1
DSW2
FTP
Server
uploaded by networktut.com

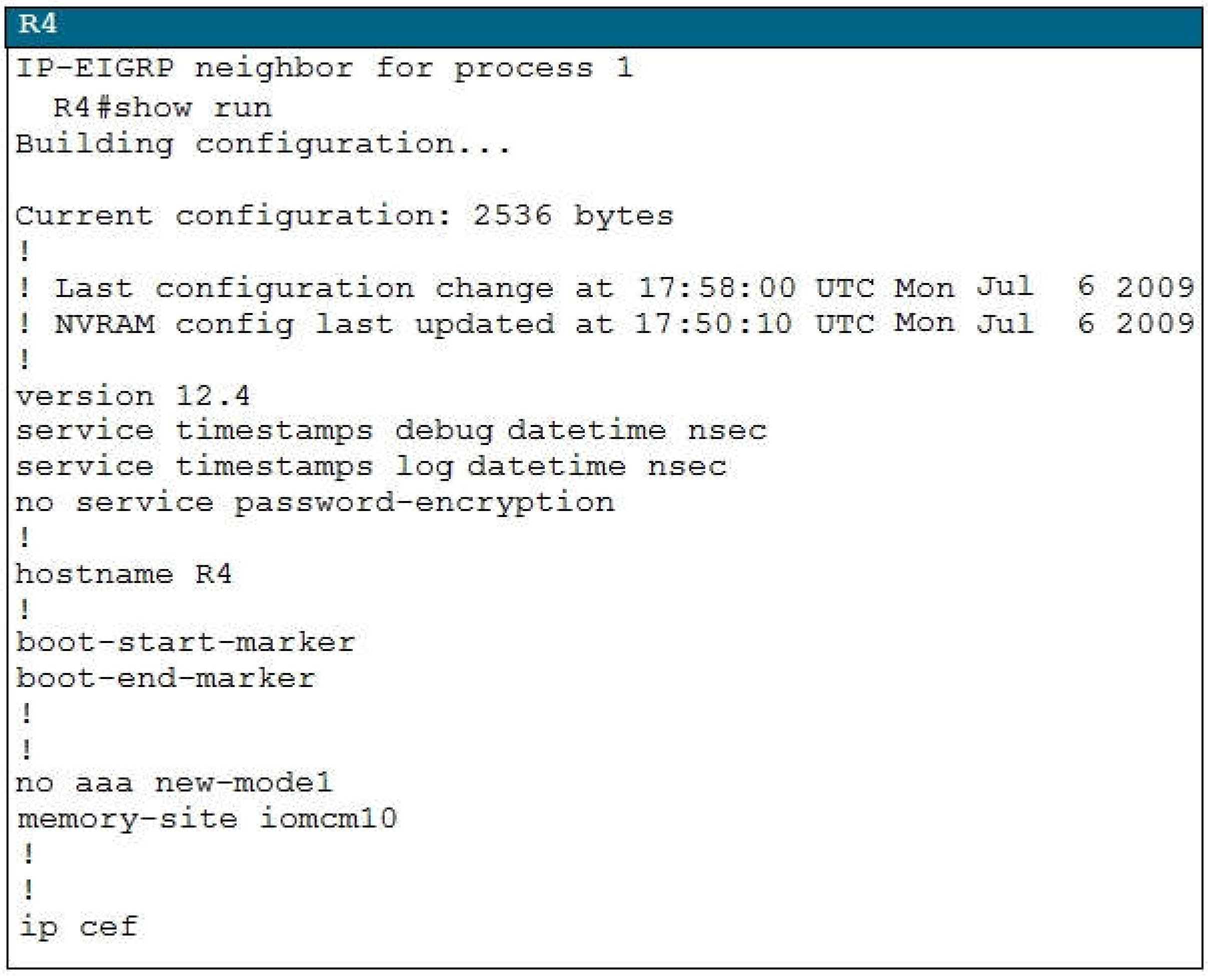

Topology
IPv6 Layer 3 Topology
R1
:1
Area 12
2026::12:/122
:2
OSPFv3
AS# 6
RIPng
RIP_ZONE
R2
Area 0
.1
2026::1:/122
.2
DSW1
:2
R3
:1
Area 34
.9
.1
10.1.1.8/30
2026::34:/122
2026::3:/122
.10
.2
GRE
TUNNEL
2026::2:/122
:1
R4
:2
DSW2





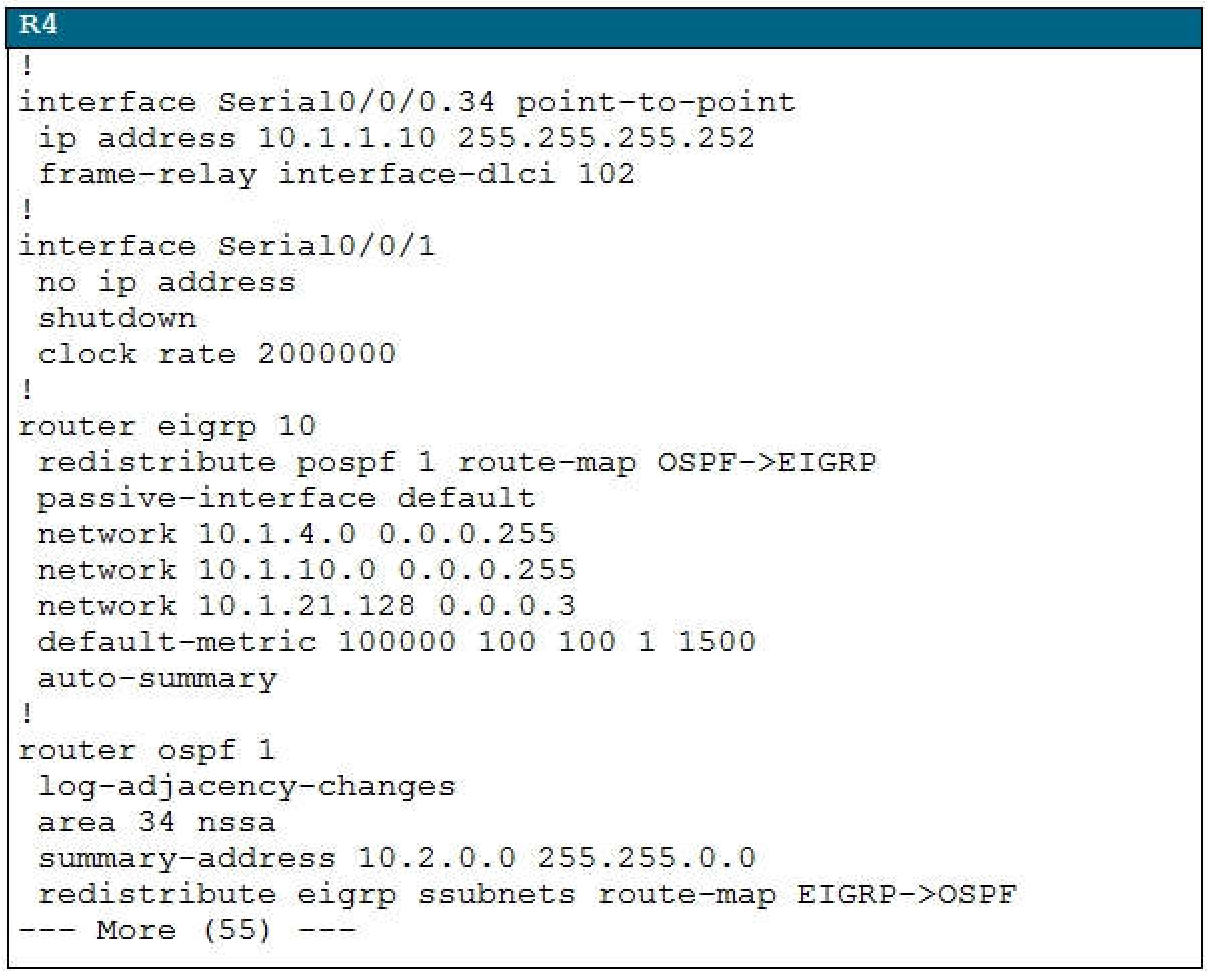
R4

```
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
ntp clock-period 17179822
ntp source Loopback1
ntp server 10.1.2.65
!
end
R4#show ip eigrp neighbors
IP-EIGR neighbors for process 1
R4#
```



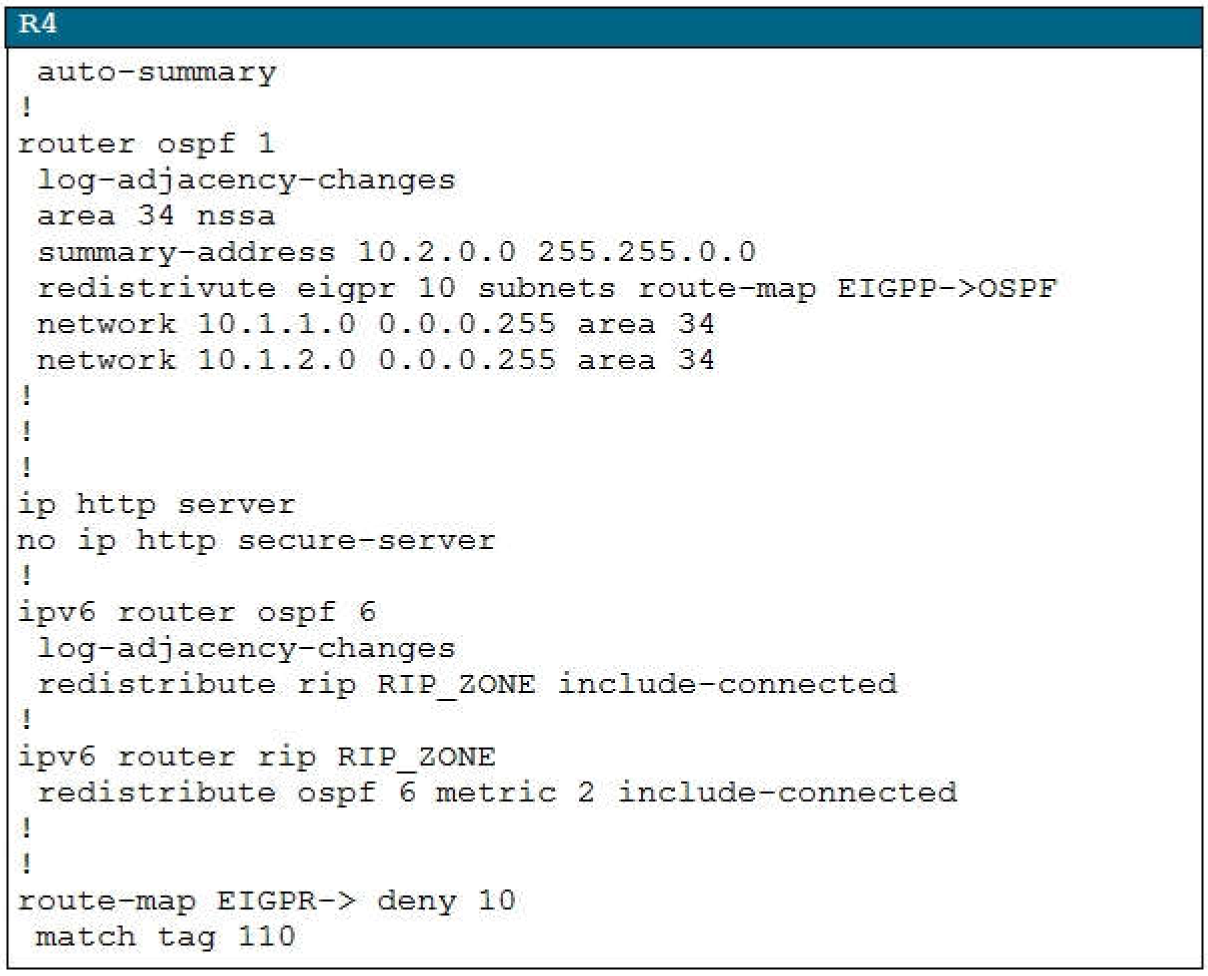
R4

```
IP-EIGRP neighbor for process 1
  R4#show run
Building configuration...

Current configuration: 2536 bytes
!
! Last configuration change at 17:58:00 UTC Mon Jul  6 2009
! NVRAM config last updated at 17:50:10 UTC Mon Jul  6 2009
!
version 12.4
service timestamps debug datetime nsec
service timestamps log datetime nsec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
no aaa new-mode1
memory-site iomcm10
!
!
ip cef
```



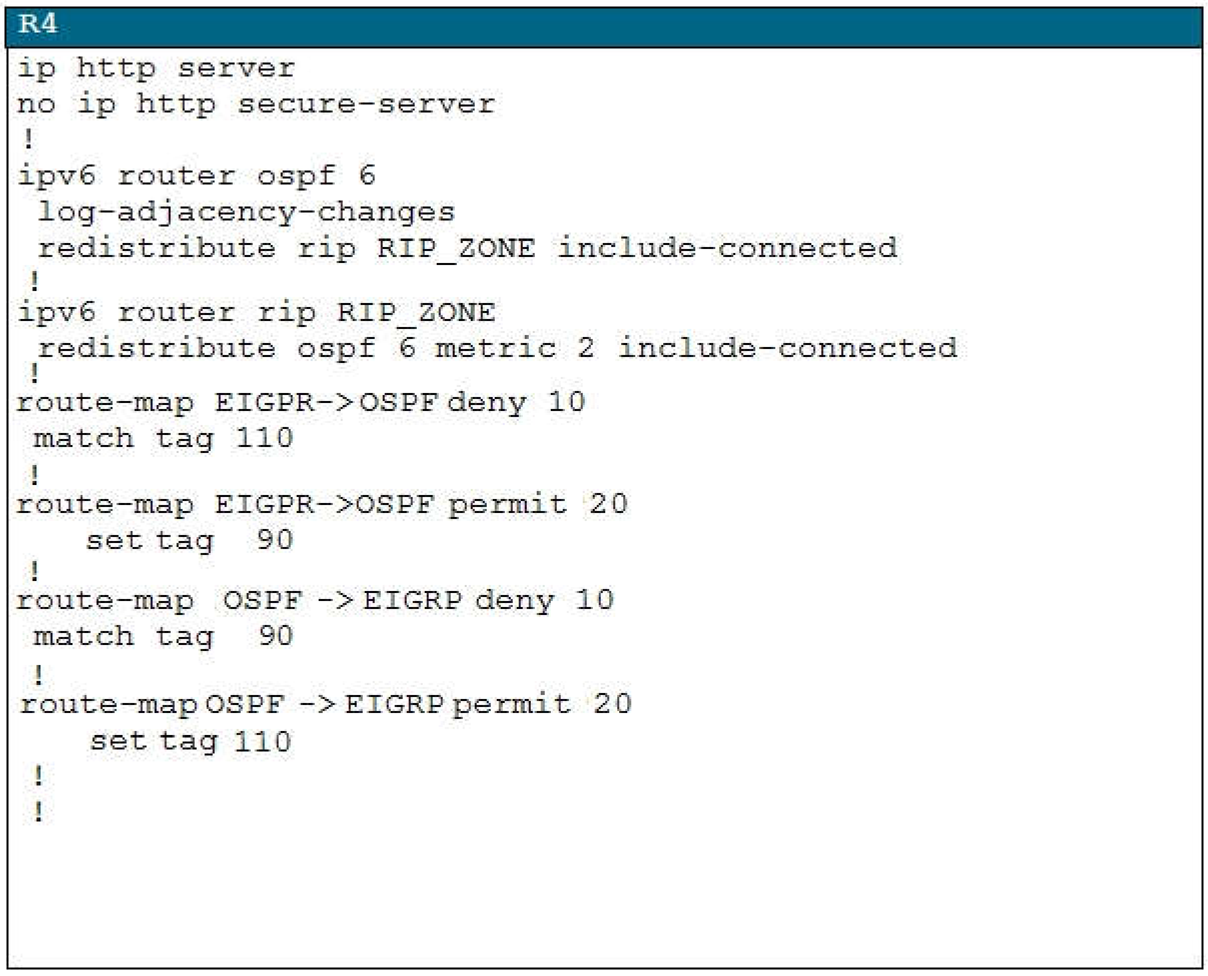
R4

```
!
interface Serial0/0/0.34 point-to-point
 ip address 10.1.1.10 255.255.255.252
 frame-relay interface-dlci 102
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router eigrp 10
 redistribute pospf 1 route-map OSPF->EIGRP
 passive-interface default
 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 ssubnets route-map EIGRP->OSPF
--- More (55) ---
```



R4

```
 auto-summary
!
router ospf 1
 log-adjacency-changes
 area 34 nssa
 summary-address 10.2.0.0 255.255.0.0
 redistrivute eigpr 10 subnets route-map EIGPP->OSPF
 network 10.1.1.0 0.0.0.255 area 34
 network 10.1.2.0 0.0.0.255 area 34
!
!
!
ip http server
no ip http secure-server
!
ipv6 router ospf 6
 log-adjacency-changes
 redistribute rip RIP_ZONE include-connected
!
ipv6 router rip RIP_ZONE
 redistribute ospf 6 metric 2 include-connected
!
!
route-map EIGPR-> deny 10
 match tag 110
```



R4

```
ip http server
no ip http secure-server
 !
ipv6 router ospf 6
 log-adjacency-changes
 redistribute rip RIP_ZONE include-connected
 !
ipv6 router rip RIP_ZONE
 redistribute ospf 6 metric 2 include-connected
 !
route-map EIGPR->OSPF deny 10
 match tag 110
 !
route-map EIGPR->OSPF permit 20
    set tag  90
 !
route-map  OSPF -> EIGRP deny 10
 match tag  90
 !
route-map OSPF -> EIGRP permit 20
    set tag 110
 !
 !
```

Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

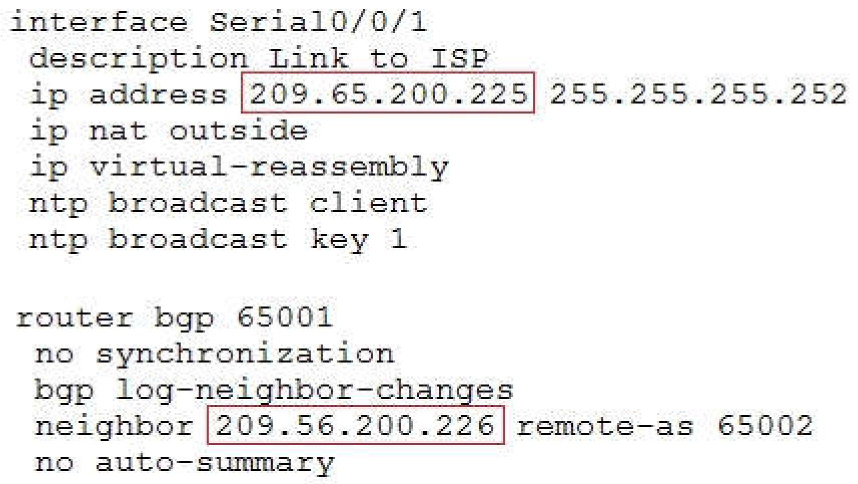
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
ipconfig ----- Client will be receiving IP address 10.2.1.3

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

3. Look for BGP Neighbourship
Sh ip bgp summary ----- No O/P will be seen

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

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



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

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

6. Since we are receiving icmp packets from Webserver interface on R1 so peering IP address under router BGP is configured wrong IP but with correct AS nos.

7. **Change required:** On R1 under router BGP Change neighbor 209.56.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65002

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

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

On which device is the fault condition located?

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The BGP neighbor statement is wrong on R1.

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

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

The fault condition is related to which technology?

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

Correct Answer: A
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

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

Correct Answer: D
Section: [none]
Explanation

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

Question Set 2

QUESTION 1
SIMULATION

Scenario
You work as Network Engineer for RADO Network Ltd company. Your colleague has set up a POC lab that simulates a customer network to study about the behavior of BGP protocol when routes are exchanged between two different autonomous systems.

Review the topology. You must identify and fix IBGP and EBGP issues on R1 router.

Topology Details
AS64520

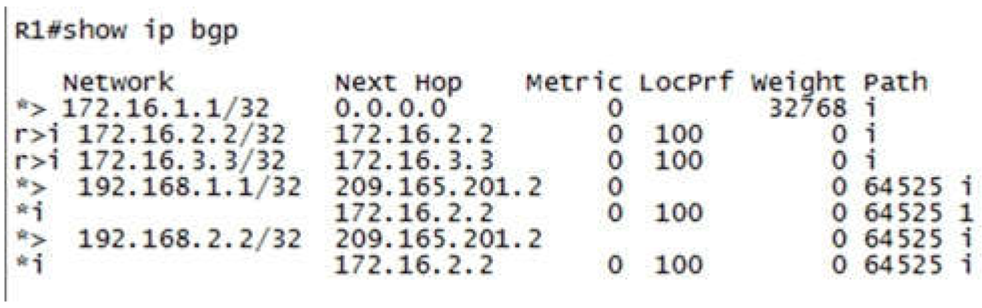
- R1, R2, and R3 are three routers on AS 64520, and OSPF is the IGP routing protocol that is configured between them.
- IBGP is configured between R1, R2, and R3 routers using peer group.
- Loopback0 address is used for IBGP peering. Loopback0 address configured on R1, R2, and R3 are advertised into BGP domain on AS64525.

AS64525

- RA and RB are two routers on AS 64525, and EIGRP is the IGP routing protocol that is configured between them.
- Loopback0 address is used for IBGP peering. Loopback0 address is configured on RA and RB and it is advertised into the BGP domain on AS64525.
- R1 and RA form a EBGP neighbor relationship using a physical interface address.
- R2 and RB form a EBGP neighbor relationship using a physical interface address.

Simulation Requirements

- Identify and fix the EBGP neighbor relationship issue between R1 and RA routers.
- Identify and fix the IBGP neighbor relationship issue between R1 and R2, and R1, and R3.
- You are allowed to remove any misconfiguration or incorrect configuration to only fix the issue. Other initial configurations that do not impact the issues must not be changed.
- After you fix two issues on the R1 router, the final BGP table must appear as shown here.



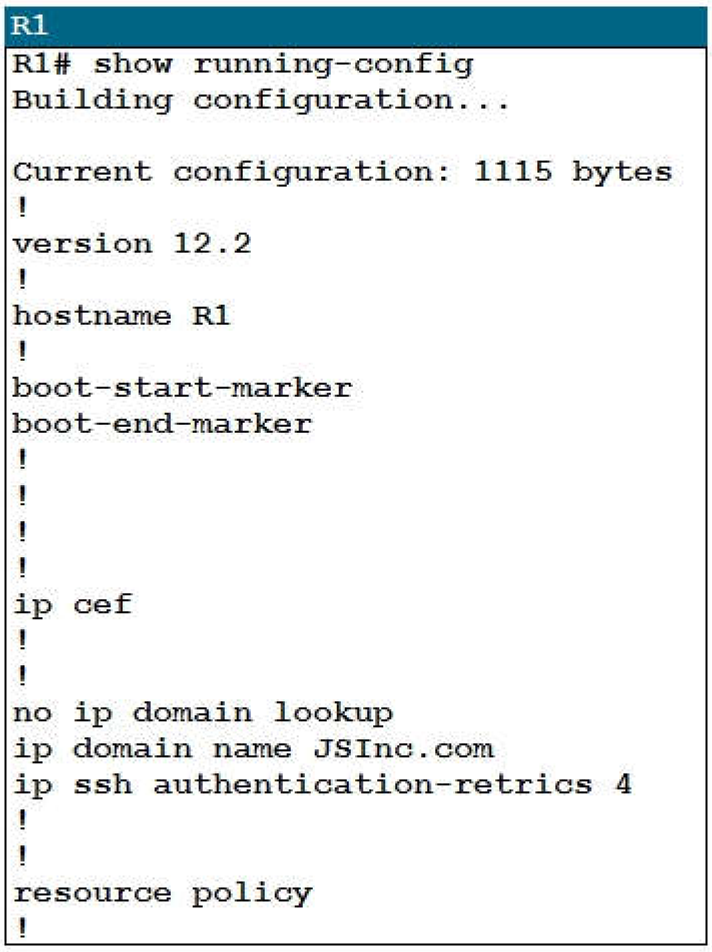
```
R1#show ip bgp

   Network          Next Hop      Metric LocPrf Weight Path
*> 172.16.1.1/32    0.0.0.0            0         32768 i
r>i 172.16.2.2/32   172.16.2.2         0  100        0 i
r>i 172.16.3.3/32   172.16.3.3         0  100        0 i
*>  192.168.1.1/32  209.165.201.2      0             0 64525 i
*i                  172.16.2.2         0  100        0 64525 1
*>  192.168.2.2/32  209.165.201.2                    0 64525 i
*i                  172.16.2.2         0  100        0 64525 i
```

Special Note: To gain the maximum number of points, you must fix IBGP and EBGP neighbor issues on router R1.

- **BGP must be configured without using address families. Do not change the BGP peer group name.**
- **Console logging and debugging features are disabled.**
- **Use show commands to verify the BGP neighbor relationship.**

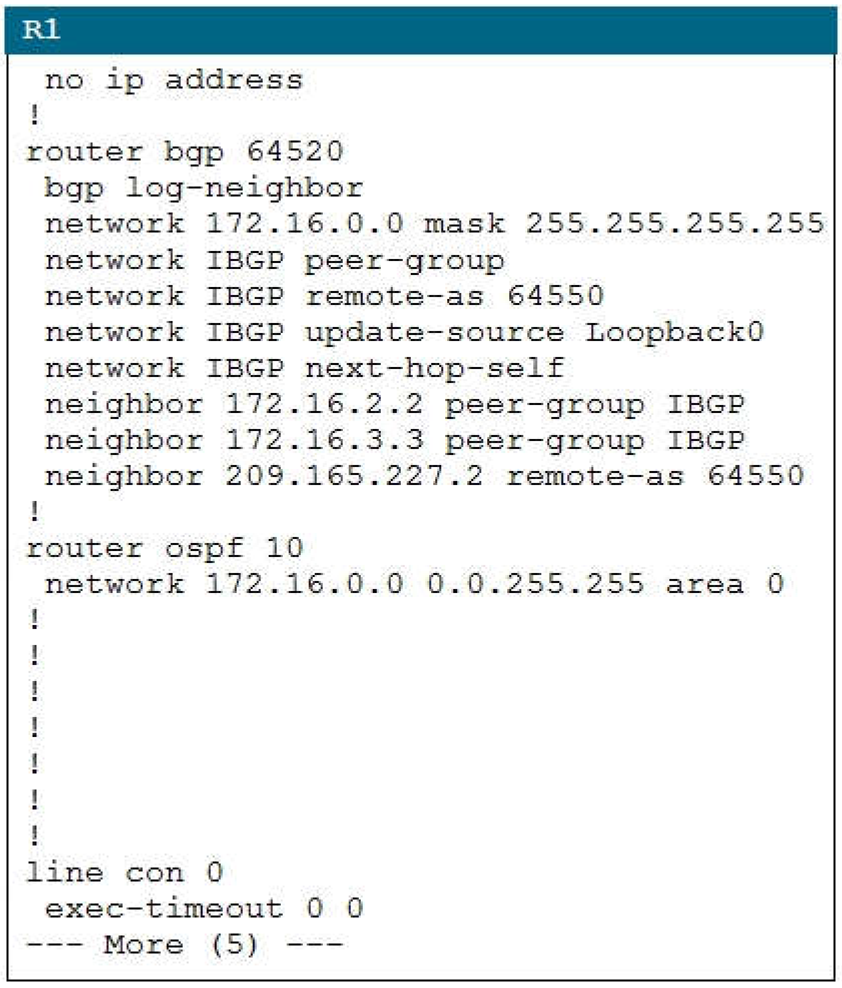
Instructions
To configure a router, click the console host icon in the topology.

To view the different windows, click the buttons at the bottom of the window.

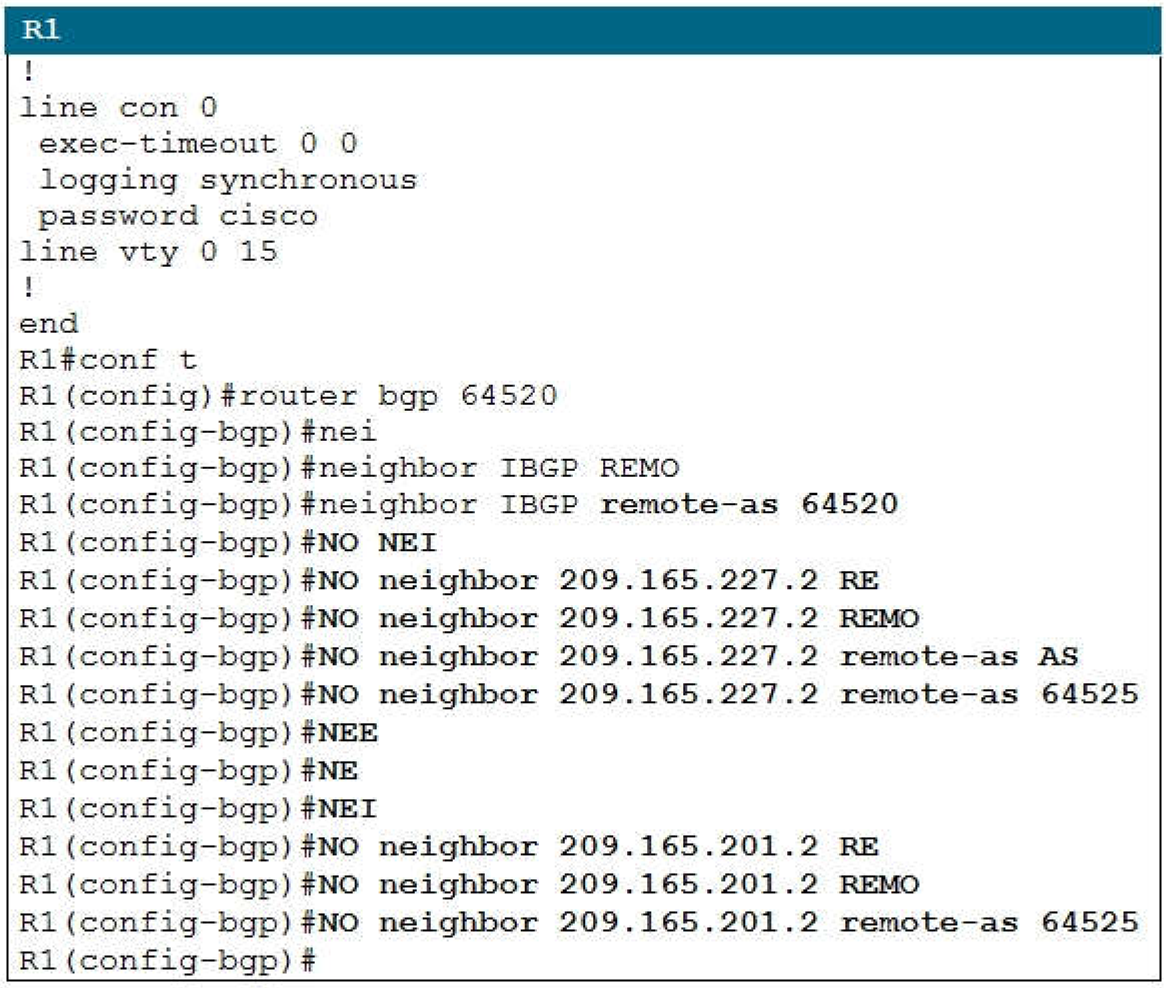


R1

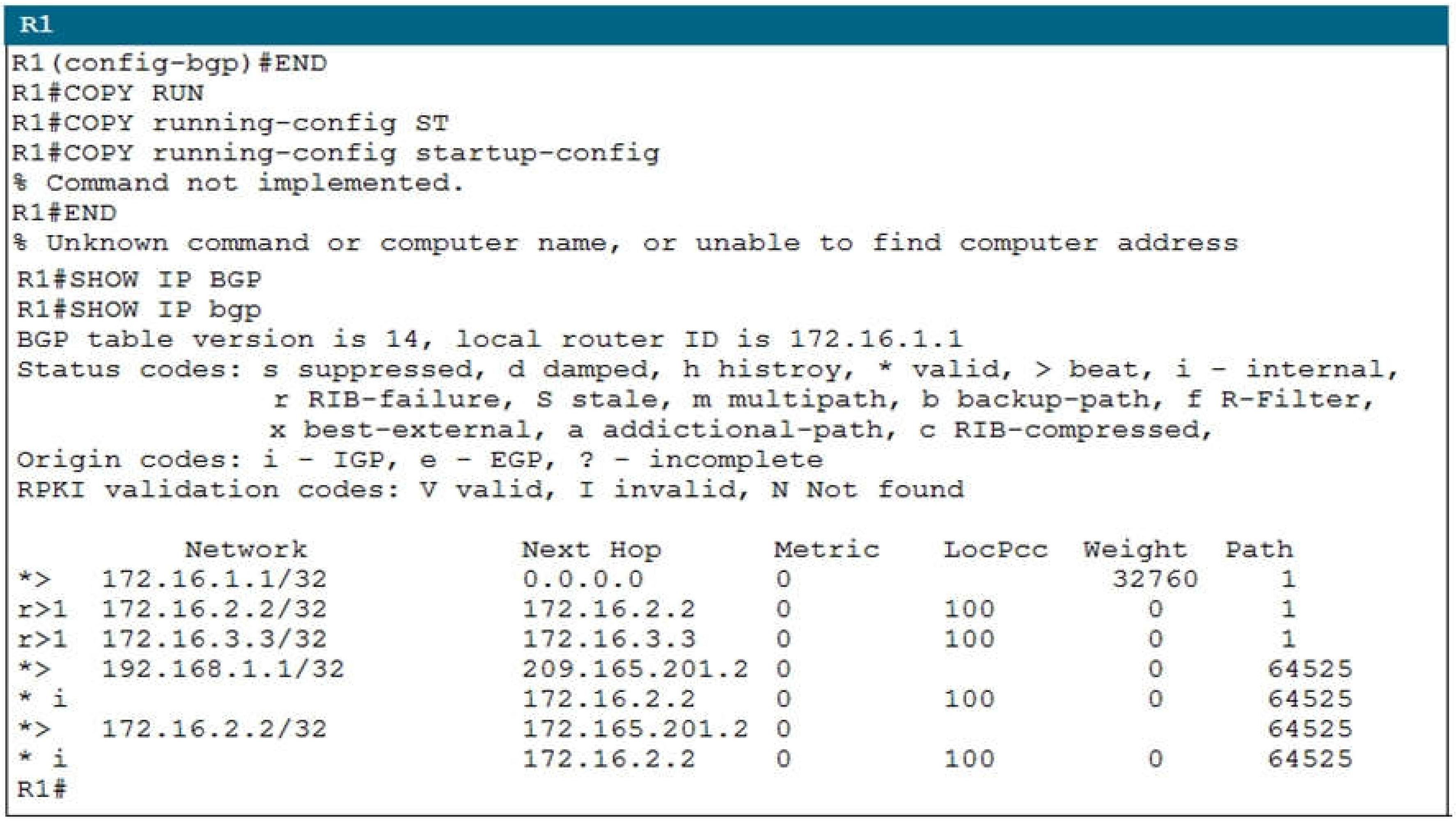
```
R1# show running-config
Building configuration...

Current configuration: 1115 bytes
!
version 12.2
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
!
ip cef
!
!
no ip domain lookup
ip domain name JSInc.com
ip ssh authentication-retrics 4
!
!
resource policy
!
```



```
 no ip address
!
router bgp 64520
 bgp log-neighbor
 network 172.16.0.0 mask 255.255.255.255
 network IBGP peer-group
 network IBGP remote-as 64550
 network IBGP update-source Loopback0
 network IBGP next-hop-self
 neighbor 172.16.2.2 peer-group IBGP
 neighbor 172.16.3.3 peer-group IBGP
 neighbor 209.165.227.2 remote-as 64550
!
router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
--- More (5) ---
```



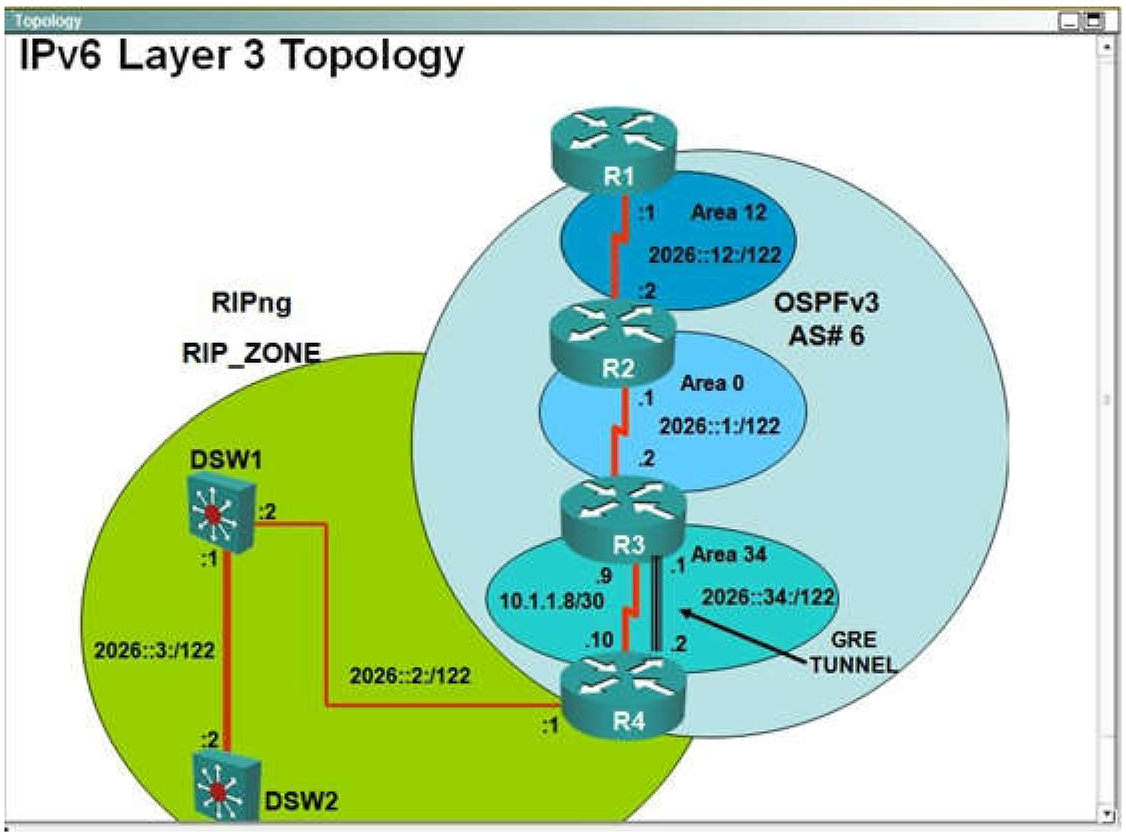
```
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
line vty 0 15
!
end
R1#conf t
R1(config)#router bgp 64520
R1(config-bgp)#nei
R1(config-bgp)#neighbor IBGP REMO
R1(config-bgp)#neighbor IBGP remote-as 64520
R1(config-bgp)#NO NEI
R1(config-bgp)#NO neighbor 209.165.227.2 RE
R1(config-bgp)#NO neighbor 209.165.227.2 REMO
R1(config-bgp)#NO neighbor 209.165.227.2 remote-as AS
R1(config-bgp)#NO neighbor 209.165.227.2 remote-as 64525
R1(config-bgp)#NEE
R1(config-bgp)#NE
R1(config-bgp)#NEI
R1(config-bgp)#NO neighbor 209.165.201.2 RE
R1(config-bgp)#NO neighbor 209.165.201.2 REMO
R1(config-bgp)#NO neighbor 209.165.201.2 remote-as 64525
R1(config-bgp)#
```



R1

```
R1(config-bgp)#END
R1#COPY RUN
R1#COPY running-config ST
R1#COPY running-config startup-config
% Command not implemented.
R1#END
% Unknown command or computer name, or unable to find computer address
R1#SHOW IP BGP
R1#SHOW IP bgp
BGP table version is 14, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h histroy, * valid, > beat, i - internal,
              r RIB-failure, S stale, m multipath, b backup-path, f R-Filter,
              x best-external, a addictional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

       Network             Next Hop       Metric    LocPcc   Weight  Path
*>   172.16.1.1/32         0.0.0.0        0                   32760     1
r>1  172.16.2.2/32         172.16.2.2     0         100         0       1
r>1  172.16.3.3/32         172.16.3.3     0         100         0       1
*>   192.168.1.1/32        209.165.201.2  0                     0      64525
* i                        172.16.2.2     0         100         0      64525
*>   172.16.2.2/32         172.165.201.2  0                            64525
* i                        172.16.2.2     0         100         0      64525
R1#
```

To minimize the windows, click the [-]. To move a window, drag it by the title bar.

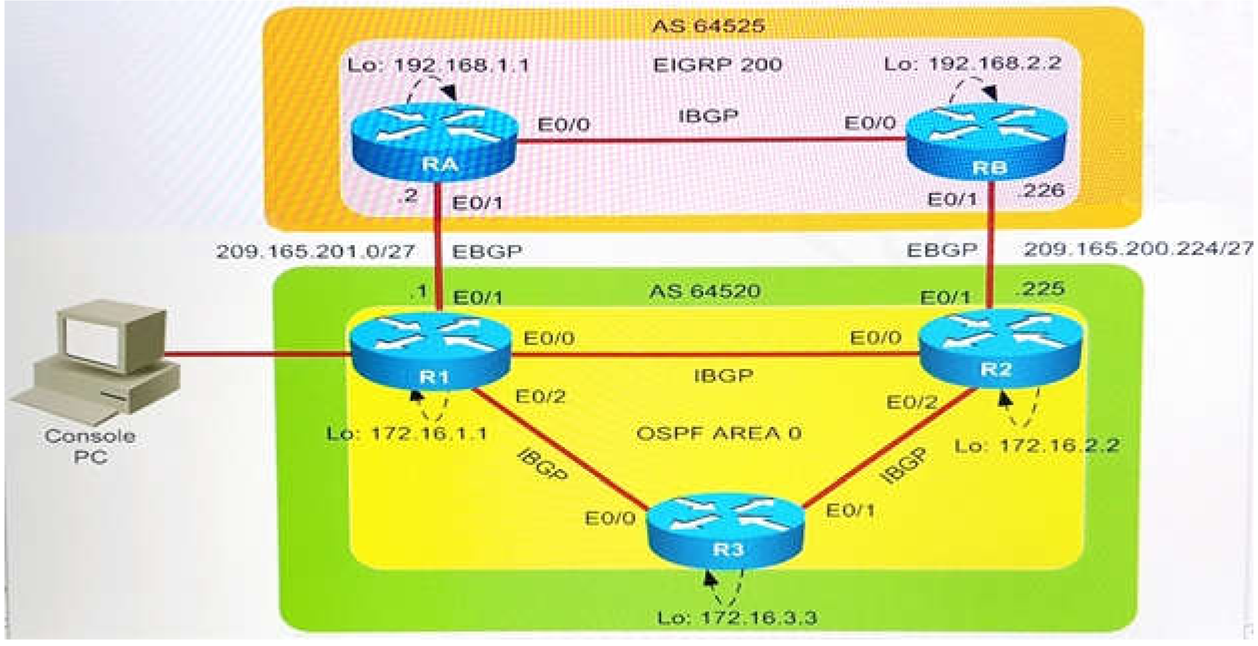


Most commands that use the “Control” or “Escape” keys are not supported and are not necessary to complete this simulation. The **help** command does not display all commands of the help system.

Console access is available to router R1.

The password that is configured on router R1 is **cisco** (all small letters).
(Console cable is connected between PC and R1.)

Topology



Correct Answer: See explanation below
Section: [none]
Explanation

Explanation/Reference:
Explanation:

For EBGP and IBGP labs you have to make corrections to the configuration in a router R1. You have only access to Router R1. R1 and RA should be neighbors through EBGP. in R1 you will find this command:

```
(config-router)#Neighbor 209.165.277.2 remote-as 64525
```

The ip address here is wrong , delete this command using:

```
(config-router)#No Neighbor 209.165.277.2 remote-as 64525
```

And replace it with new command with the correct IP of RA E0/1 interface by typing this command:

```
(config-router)#Neighbor 209.165.201.2 remote-as 64525
```

R1 and R2 and R3 are neighbors through IBGP, and R1 use the peer-group IBGP to form neighborship between R1 and R2, and between R1 and R3, but actually there is an issue with the IBGP peer-group commands in R1 You will find in R1 these following commands:

```
(config-router)#neighbor IBGP peer-group
(config-router)#neighbor IBGP remote-as 64550
(config-router)#neighbor IBGP next-hop-self
(config-router)#neighbor IBGP update-source loopback 0
```

You must correct the Remote-AS for the Peer-Group IBGP to 64520 to form the neighborship correctly. Be aware, if you delete the config with no neighbor IBGP remote-as 64550 you also will delete the following lines:

```
(config-router)#neighbor IBGP peer-group
(config-router)#neighbor IBGP next-hop-self
(config-router)#neighbor IBGP update-source loopback 0
```

So dont delete the line regarding the remote-as, just replace it with:

```
(config-router)#neighbor IBGP remote-as 64520
```

In the Scenario regarding the Lab, they tell you how the routing-table should look if you have done everything right! So if you routing-table on R1 looks like the one they posted in the scenario you have done everything right and can go on to the next topic. You have to use the command "#show ip bgp " to show bgp routing table , dont use "#show ip route"

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

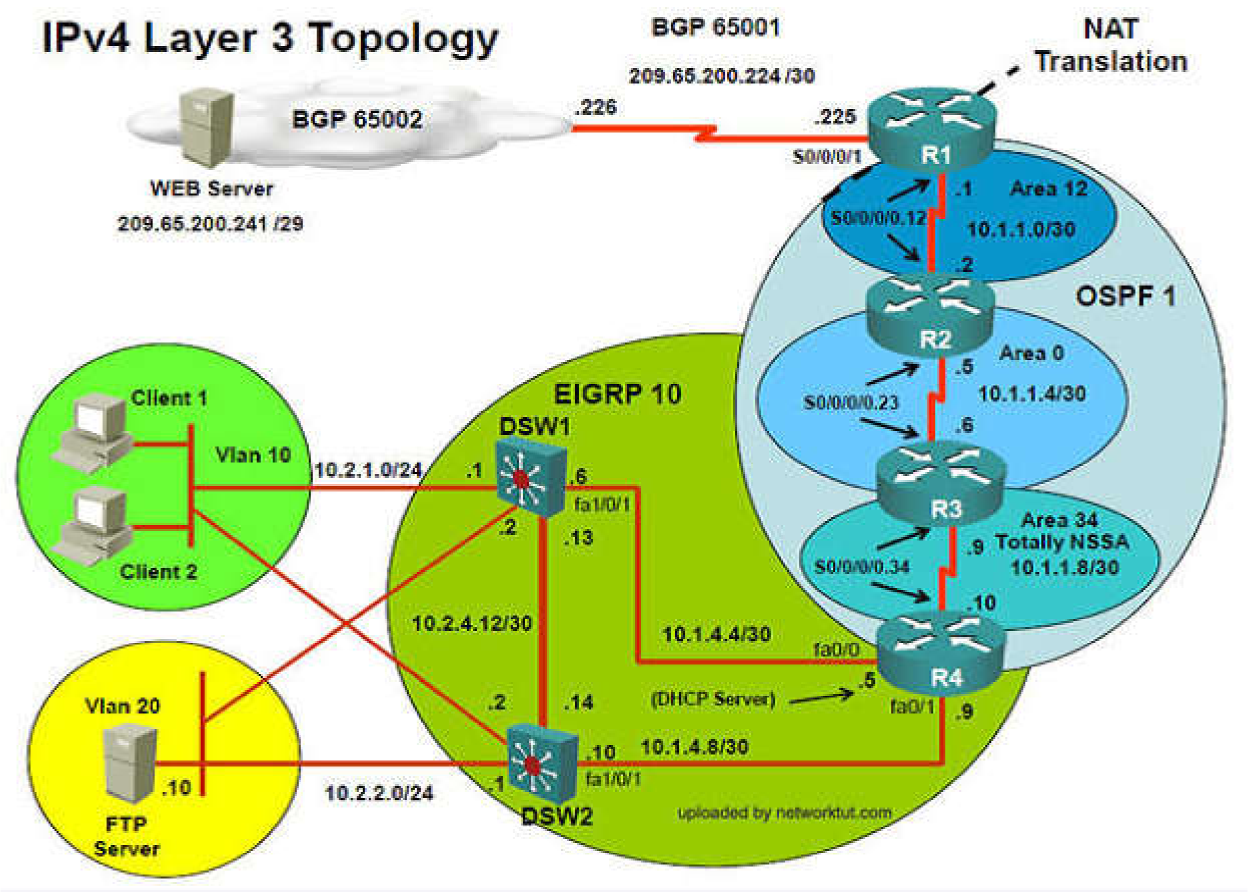
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

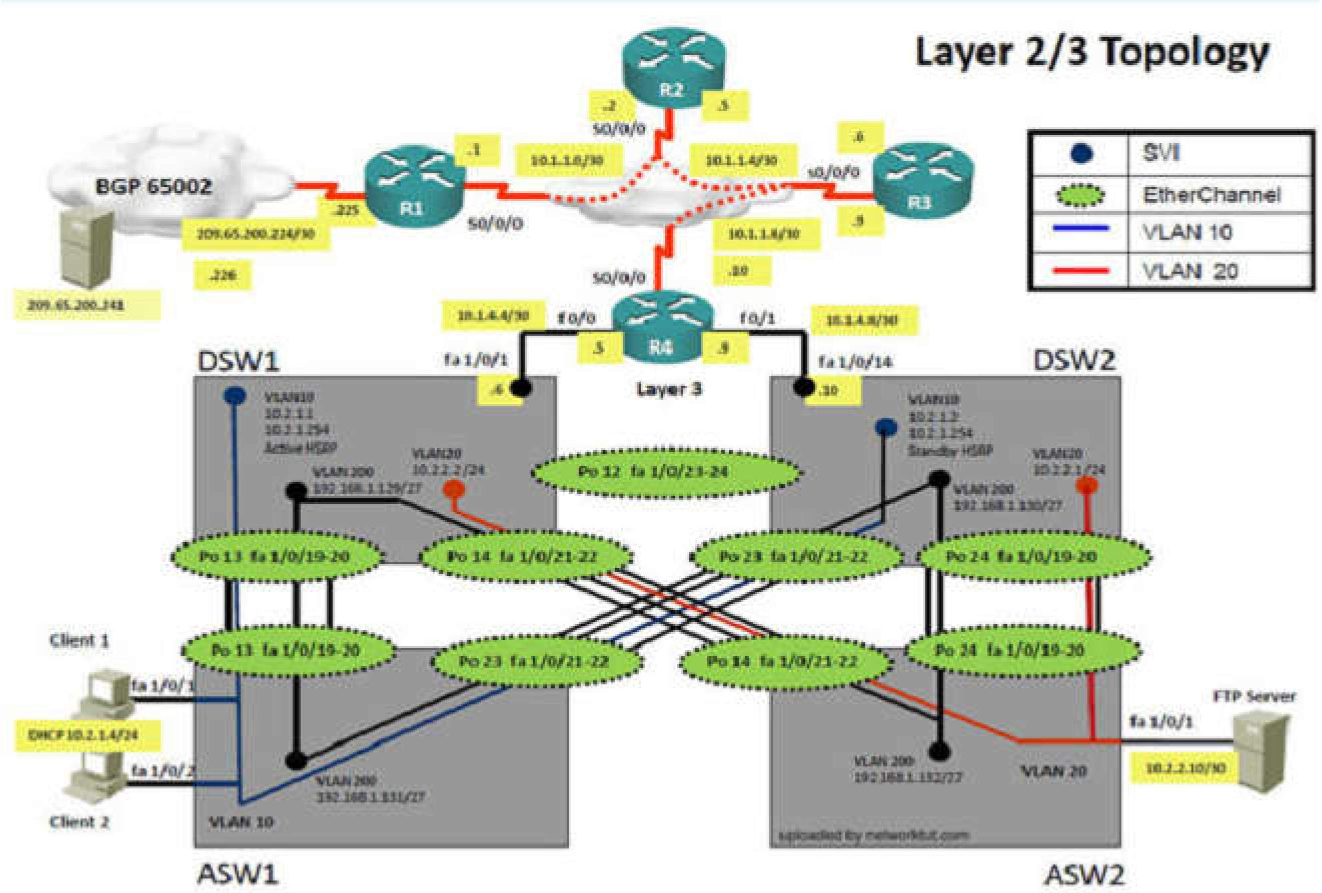
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution





Client is unable to ping IP 209.65.200.241

Solution

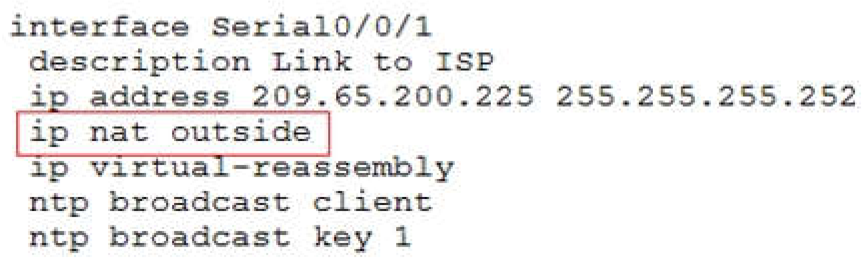
Steps need to follow as below:-

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

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

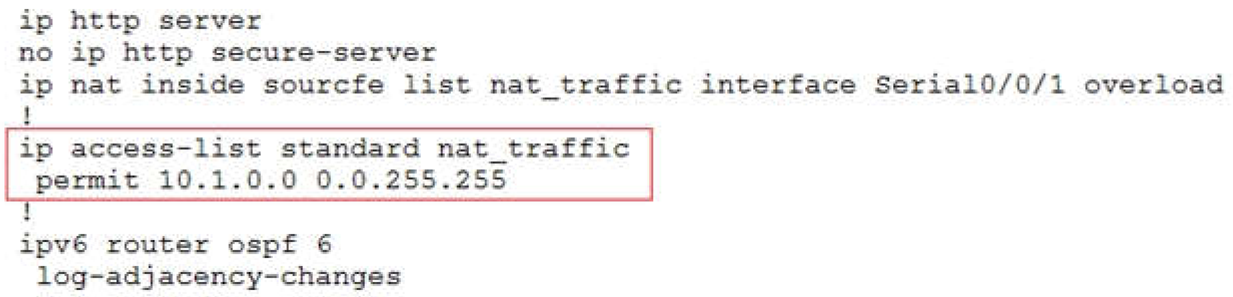
3. Look for BGP Neighbourship
Sh ip bgp summary ----- State of BGP will be in established state & will be able to receive I prefix (209.65.200.241)

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



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

!



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

!

From above snapshot we are able to see that IP needs to be PAT to serial 0/0/1 to reach web server IP (209.65.200.241). But in access-list of NAT IP allowed IP is 10.1.0.0/16 is allowed & need 10.2.0.0 /16 to
6. As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of web server & we are able to ping the same from R1. Its should be checked further for running config of interface for stopping

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

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

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

On which device is the fault condition located?

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

Correct Answer: A
Section: [none]
Explanation

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

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

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

The fault condition is related to which technology?

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

Correct Answer: C
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

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

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

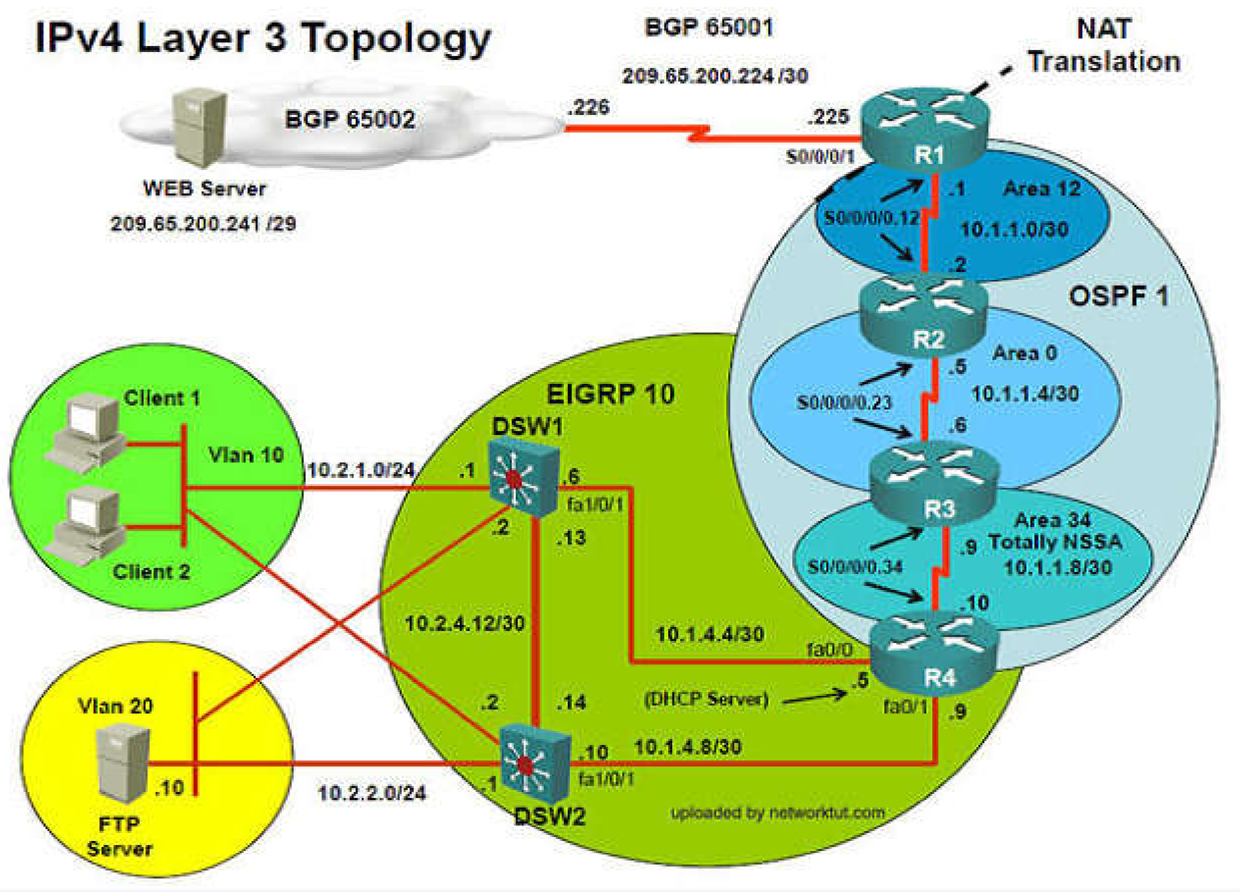
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

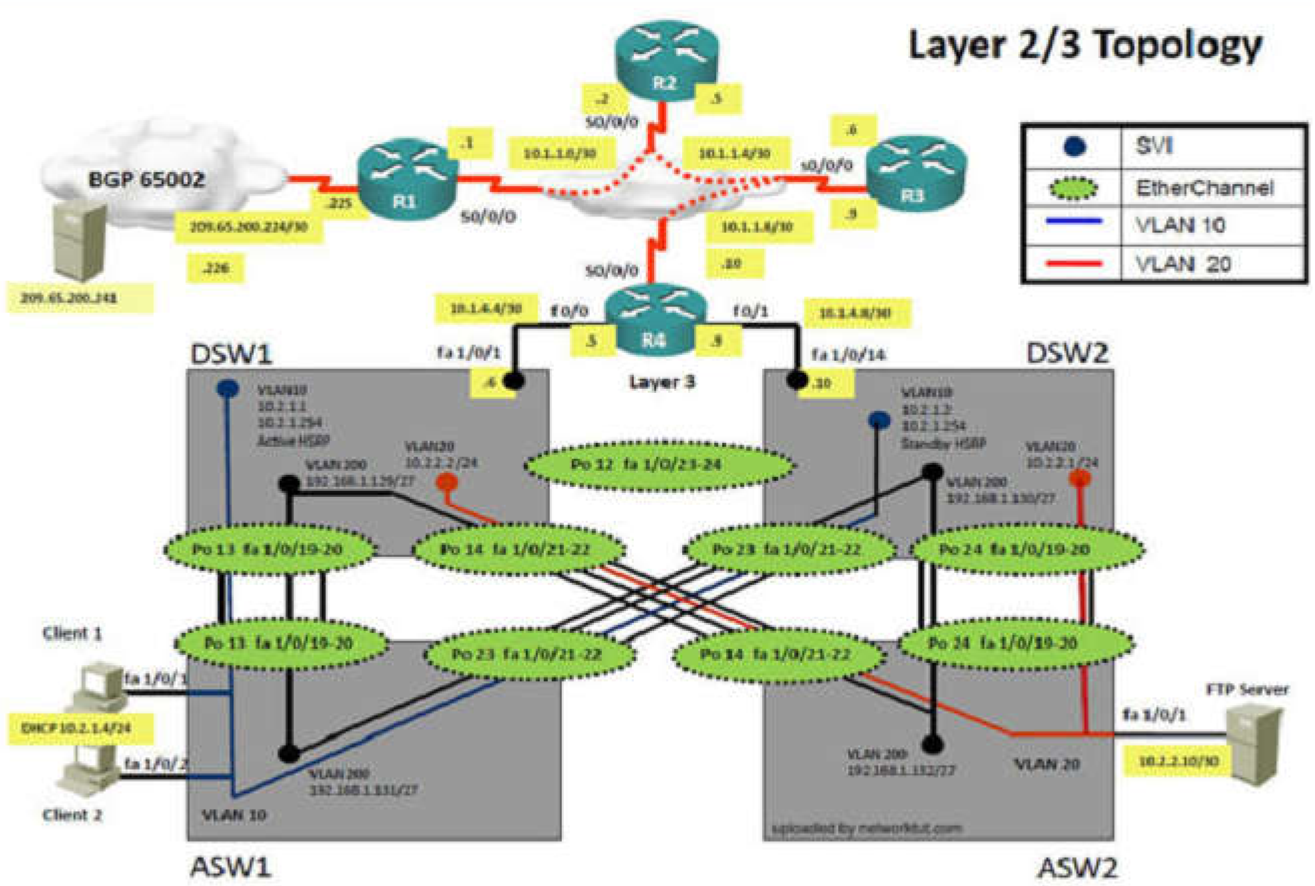
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution





Client is unable to ping IP 209.65.200.241…

Solution

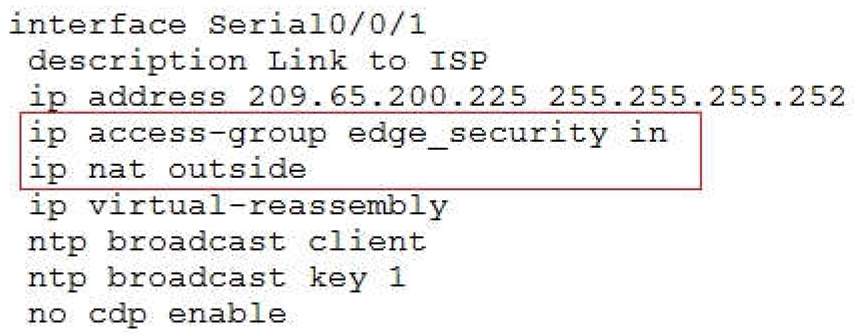
Steps need to follow as below:-

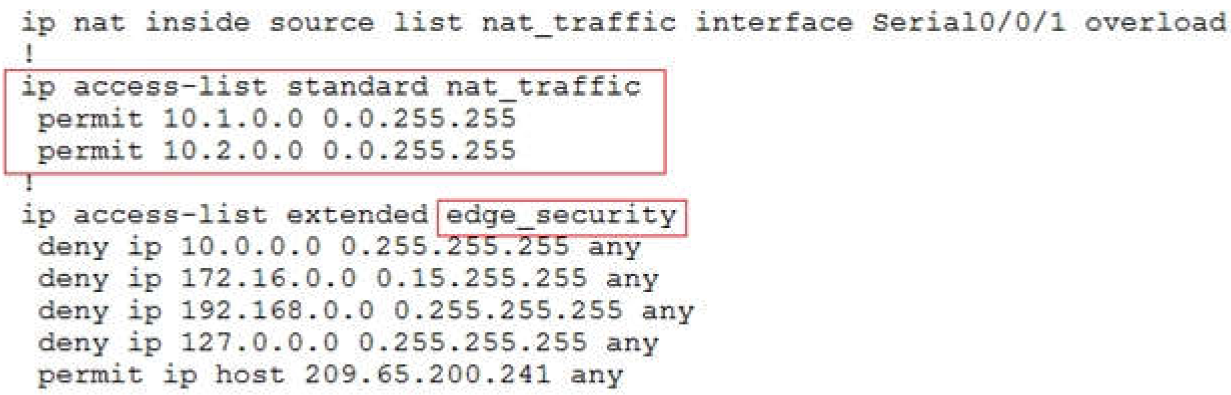
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
2. Ipconfig ----- Client will be receiving IP address 10.2.1.3

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

4. Look for BGP Neighbourship
5. Sh ip bgp summary ----- State of BGP will be in active state. This means connectivity issue between serial

6. Check for running config. i.e sh run --- over here check for access-list configured on interface as BGP is down (No need to check for NAT configuration as its configuration should be right as first need to bring BGP up)


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



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

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

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

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

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

On which device is the fault condition located?

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

Correct Answer: A
Section: [none]
Explanation

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

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

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

The fault condition is related to which technology?

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

Correct Answer: G
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

A. Under the interface Serial0/0/1 enter the ip access-group edge_security out command.
B. Under the ip access-list extended edge_security configuration add the permit ip 209.65.200.224 0.0.0.3 any command.
C. Under the ip access-list extended edge_security configuration delete the deny ip 10.0.0.0 0.255.255.255 any command.
D. Under the interface Serial0/0/0 configuration delete the ip access-group edge_security in command and enter the ip access-group edge_security out command.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

Explanation:

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

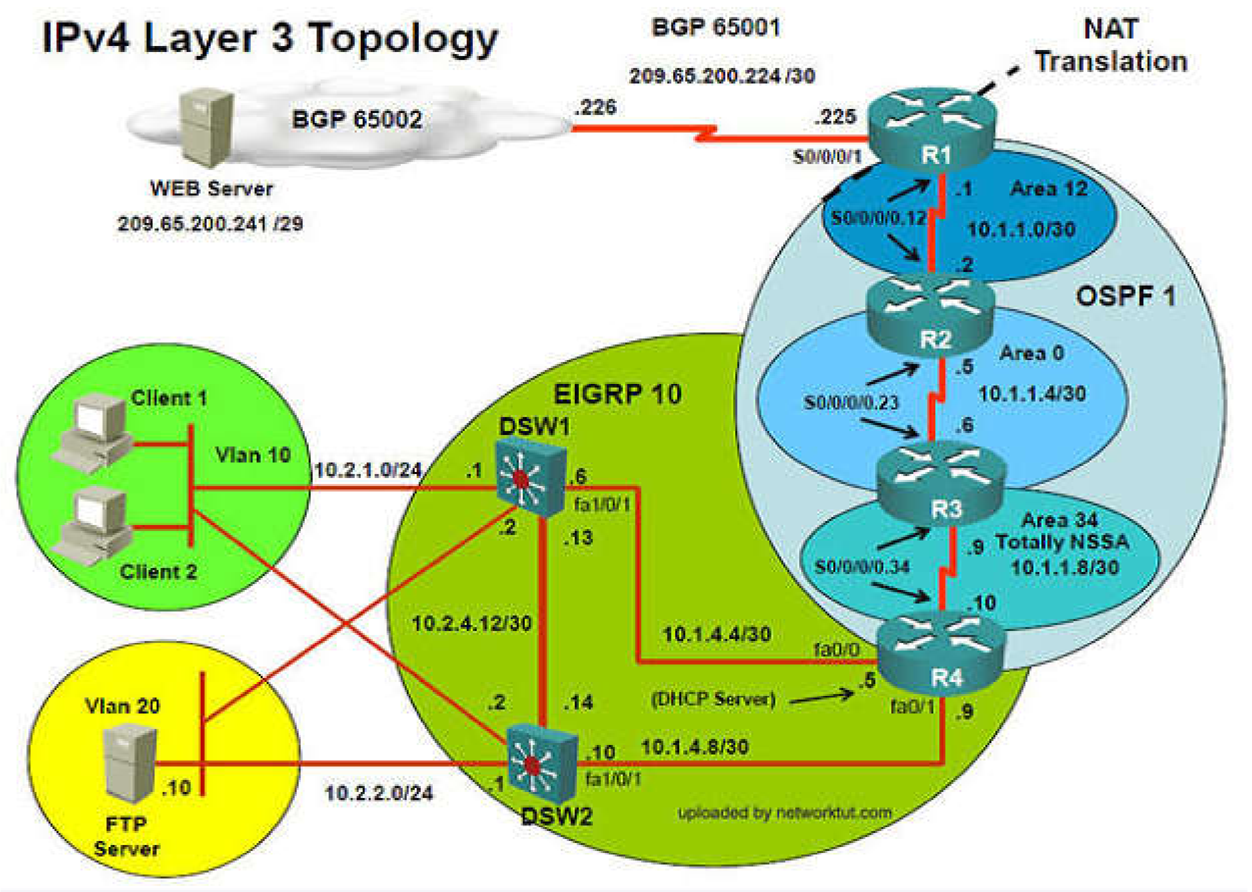
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

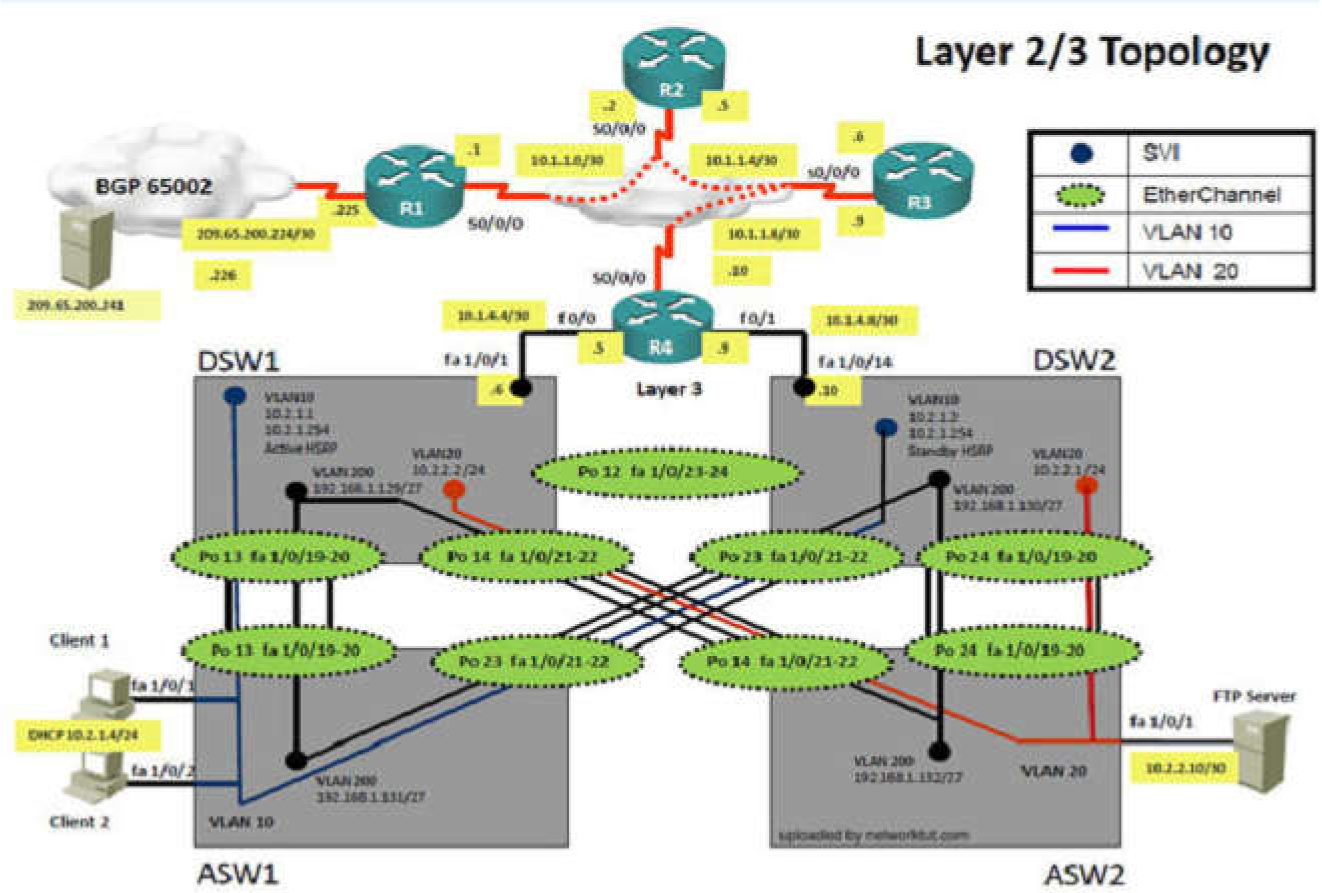
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==





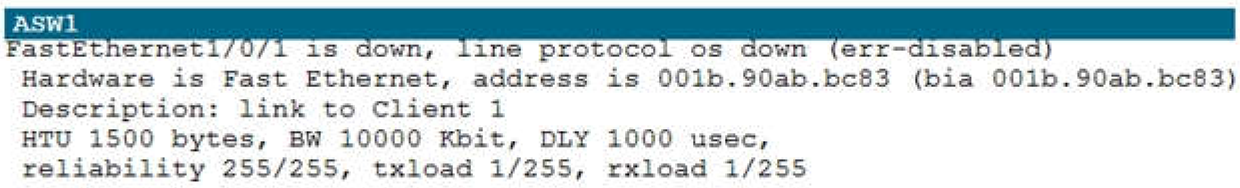
Client is unable to ping IP 209.65.200.241

Solution

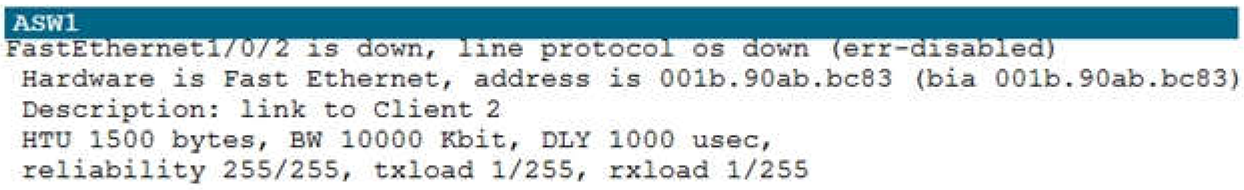
Steps need to follow as below:-

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

2. On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned but when we checked interface it was showing down
Sh run ------- check for running config of int fa1/0/1 & fa1/0/2 (switchport access Vlan 10 will be there with switch port security command). Now check as below
Sh int fa1/0/1 & sh int fa1/0/2



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



```
ASW1
FastEthernet1/0/2 is down, line protocol os down (err-disabled)
 Hardware is Fast Ethernet, address is 001b.90ab.bc83 (bia 001b.90ab.bc83)
 Description: link to Client 2
 HTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
```

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

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
On which device is the fault condition located?

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

Correct Answer: G
Section: [none]
Explanation

Explanation/Reference:
Explanation:
port security needs is configured on ASW1.

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

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

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolated the cause of this fault and answer the following questions.
What is the solution to the fault condition?

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

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
On ASW1, we need to remove port-security under interface fa1/0/1 & fa1/0/2.

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

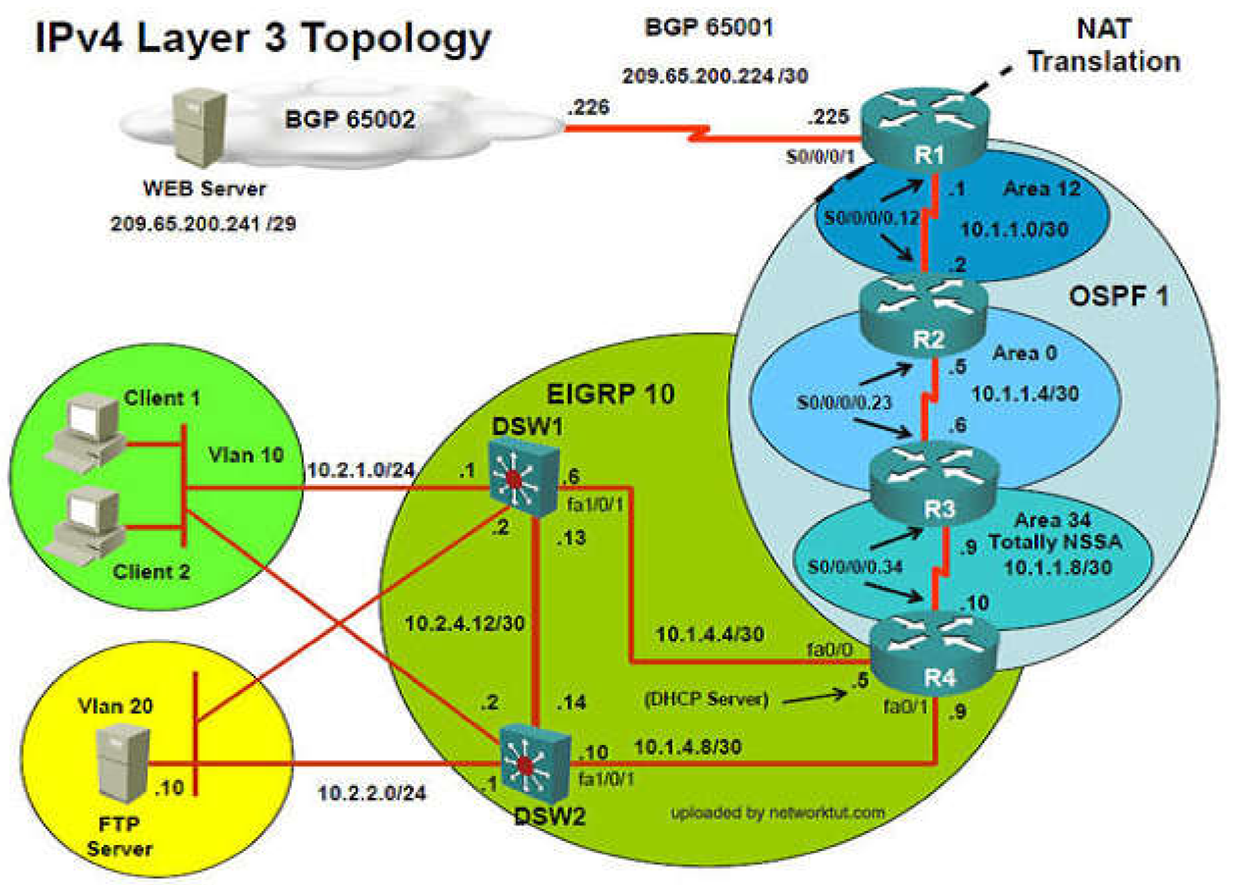
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

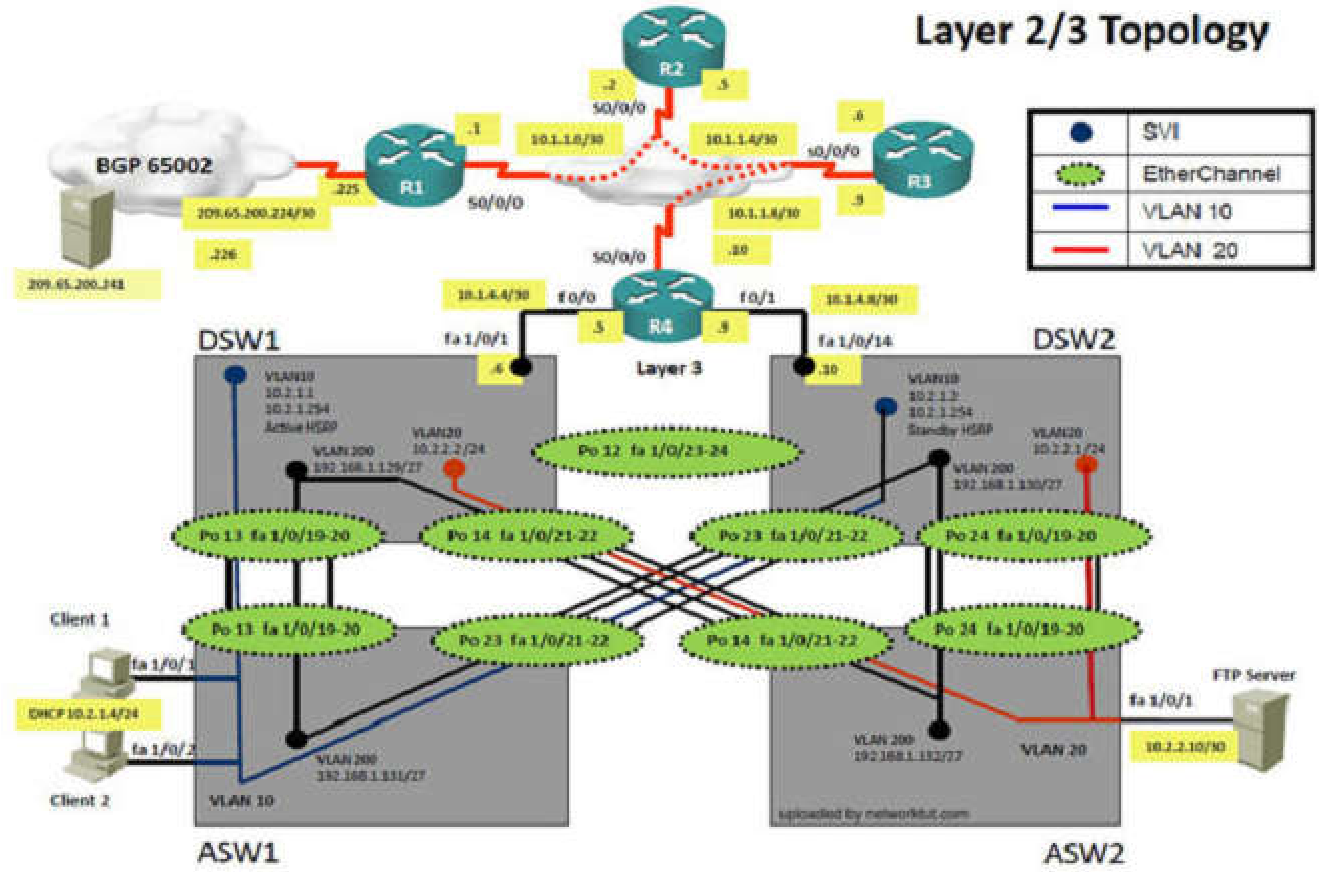
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==



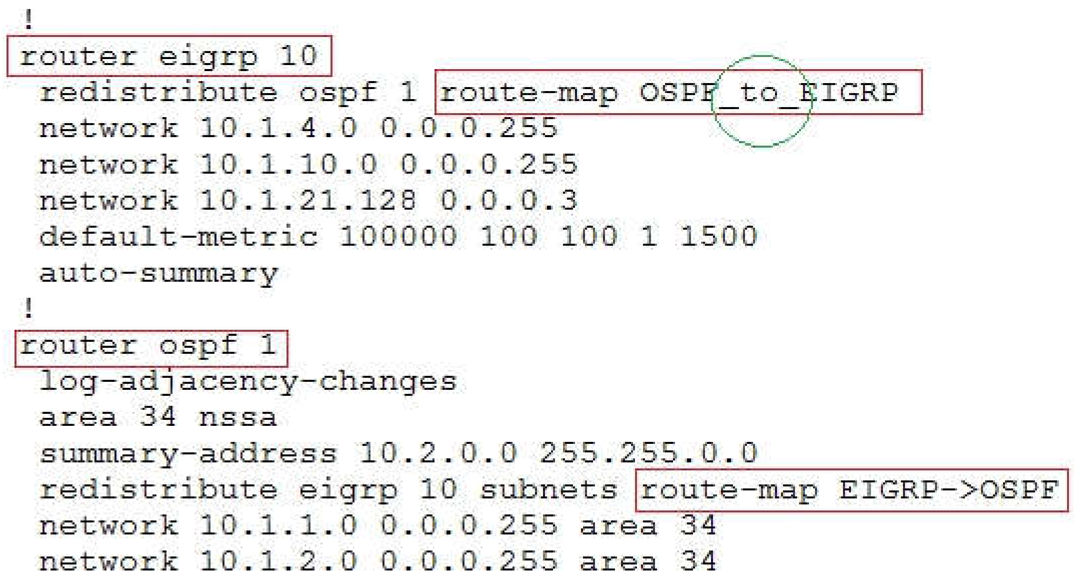


Client is unable to ping IP 209.65.200.241
Solution
Steps need to follow as below:-
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
ipconfig ----- Client will be receiving IP address 10.2.1.3

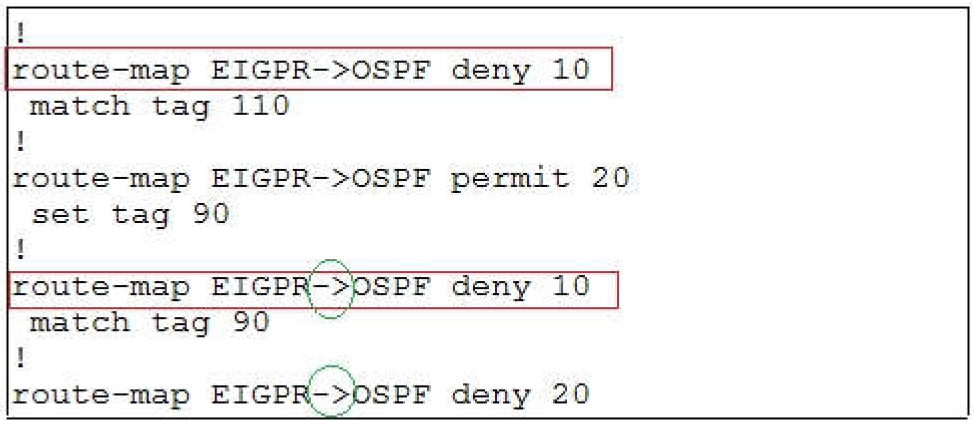
2. IP 10.2.1.3 will be able to ping from R4 , but cannot ping from R3, R2, R1

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

4. Since R4 is able to ping 10.2.1.3 it means that routes are received in EIGRP & same needs to be advertised in OSPF to ping from R3, R2, R1.
5. Need to check the routes are being advertised properly or not in OSPF & EIGRP vice-versa.



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



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

6. From above snap shot it clearly indicates that redistribution done in EIGRP is having problem & by default all routes are denied from ospf to EIGRP… so need to change route-map name.
7. **Change required:** On R4, in the redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue. It references route-map OSPF_to_EIGRP but the actual route map is called OSPF->EIGRP.

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
On which device is the fault condition located?

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

Correct Answer: D
Section: [none]
Explanation

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
The fault condition is related to which technology?

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

Correct Answer: E
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

Which is the solution to the fault condition?

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

Correct Answer: A
Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

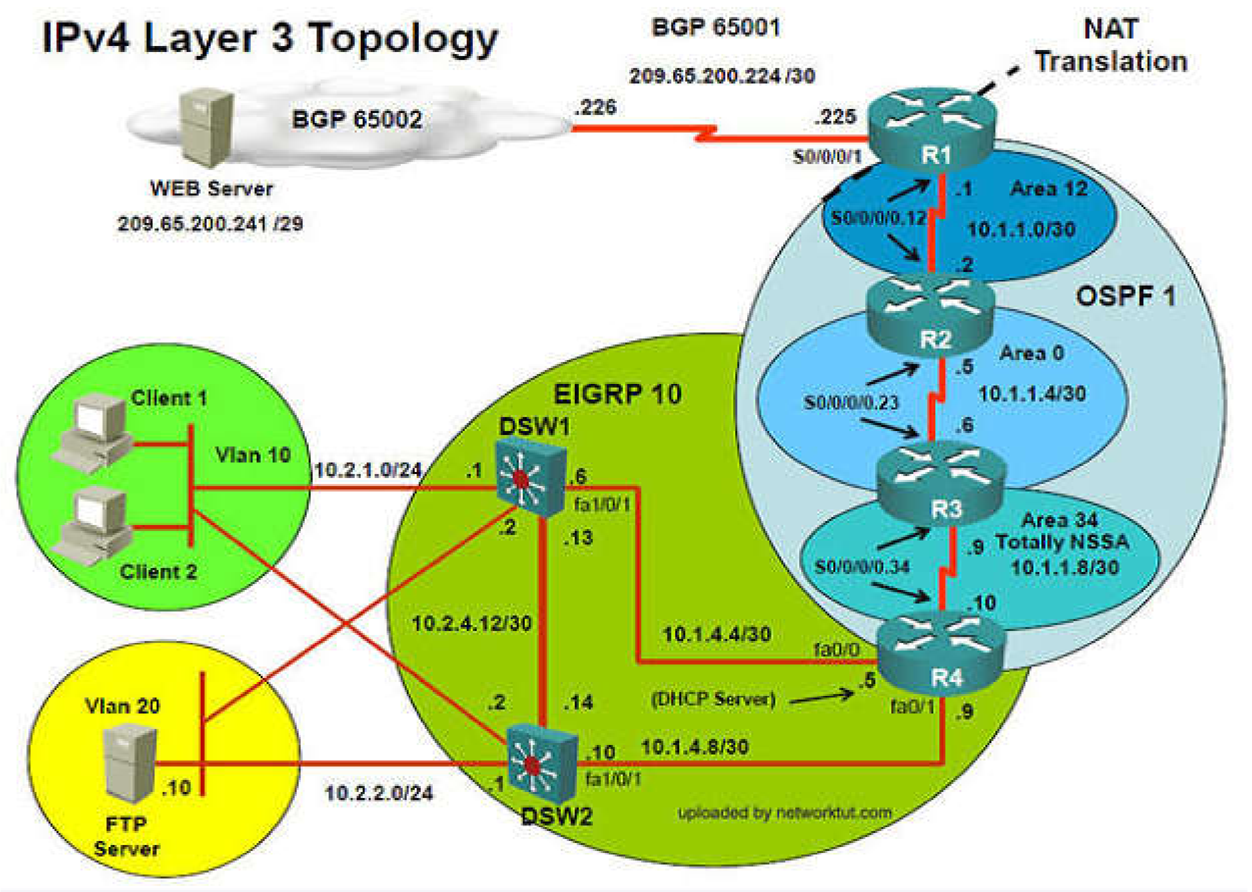
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

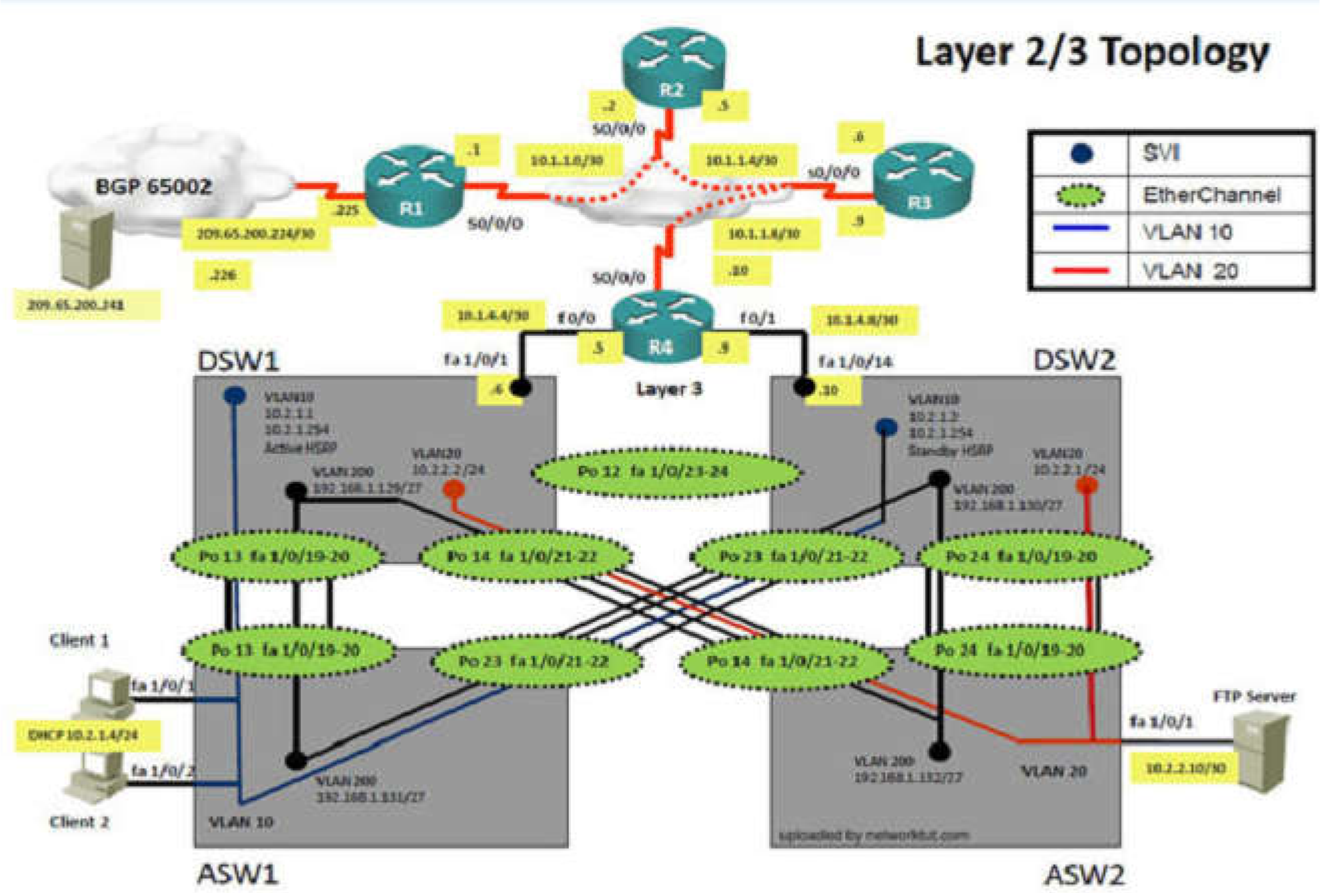
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==





Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

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

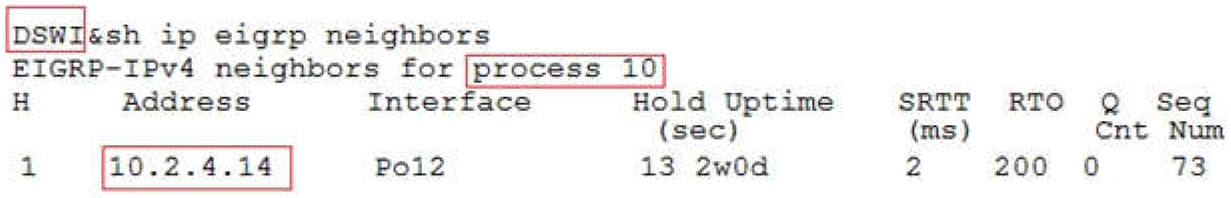
2. From Client PC we can ping 10.2.1.254

3. But IP 10.2.1.3 is not able to ping from R4, R3, R2, R1

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

5. Check the neighborship of EIGRP on R4; there are no neighbor seen from DSW1 & DSW2 check the running config of EIGRP protocol it shows EIGRP AS 1 process…. Now check on DSW1 & DSW2

On DSW1 only one Eigrp neighbour is there with DSW2 but its not with R4…



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

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

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

QUESTION 1

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
On which device is the fault condition located?

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

Correct Answer: D
Section: [none]
Explanation

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
The fault condition is related to which technology?

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

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

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

Correct Answer: C
Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

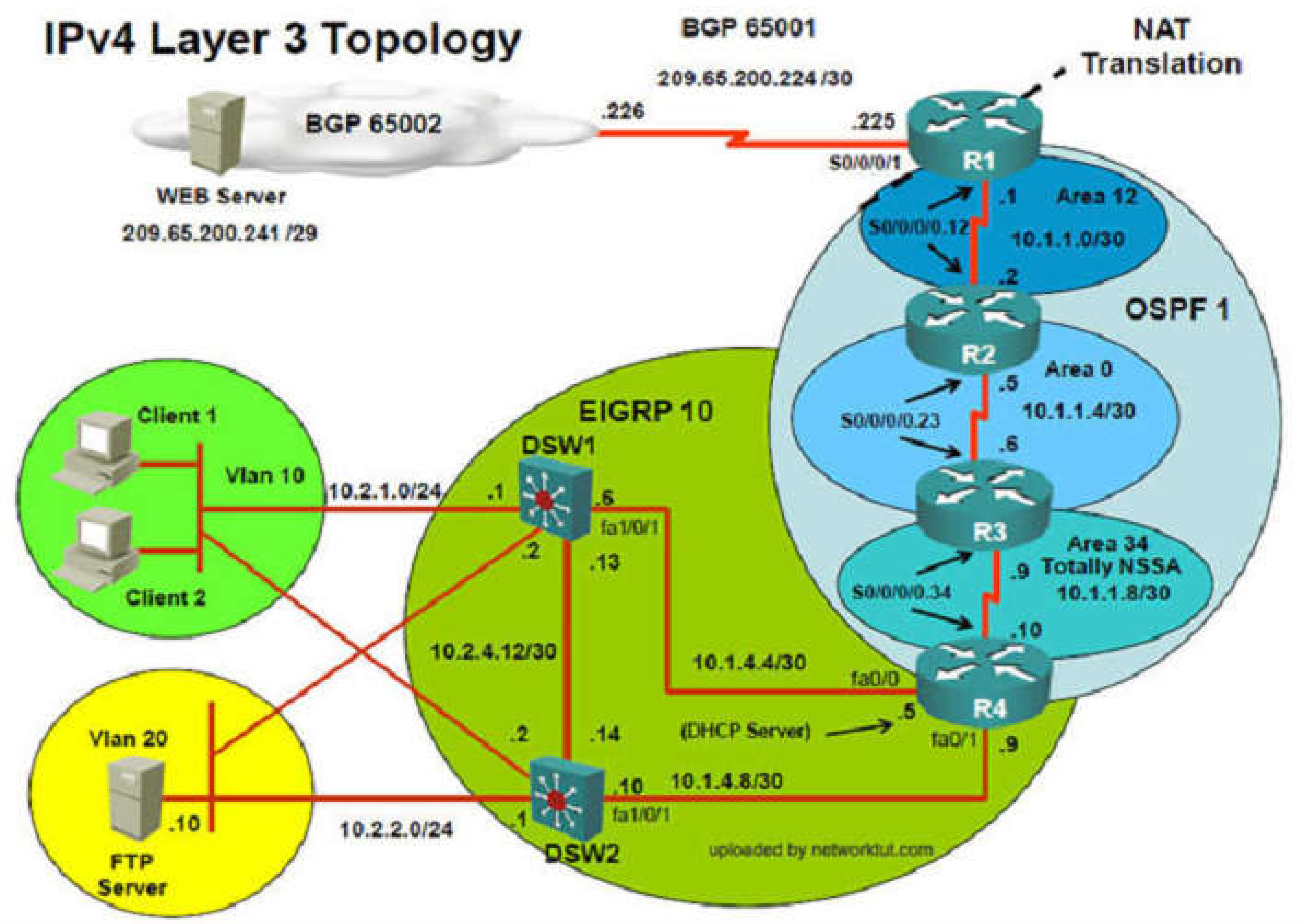
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

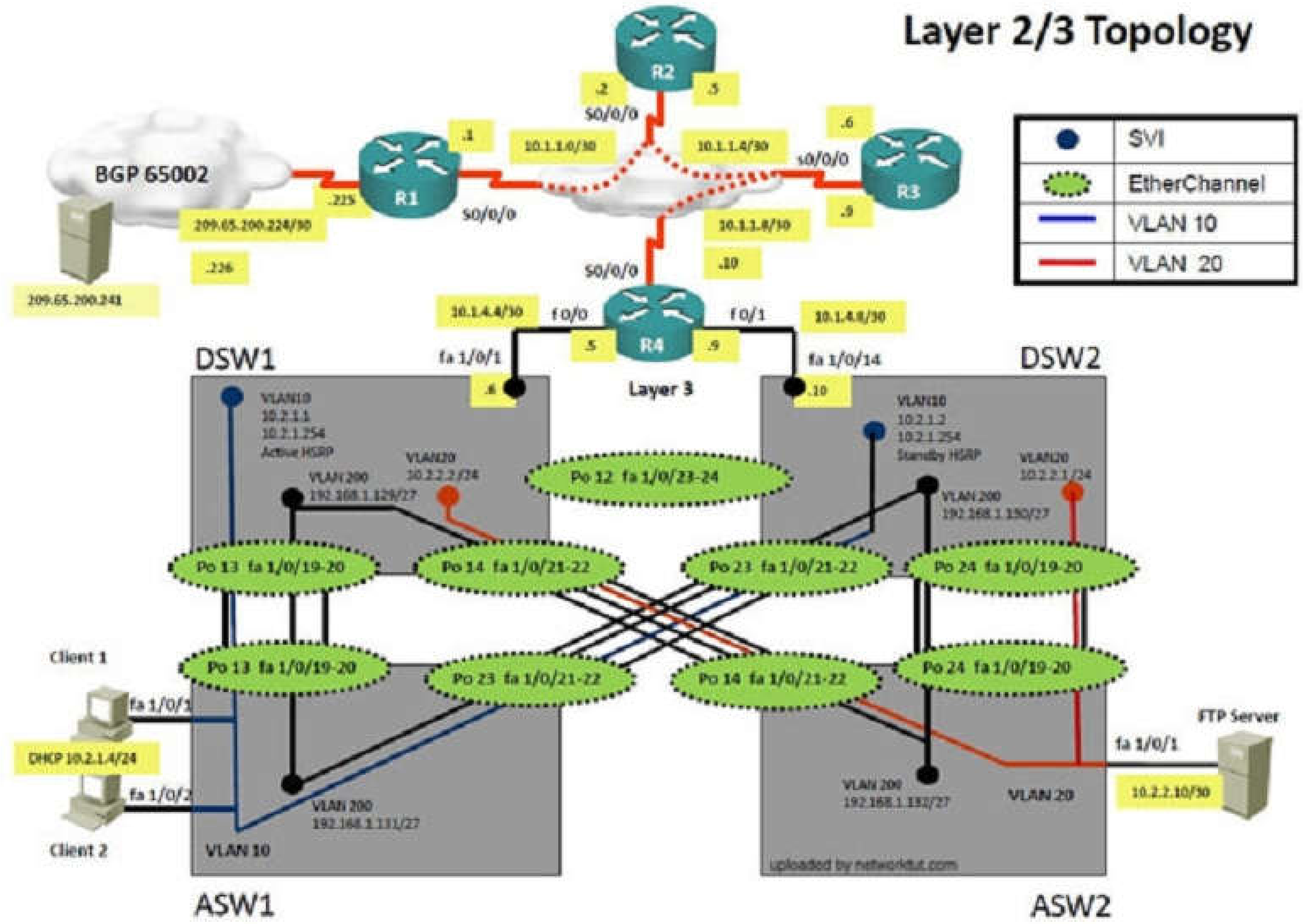
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==





Client 1 is unable to ping IP 209.65.200.241

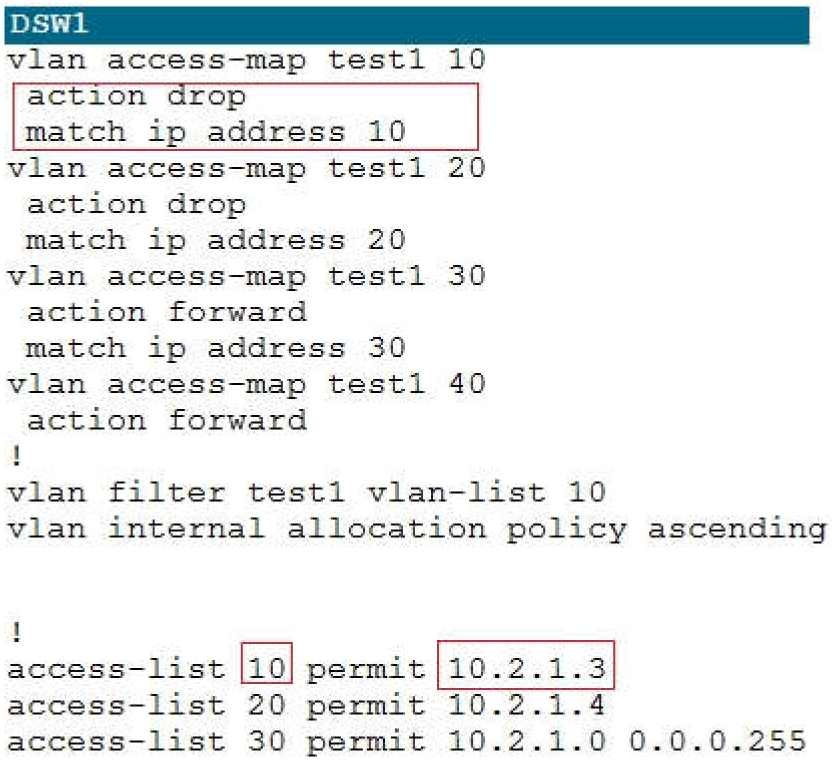
Solution

Steps need to follow as below:-

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

2. From Client PC we can ping 10.2.1.254….

3. But IP 10.2.1.3 is not able to ping from R4, R3, R2, R1



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


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

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
On which device is the fault condition located?

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

Correct Answer: E
Section: [none]
Explanation

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
The fault condition is related to which technology?

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

Correct Answer: J
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to isolated the cause of this fault and answer the following questions.
The fault condition is related to which technology?

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

Correct Answer: C
Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

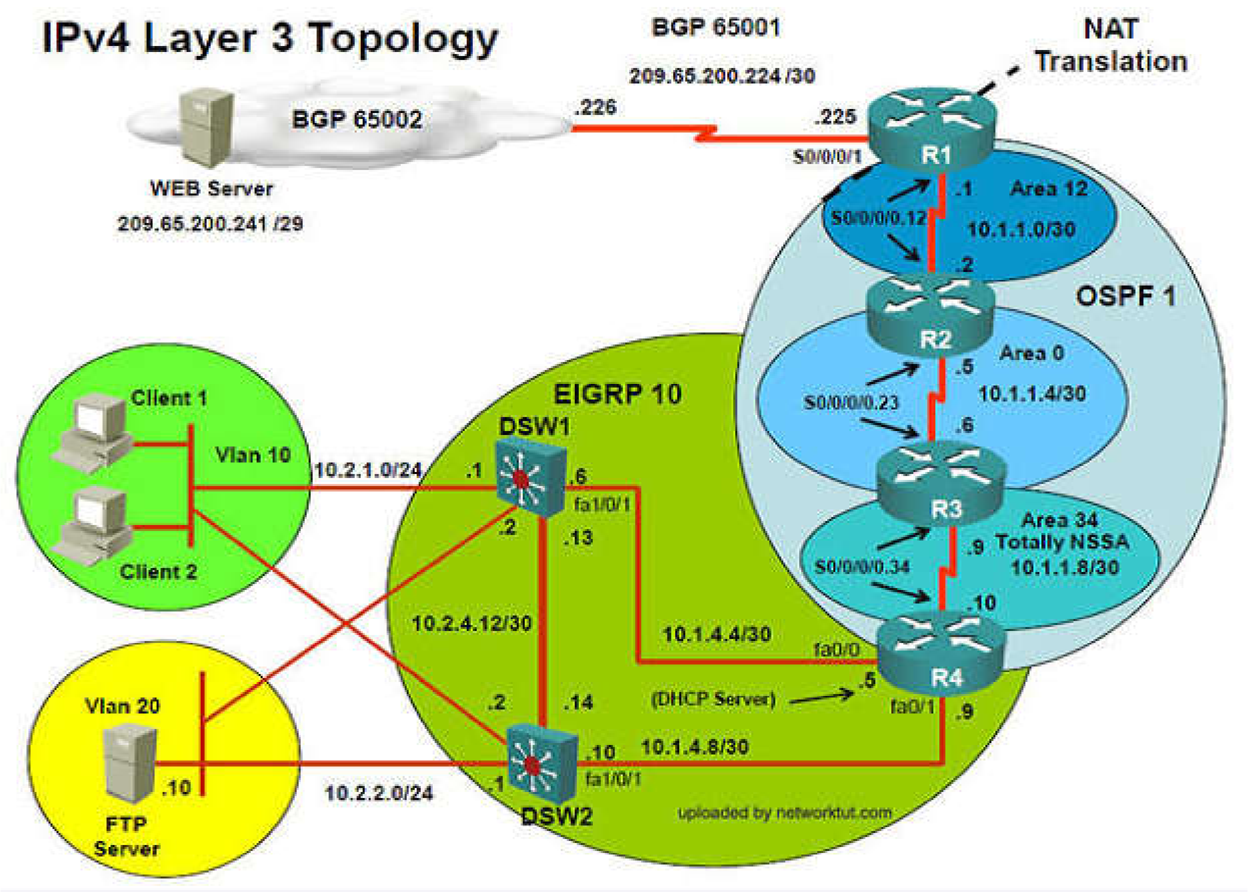
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

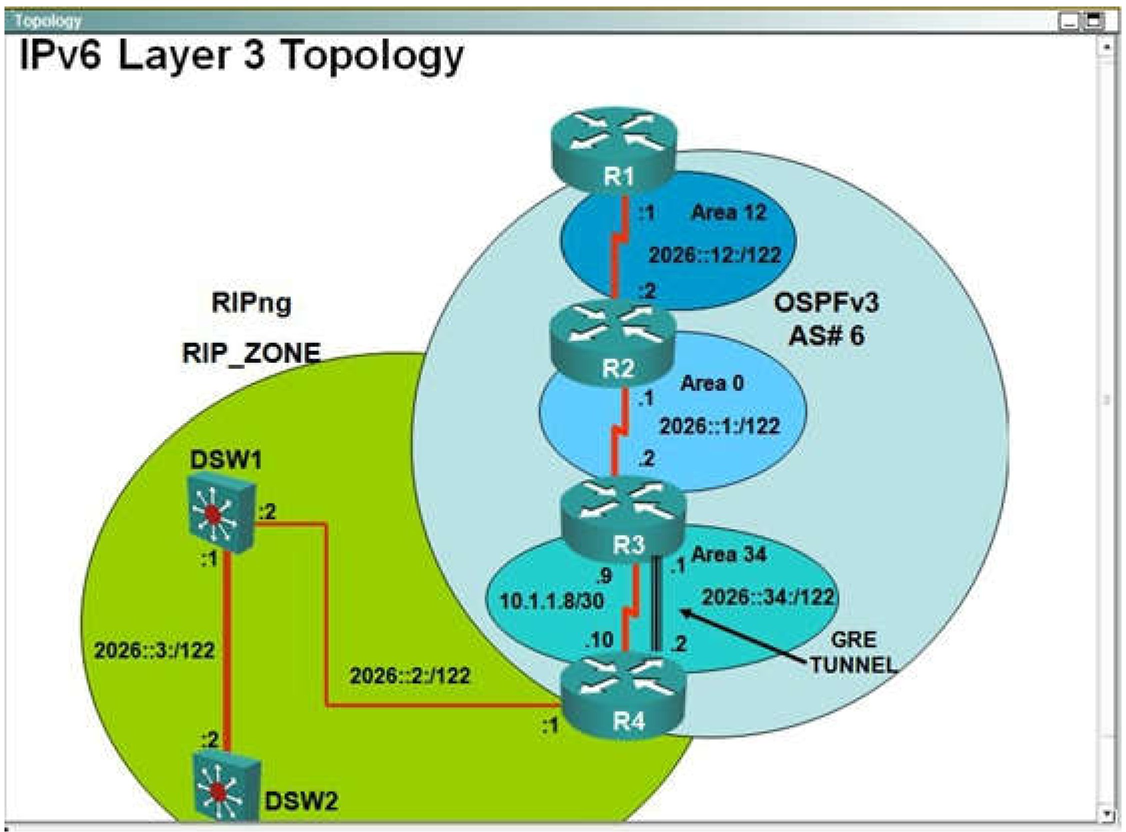
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

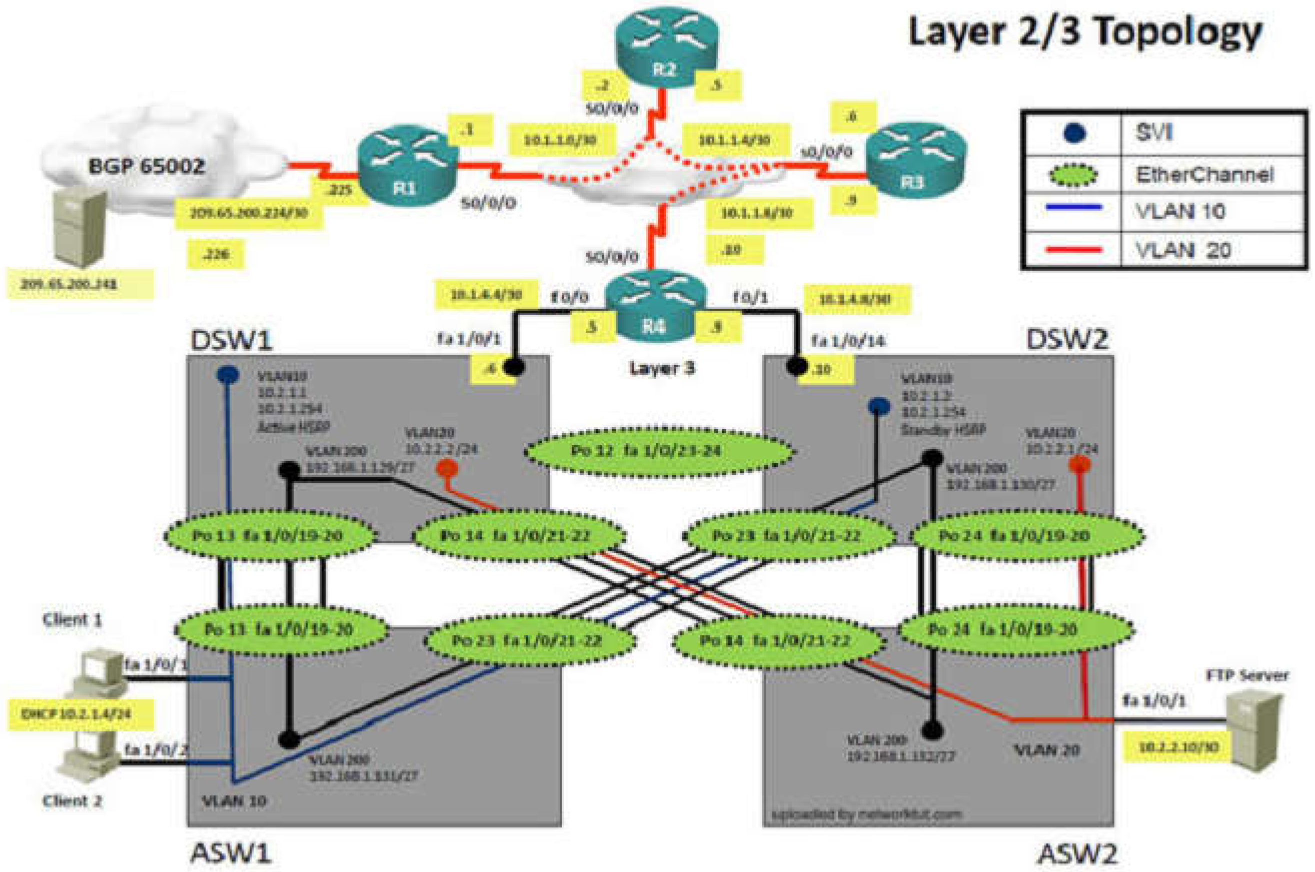
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

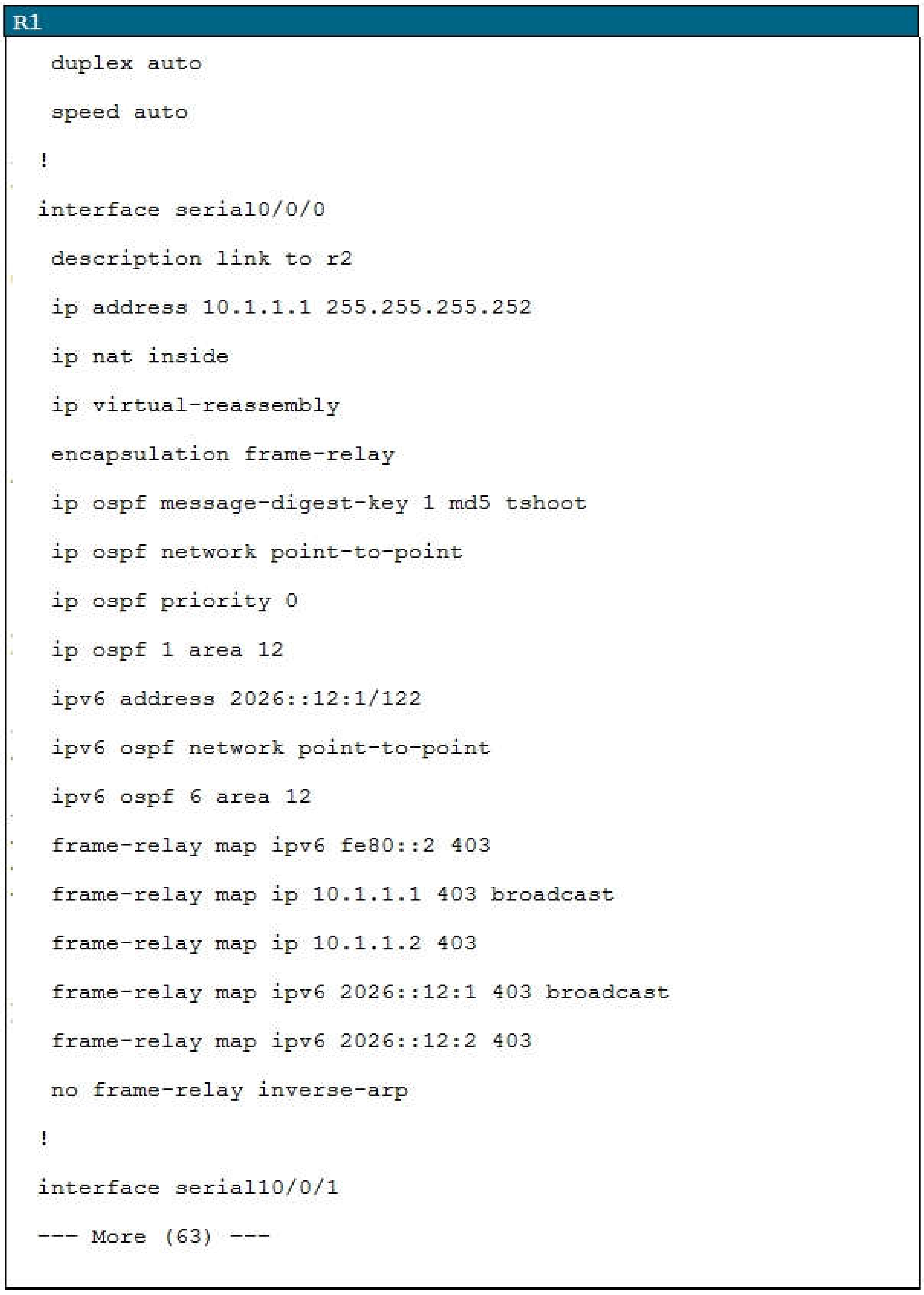
Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==


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

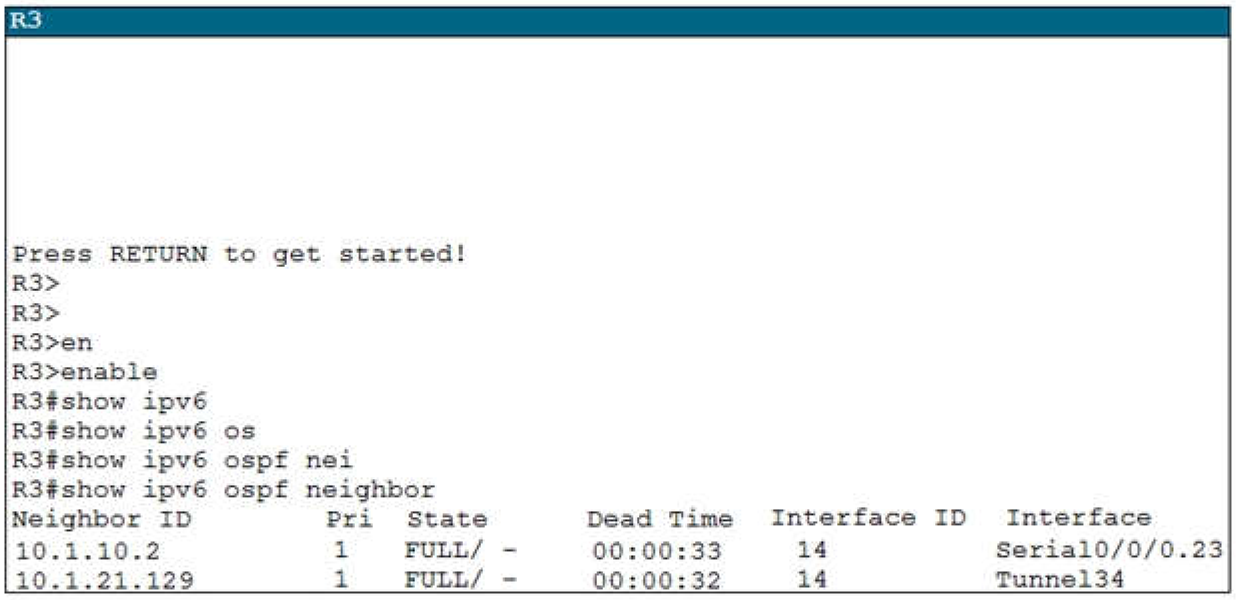

Topology
IPv6 Layer 3 Topology
R1
:1
Area 12
2026::12:/122
:2
OSPFv3
AS# 6
RIPng
RIP_ZONE
R2
Area 0
.1
2026::1:/122
.2
DSW1
:2
:1
R3
Area 34
.9
.1
10.1.1.8/30
2026::34:/122
2026::3:/122
2026::2:/122
.10
.2
GRE
TUNNEL
:1
R4
:2
DSW2


Layer 2/3 Topology
R2
.2
.5
S0/0/0
BGP 65002
.1
10.1.1.0/30
10.1.1.4/30
.6
s0/0/0
R1
R3
.225
S0/0/0
209.65.200.224/30
10.1.1.8/30
.9
.226
.10
209.65.200.241
S0/0/0
10.1.4.4/30
f0/0
f0/1
10.1.4.8/30
R4
.5
.9
DSW1
fa 1/0/1
.6
Layer 3
fa 1/0/14
.10
DSW2
VLAN10
10.2.1.1
10.2.1.254
Active HSRP
VLAN20
10.2.2.2/24
VLAN 200
192.168.1.129/27
Po 12 fa 1/0/23-24
VLAN10
10.2.1.2
10.2.1.254
Standby HSRP
VLAN20
10.2.2.1/24
VLAN 200
192.168.1.130/27
Po 13 fa 1/0/19-20
Po 14 fa 1/0/21-22
Po 23 fa 1/0/21-22
Po 24 fa 1/0/19-20
Client 1
Po 13 fa 1/0/19-20
Po 23 fa 1/0/21-22
Po 14 fa 1/0/21-22
Po 24 fa 1/0/19-20
fa 1/0/1
DHCP 10.2.1.4/24
fa 1/0/2
Client 2
VLAN 200
192.168.1.131/27
VLAN 10
VLAN 200
192.168.1.132/27
VLAN 20
FTP Server
fa 1/0/1
10.2.2.10/30
uploaded by networktut.com
ASW1
ASW2
● SVI
EtherChannel
VLAN 10
VLAN 20



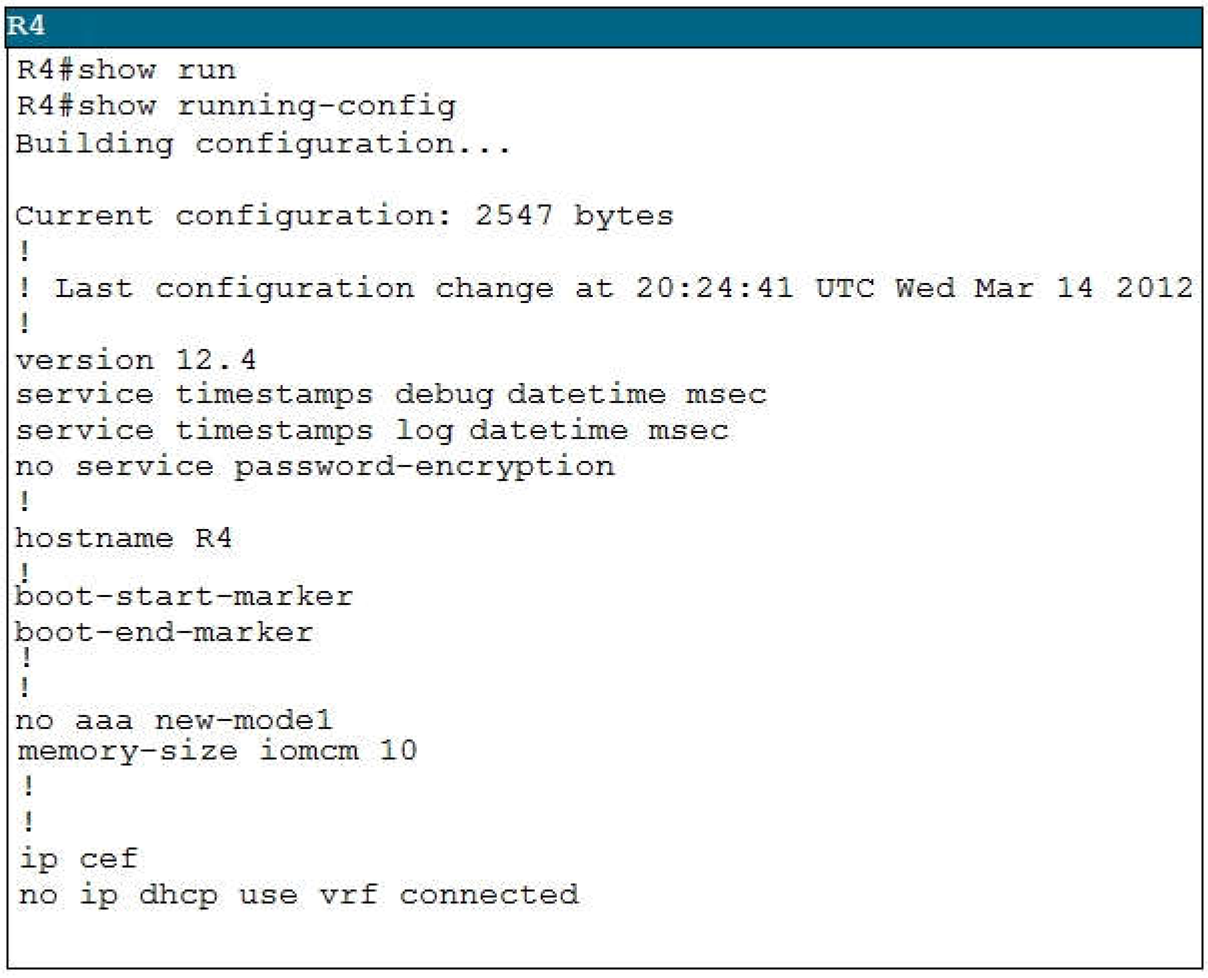
R1

```
  duplex auto
  speed auto
 !
 interface serial0/0/0
  description link to r2
  ip address 10.1.1.1 255.255.255.252
  ip nat inside
  ip virtual-reassembly
  encapsulation frame-relay
  ip ospf message-digest-key 1 md5 tshoot
  ip ospf network point-to-point
  ip ospf priority 0
  ip ospf 1 area 12
  ipv6 address 2026::12:1/122
  ipv6 ospf network point-to-point
  ipv6 ospf 6 area 12
  frame-relay map ipv6 fe80::2 403
  frame-relay map ip 10.1.1.1 403 broadcast
  frame-relay map ip 10.1.1.2 403
  frame-relay map ipv6 2026::12:1 403 broadcast
  frame-relay map ipv6 2026::12:2 403
  no frame-relay inverse-arp
 !
 interface serial10/0/1
 --- More (63) ---
```



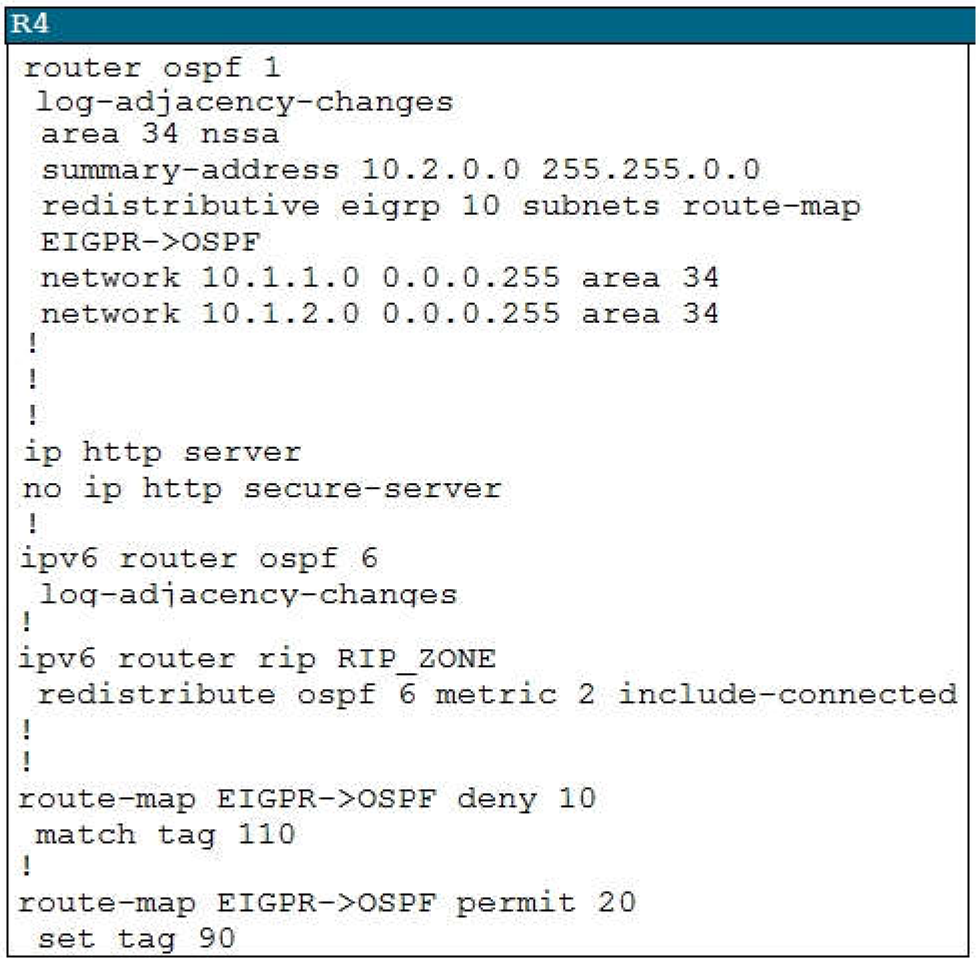
R3

```
Press RETURN to get started!
R3>
R3>
R3>en
R3>enable
R3#show ipv6
R3#show ipv6 os
R3#show ipv6 ospf nei
R3#show ipv6 ospf neighbor
Neighbor ID         Pri   State       Dead Time   Interface ID   Interface
10.1.10.2            1    FULL/ -      00:00:33     14           Serial0/0/0.23
10.1.21.129          1    FULL/ -      00:00:32     14           Tunnel34
```



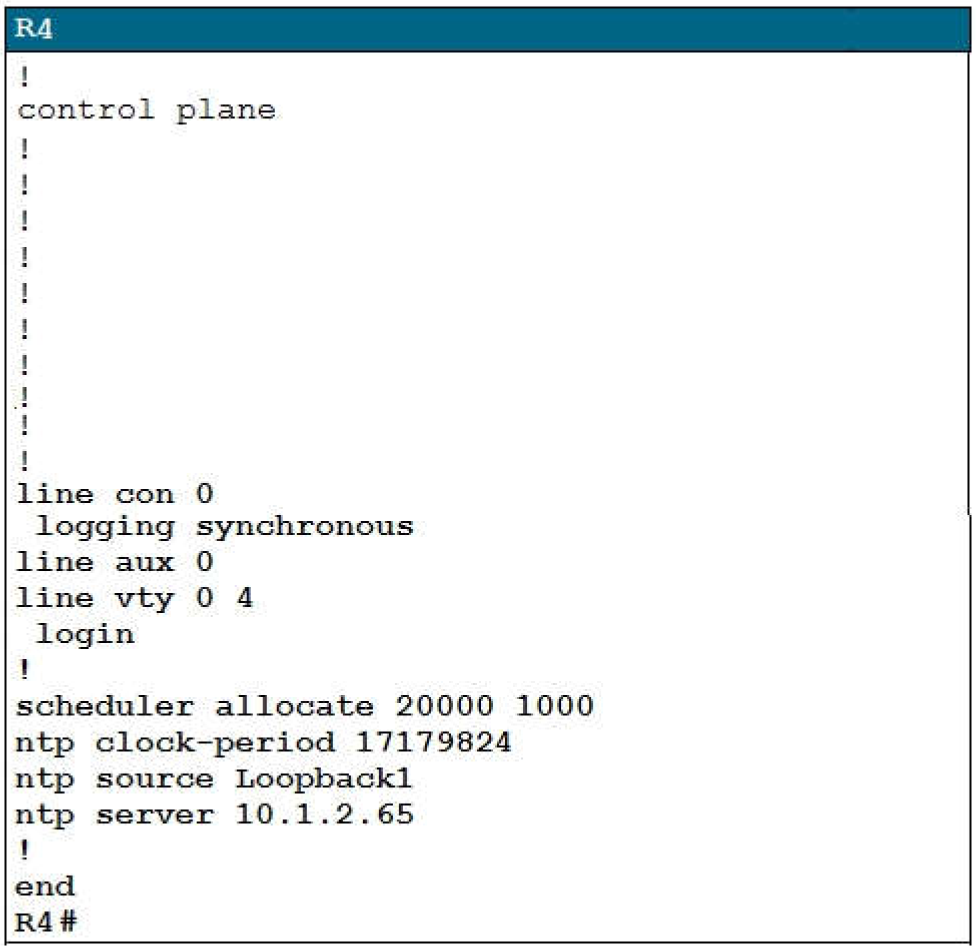
R4

```
R4#show run
R4#show running-config
Building configuration...

Current configuration: 2547 bytes
!
! Last configuration change at 20:24:41 UTC Wed Mar 14 2012
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
no aaa new-mode1
memory-size iomcm 10
!
!
ip cef
no ip dhcp use vrf connected
```

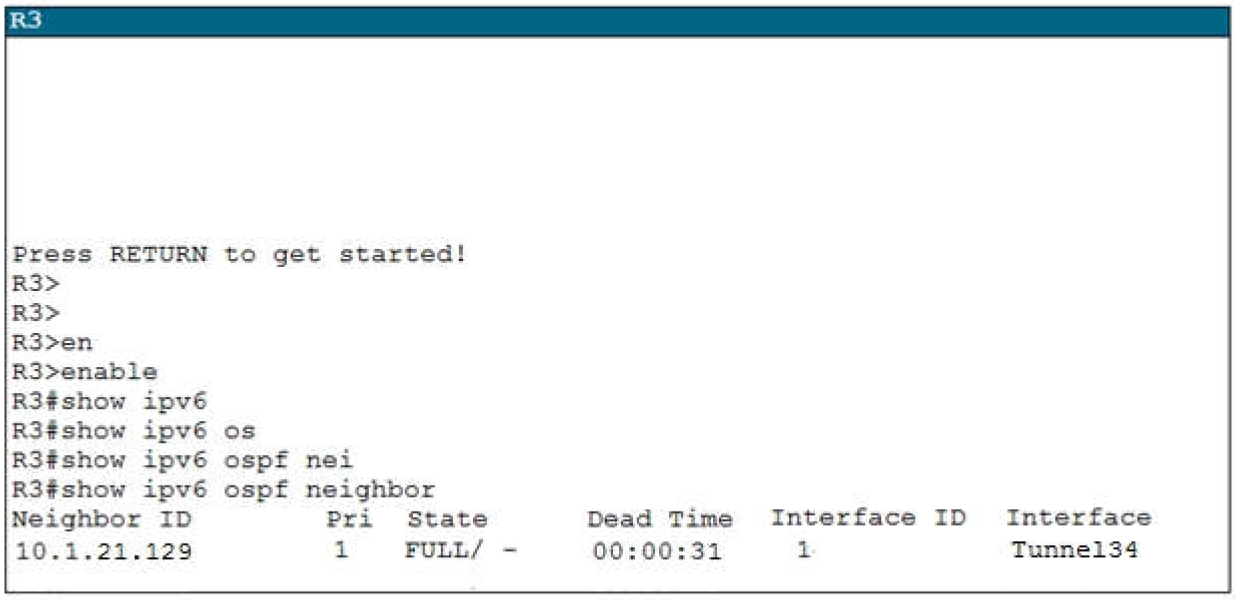


R4

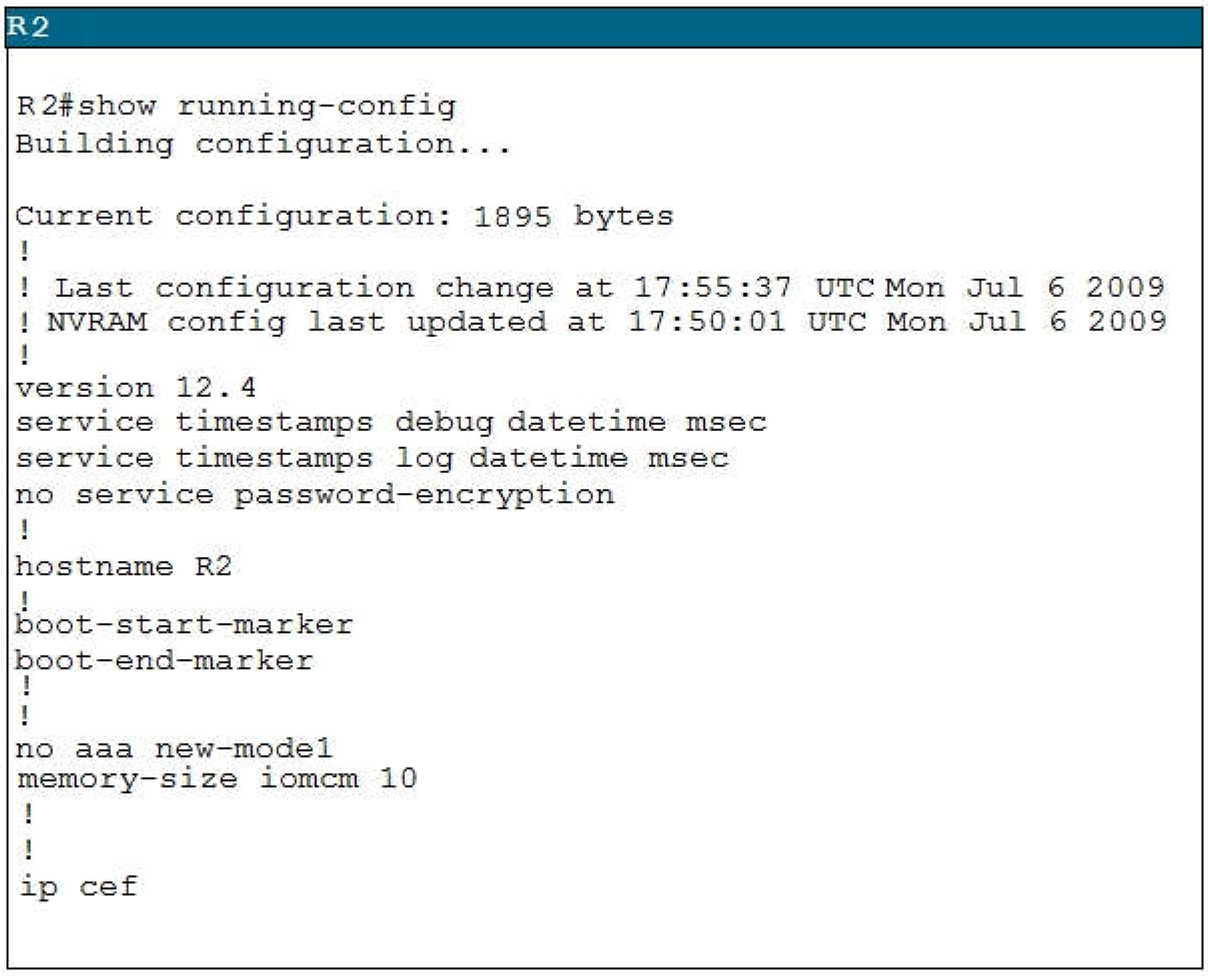
```
router ospf 1
 log-adjacency-changes
 area 34 nssa
 summary-address 10.2.0.0 255.255.0.0
 redistributive eigrp 10 subnets route-map
 EIGPR->OSPF
 network 10.1.1.0 0.0.0.255 area 34
 network 10.1.2.0 0.0.0.255 area 34
!
!
!
ip http server
no ip http secure-server
!
ipv6 router ospf 6
 log-adjacency-changes
!
ipv6 router rip RIP_ZONE
 redistribute ospf 6 metric 2 include-connected
!
!
route-map EIGPR->OSPF deny 10
 match tag 110
!
route-map EIGPR->OSPF permit 20
 set tag 90
```



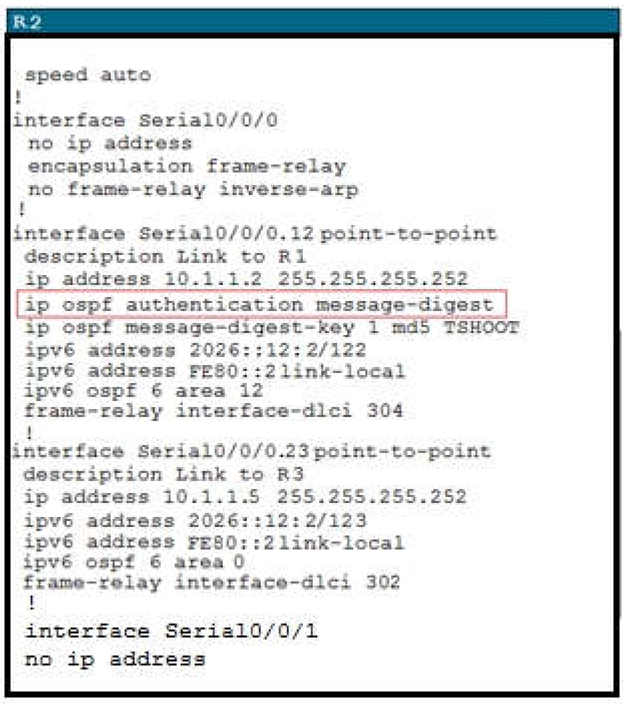
```
!
control plane
!
!
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
ntp clock-period 17179824
ntp source Loopback1
ntp server 10.1.2.65
!
end
R4#
```



```
Press RETURN to get started!
R3>
R3>
R3>en
R3>enable
R3#show ipv6
R3#show ipv6 os
R3#show ipv6 ospf nei
R3#show ipv6 ospf neighbor
Neighbor ID      Pri  State       Dead Time   Interface ID   Interface
10.1.21.129       1   FULL/ -     00:00:31     1             Tunnel34
```

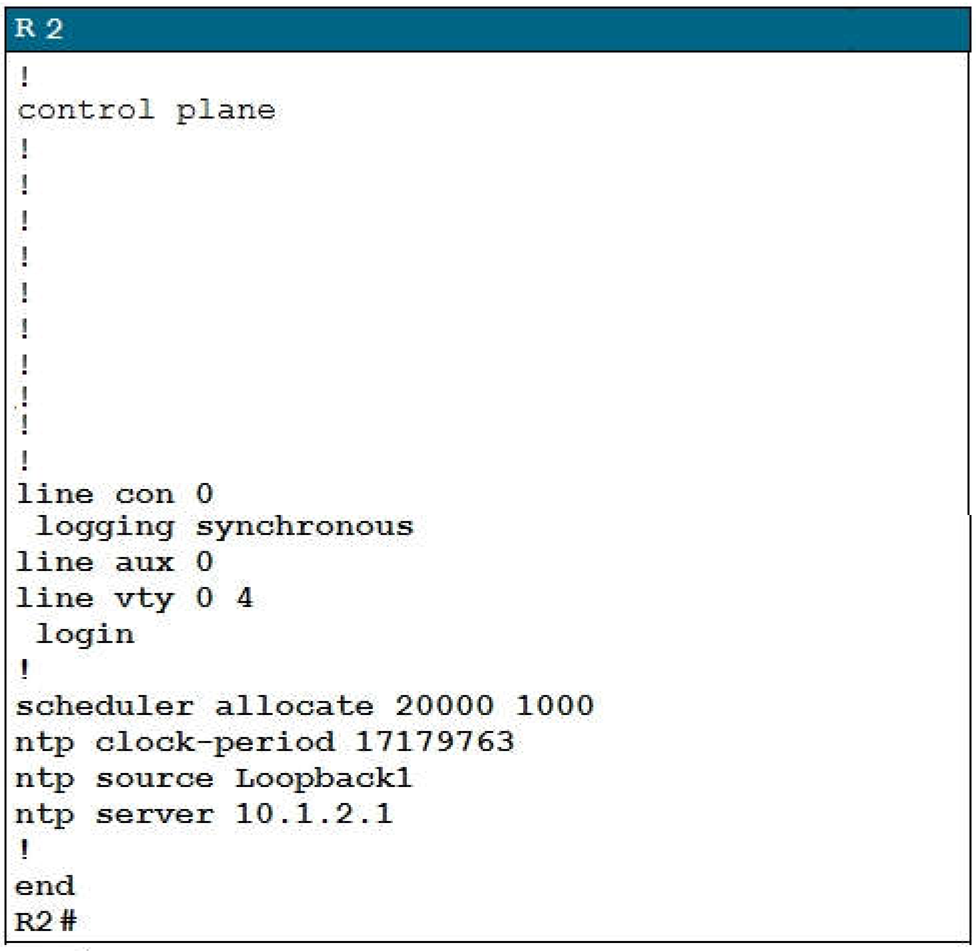


```
R2#show running-config
Building configuration...

Current configuration: 1895 bytes
!
! Last configuration change at 17:55:37 UTC Mon Jul 6 2009
! NVRAM config last updated at 17:50:01 UTC Mon Jul 6 2009
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-mode1
memory-size iomcm 10
!
!
ip cef
```



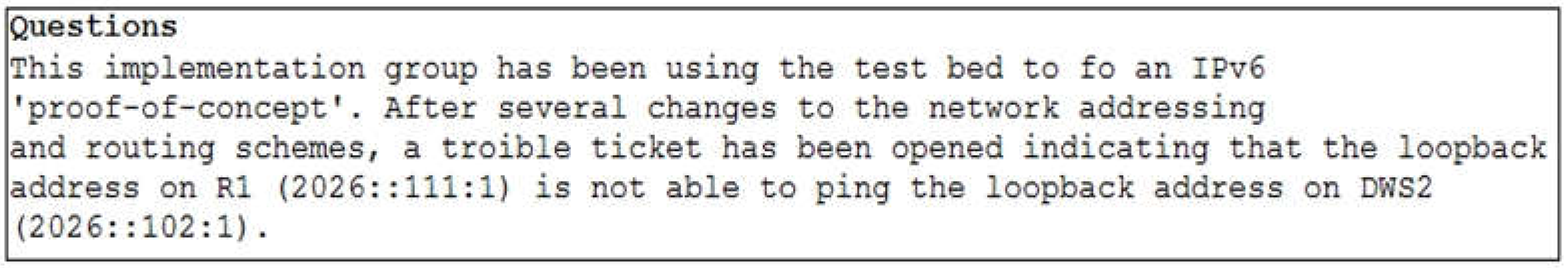
R2

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



R 2

```
!
control plane
!
!
!
!
!
!
!
!
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
ntp clock-period 17179763
ntp source Loopback1
ntp server 10.1.2.1
!
end
R2#
```



```
Questions
This implementation group has been using the test bed to fo an IPv6
'proof-of-concept'. After several changes to the network addressing
and routing schemes, a troible ticket has been opened indicating that the loopback
address on R1 (2026::111:1) is not able to ping the loopback address on DWS2
(2026::102:1).
```

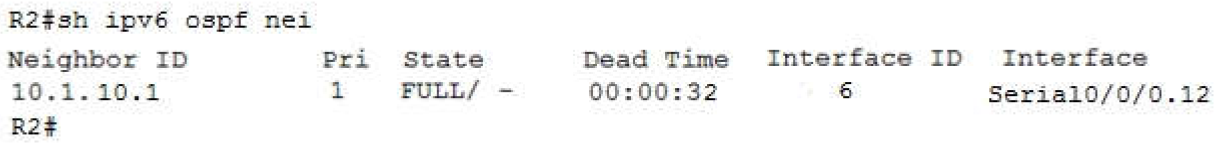
Solution
Steps need to follow as below:-
1. When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4
   ipconfig ----- Client will be receiving IP address 10.2.1.3

2. From Client PC we can ping 10.2.1.254….

3. But IP 10.2.1.3 is able to ping from R4, R3, R2, R1.

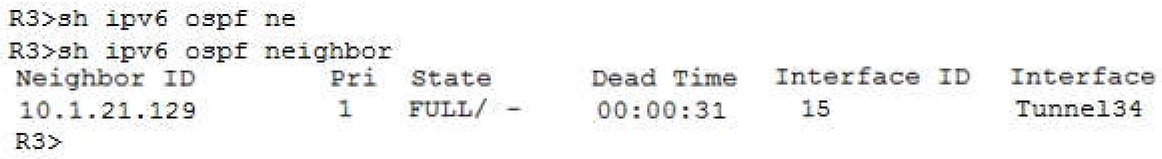
4. Since the problem is R1 (**2026::111:1**) is not able to ping loopback of DSW1 (**2026::102:1**).

5. Kindly check for neighbourship of routers as IPV6…. As per design below neighbourship should be present for IPV6
R1 ---R2 --- R3 --- R4--- DSW1 & DSW2 ----- Neighbourship between devices of IPV6



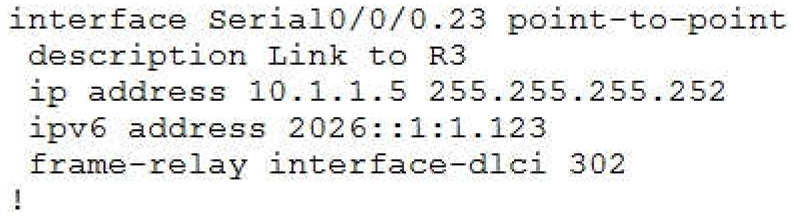
```
R2#sh ipv6 ospf nei
Neighbor ID       Pri  State       Dead Time   Interface ID   Interface
10.1.10.1          1   FULL/ -     00:00:32         6         Serial0/0/0.12
R2#
```

R2 IPV6 OSPF neighbourship is with R1

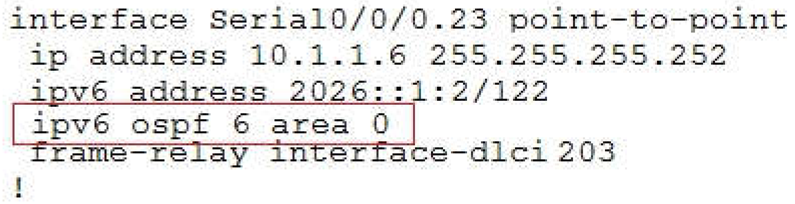


```
R3>sh ipv6 ospf ne
R3>sh ipv6 ospf neighbor
 Neighbor ID        Pri  State      Dead Time  Interface ID  Interface
 10.1.21.129         1   FULL/ -    00:00:31     15          Tunnel34
 R3>
```

R3 IPV6 OSPF neighbourship is with R4



```
interface Serial0/0/0.23 point-to-point
 description Link to R3
 ip address 10.1.1.5 255.255.255.252
 ipv6 address 2026::1:1.123
 frame-relay interface-dlci 302
!
```



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

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

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
On which device is the fault condition located?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 2
The implementations group has been using the test bed to do a ‘proof-of-concept’. After several changes to the network addressing, routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2(2026::102:1).

Use the supported commands to isolated the cause of this fault and answer the following questions.
The fault condition is related to which technology?

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

Correct Answer: C
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a ‘proof-of-concept’. After several changes to the network addressing, routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2(2026::102:1).

Use the supported commands to isolated the cause of this fault and answer the following questions.
What is the solution to fault condition?

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

Correct Answer: A

Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

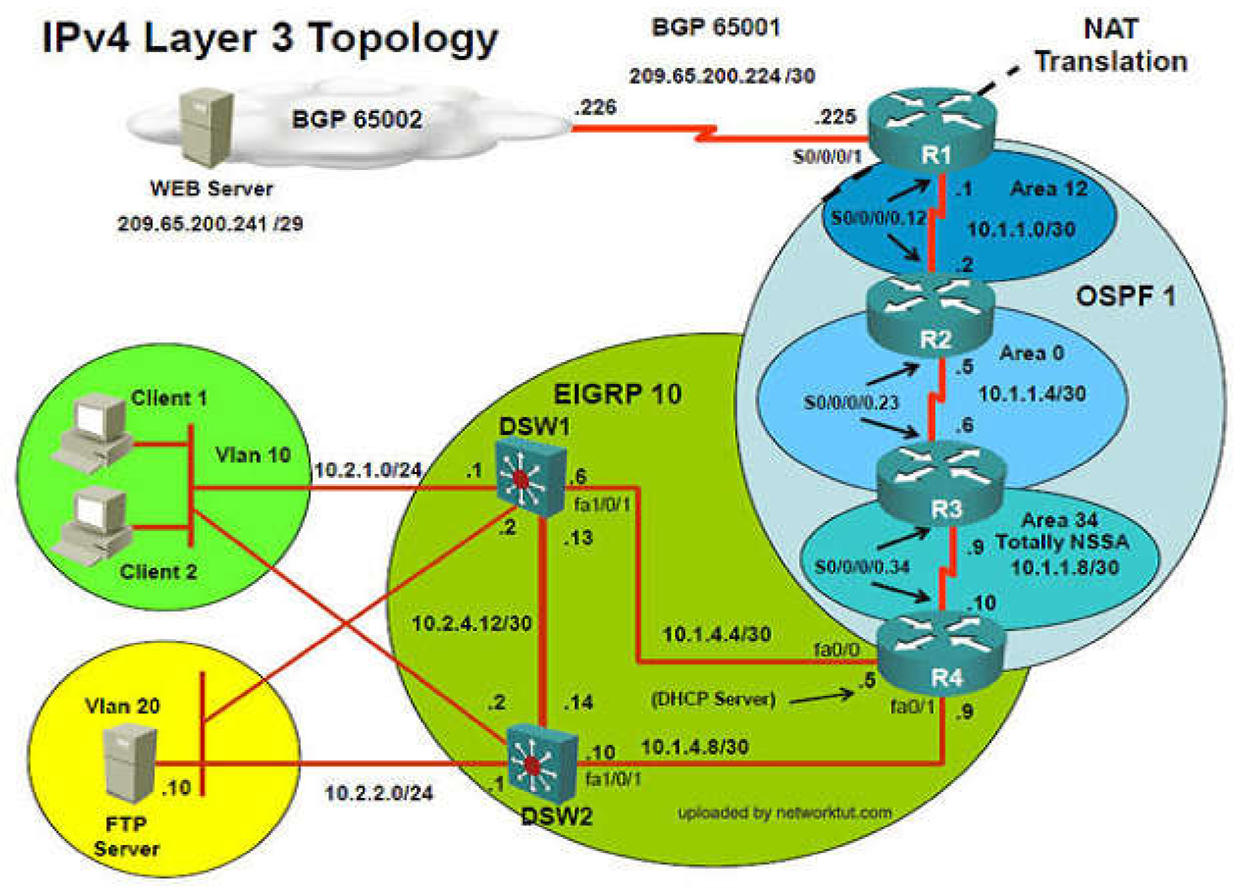
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

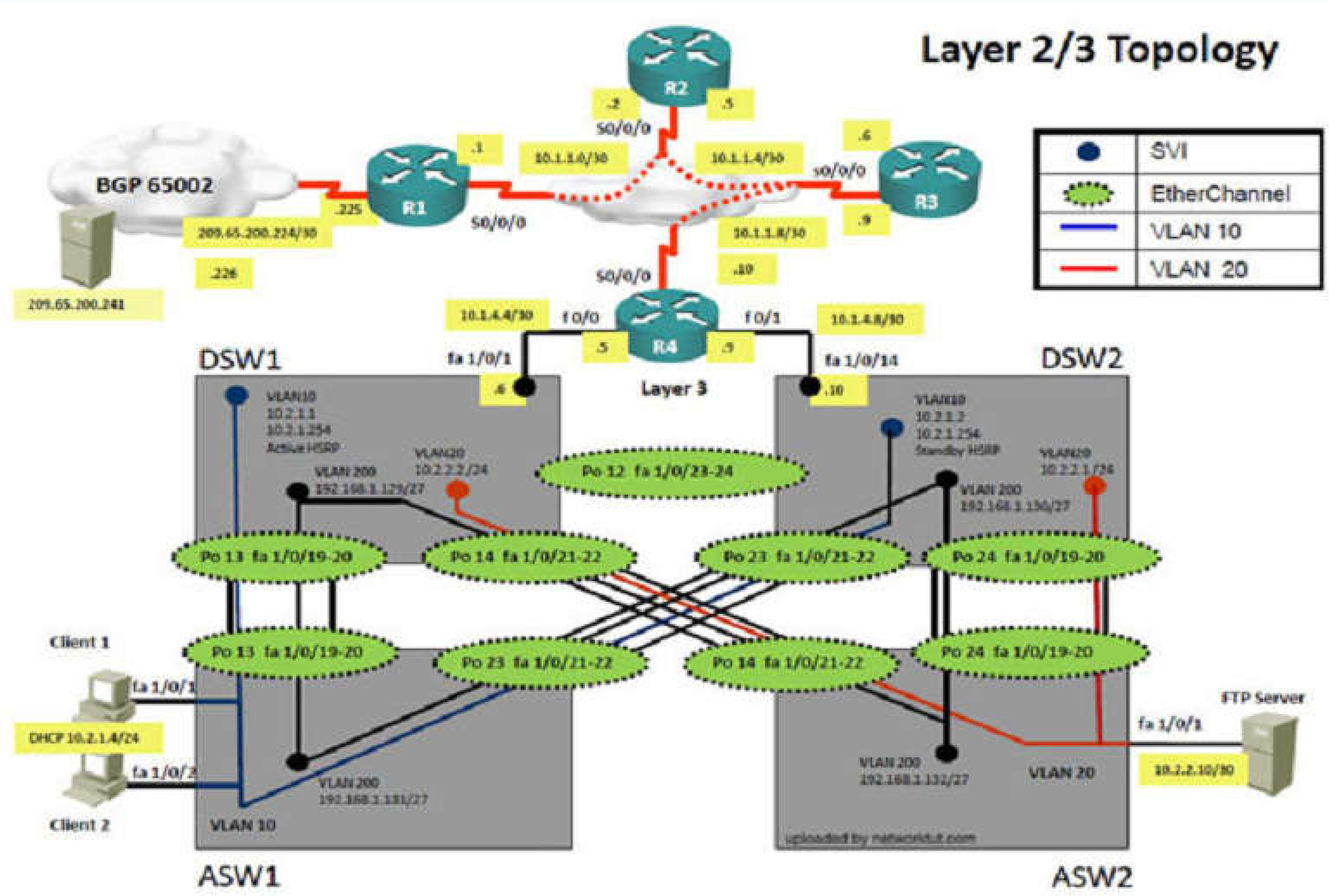
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

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

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==



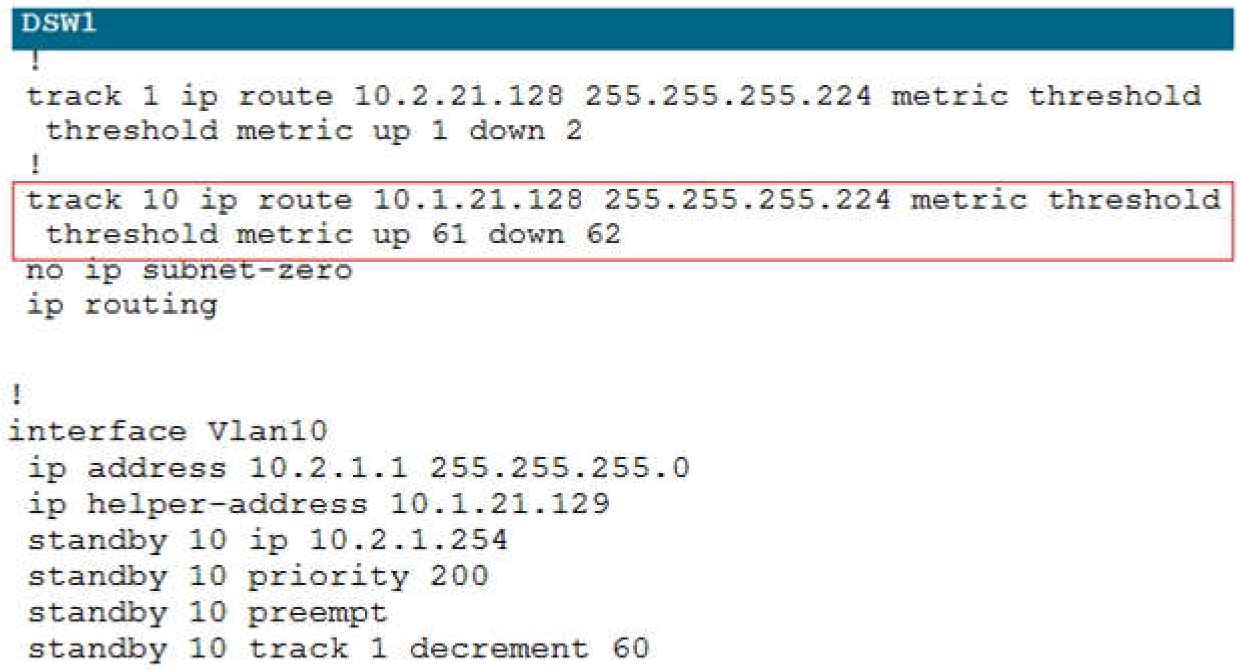


The implementation group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services layer 2 connectivity. FHRP services, and,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

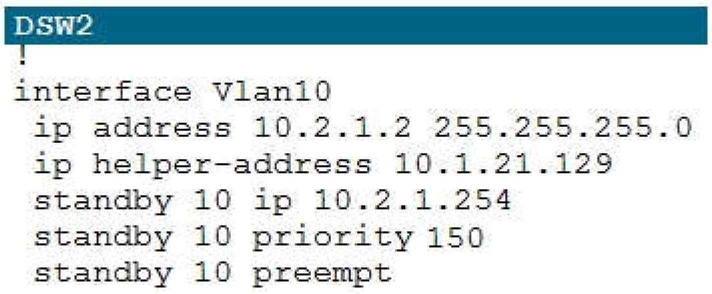
Solution

Steps need to follow as below:-

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



```
DSW1
 !
 track 1 ip route 10.2.21.128 255.255.255.224 metric threshold
  threshold metric up 1 down 2
 !
 track 10 ip route 10.1.21.128 255.255.255.224 metric threshold
  threshold metric up 61 down 62
 no ip subnet-zero
 ip routing


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



```
DSW2
 !
 interface Vlan10
  ip address 10.2.1.2 255.255.255.0
  ip helper-address 10.1.21.129
  standby 10 ip 10.2.1.254
  standby 10 priority 150
  standby 10 preempt
```

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

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

Use the supported commands to isolated the cause of this fault and answer the following questions.
On which device is the fault condition located?

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

Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:
Explanation:
DSW references the wrong track ID number.

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

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

The fault condition is related to which technology?

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

Correct Answer: B
Section: [none]

Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened DSW1 will not become the active router for HSRP group 10.

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

What is the solution to the fault condition?

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

Correct Answer: D
Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

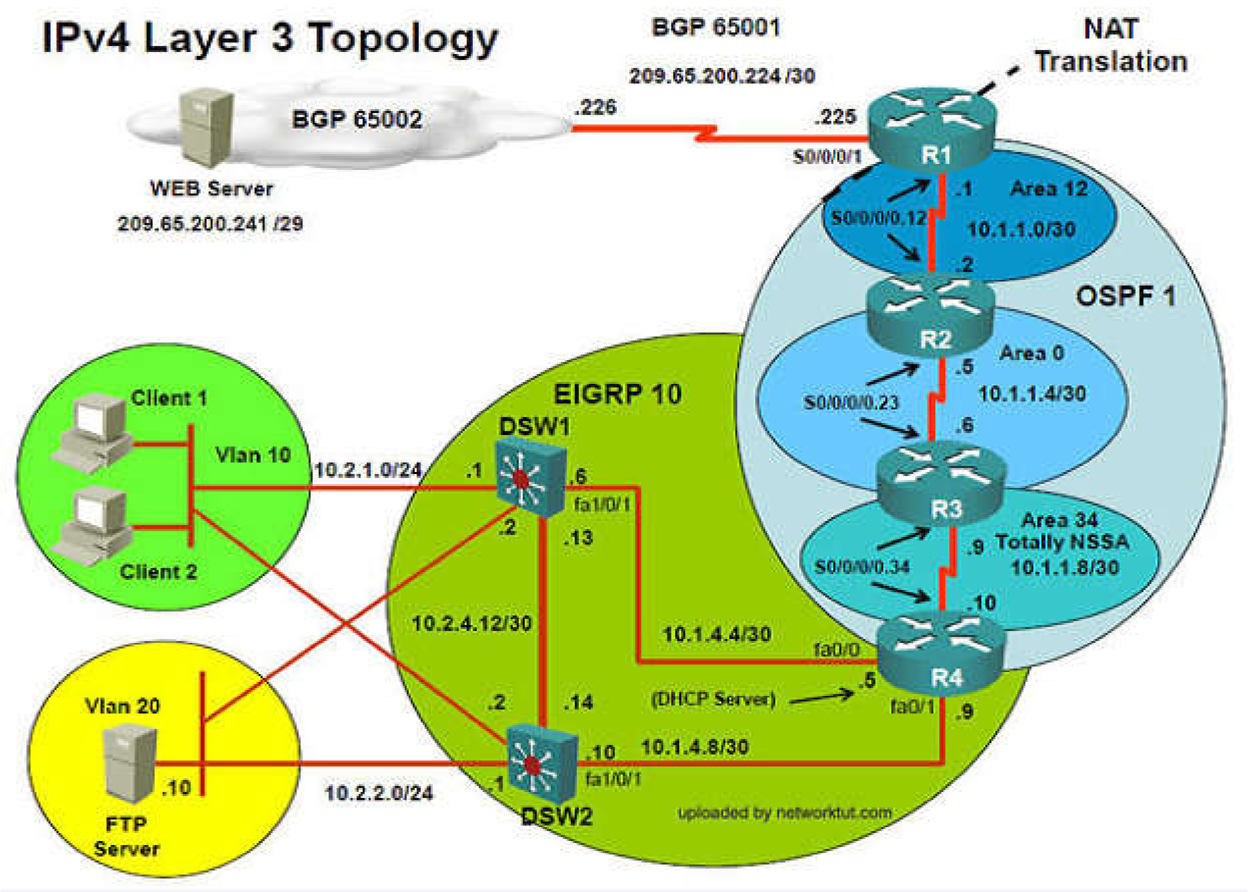
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

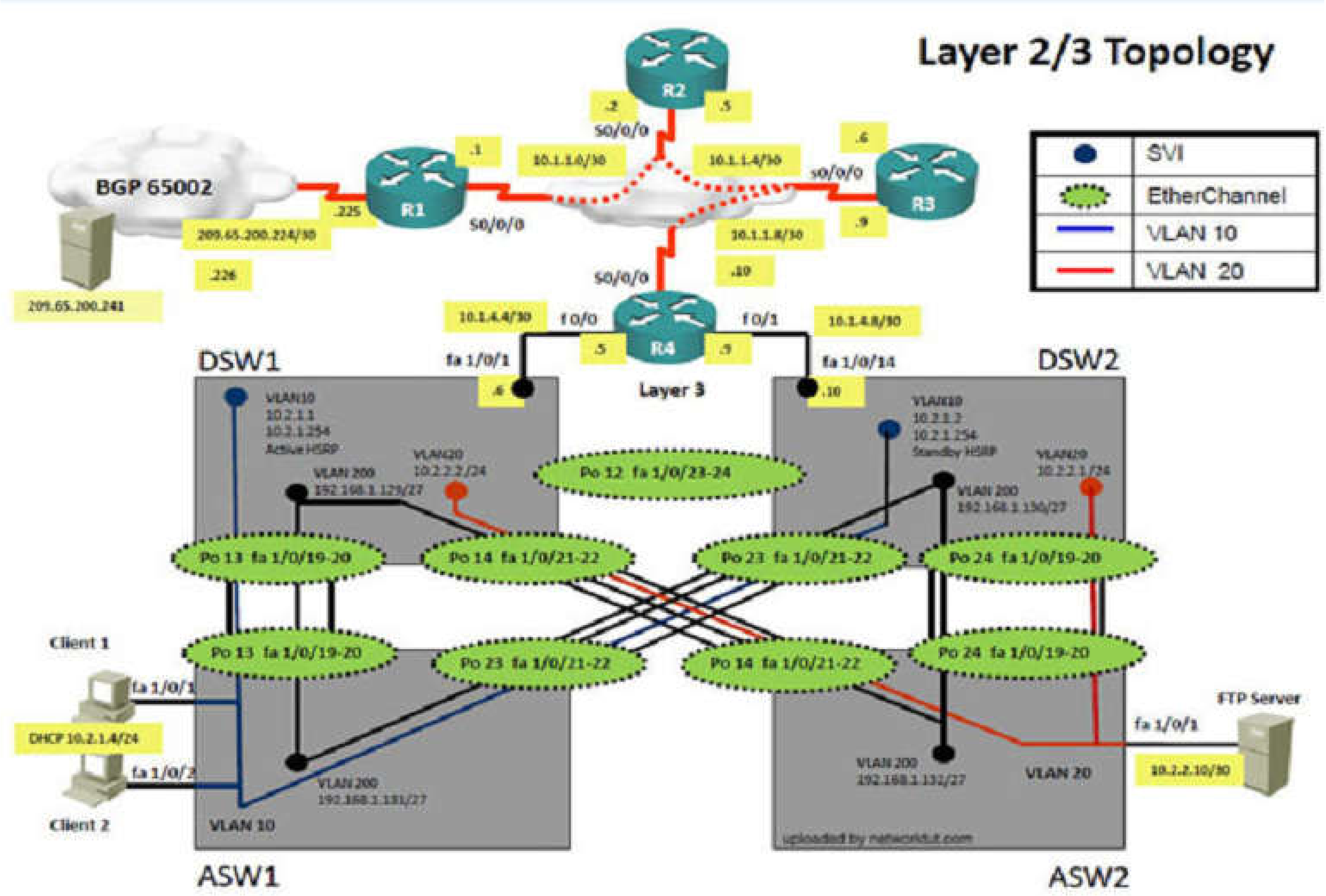
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

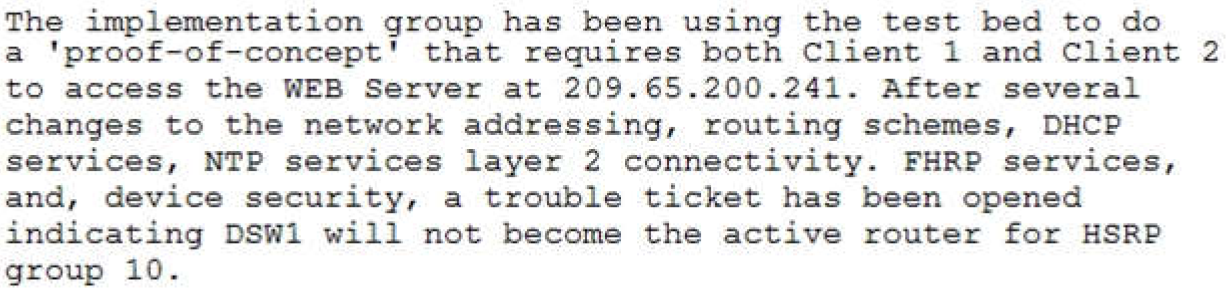
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==






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

Solution

Steps need to follow as below:-

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

2. From ASW1 we can ping 10.2.1.254….

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

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

QUESTION 1

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

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

On which device is the fault condition located?

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

Correct Answer: D
Section: [none]
Explanation

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

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

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

The fault condition is related to which technology?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 3
The implementations group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.
Use the supported commands to isolate the cause of this fault and answer the following question.

What is the solution to the fault condition?

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

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 4
The implementation group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, Layer 2 connectivity, FHRP services, and device security, a trouble ticket has been operated indicating that Client 1 cannot ping the 209.65.200.241 address.

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

On which device is the fault condition located?

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

F. DSW2
G. ASW1
H. ASW2

Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Configuration on DSW1:

```
!
interface Vlan 10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 10.2.21.129
!
```

In this ticket you will find port-security configured on ASW1 but it is not the problem as the port-security is good (check with the “show interface fa1/0/1” command on ASW1. Also you can easily identify this ticket with the “ipconfig” command on Client1, which shows APIPA address (169.254.x.x).

QUESTION 5
The implementation group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, Layer 2 connectivity, FHRP services, and device security, a trouble ticket has been operated indicating that Client 1 cannot ping the 209.65.200.241 address.

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

The fault condition is related to which technology?

A. NTP
B. HSRP
C. IP DHCP Helper
D. IPv4 EIGRP Routing
E. IPV6 RIP Routing
F. IPv4 layer 3 security
G. Switch-to-Switch Connectivity
H. Loop Prevention
I. Access Vlans

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Configuration on DSW1:

```
!
interface Vlan 10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 10.2.21.129
!
```

In this ticket you will find port-security configured on ASW1 but it is not the problem as the port-security is good (check with the “show interface fa1/0/1” command on ASW1. Also you can easily identify this ticket with the “ipconfig” command on Client1, which shows APIPA address (169.254.x.x).

QUESTION 6
The implementation group has been using the test bed to do a ‘proof-of-concept’ that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing schemes, DHCP services, NTP services, Layer 2 connectivity, FHRP services, and device security, a trouble ticket has been operated indicating that Client 1 cannot ping the 209.65.200.241 address.

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

What is the solution to the fault condition?

A. Under the global configuration enter the **ip dhcp excluded-address 10.2.1.1 10.2.1.2** command.
B. Under the interlace Vlan10 configuration delete the **ip helper-address 10.1.21.129** command and under the global configuration create a DHCP pool for the 10.1.21.0 network.
C. Under the interface Vlan10 configuration delete the **ip helper-address 10.1.21.129** command and under the interface FastEthernet1/0/1 configuration enter the **ip helper-address 10.1.21.129** command.
D. Under the interface Vlan10 configuration delete the **ip helper-address 10.2.21.129** command and under the interface Vlan10 configuration enter the **ip helper-address 10.1.21.129** command.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Configuration on DSW1:

```
!
interface Vlan 10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 10.2.21.129
!
```

In this ticket you will find port-security configured on ASW1 but it is not the problem as the port-security is good (check with the “show interface fa1/0/1” command on ASW1. Also you can easily identify this ticket with the “ipconfig” command on Client1, which shows APIPA address (169.254.x.x).

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

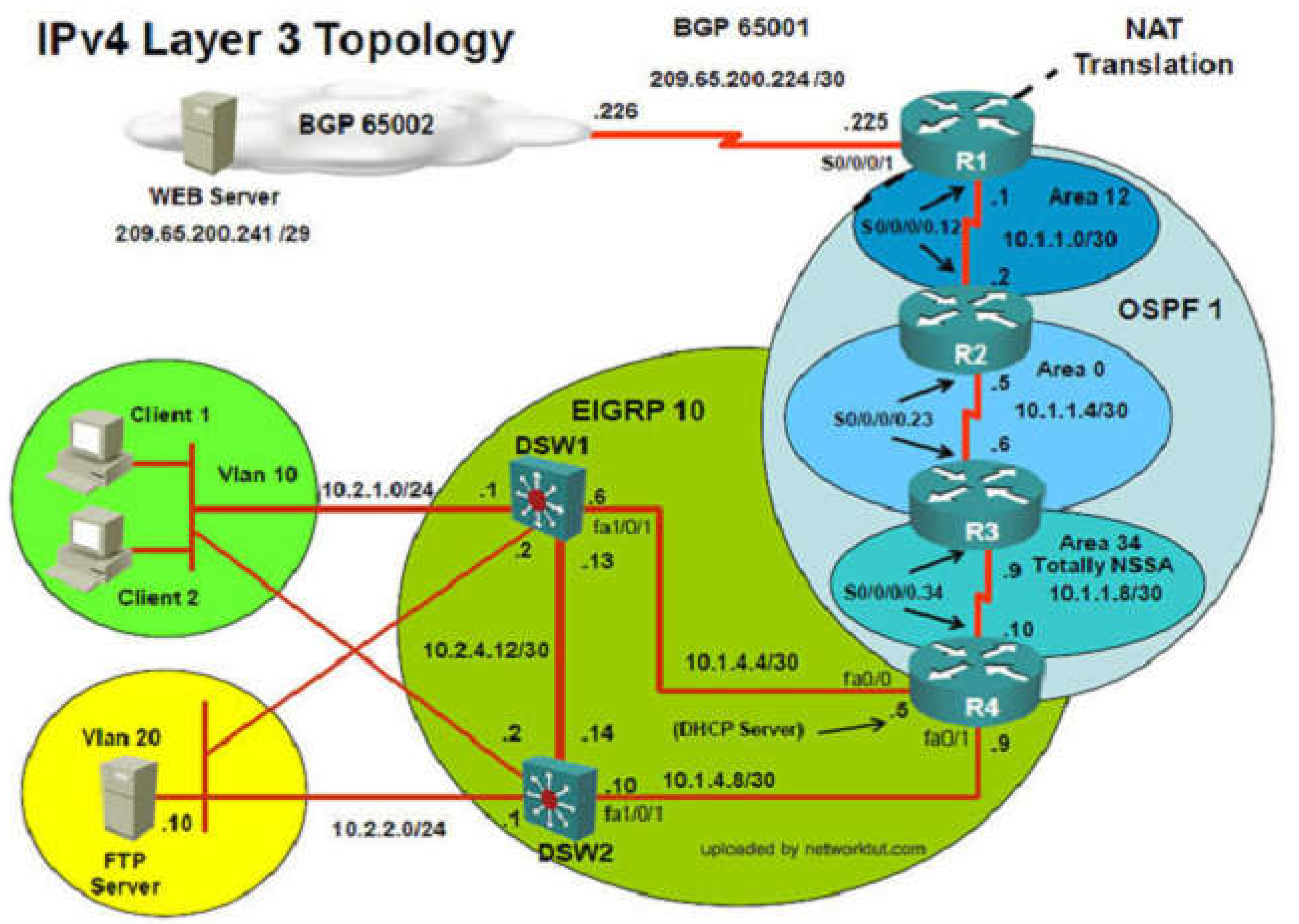
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

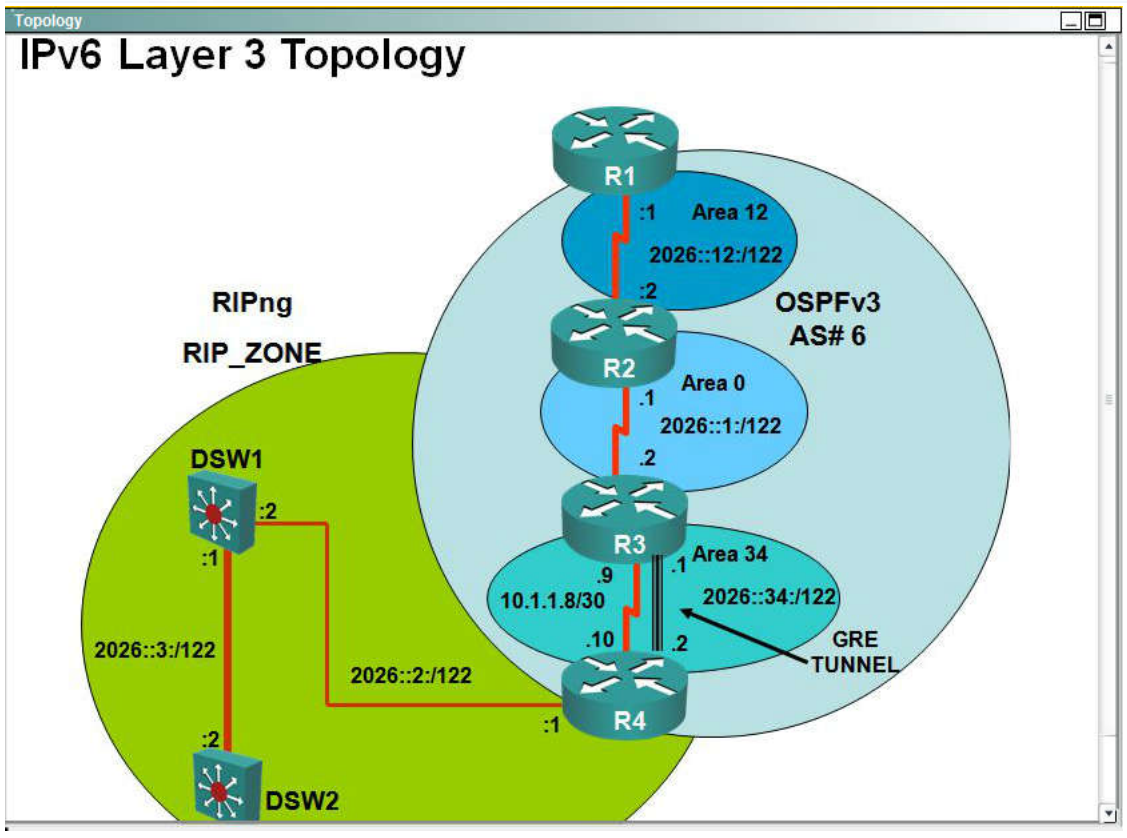
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

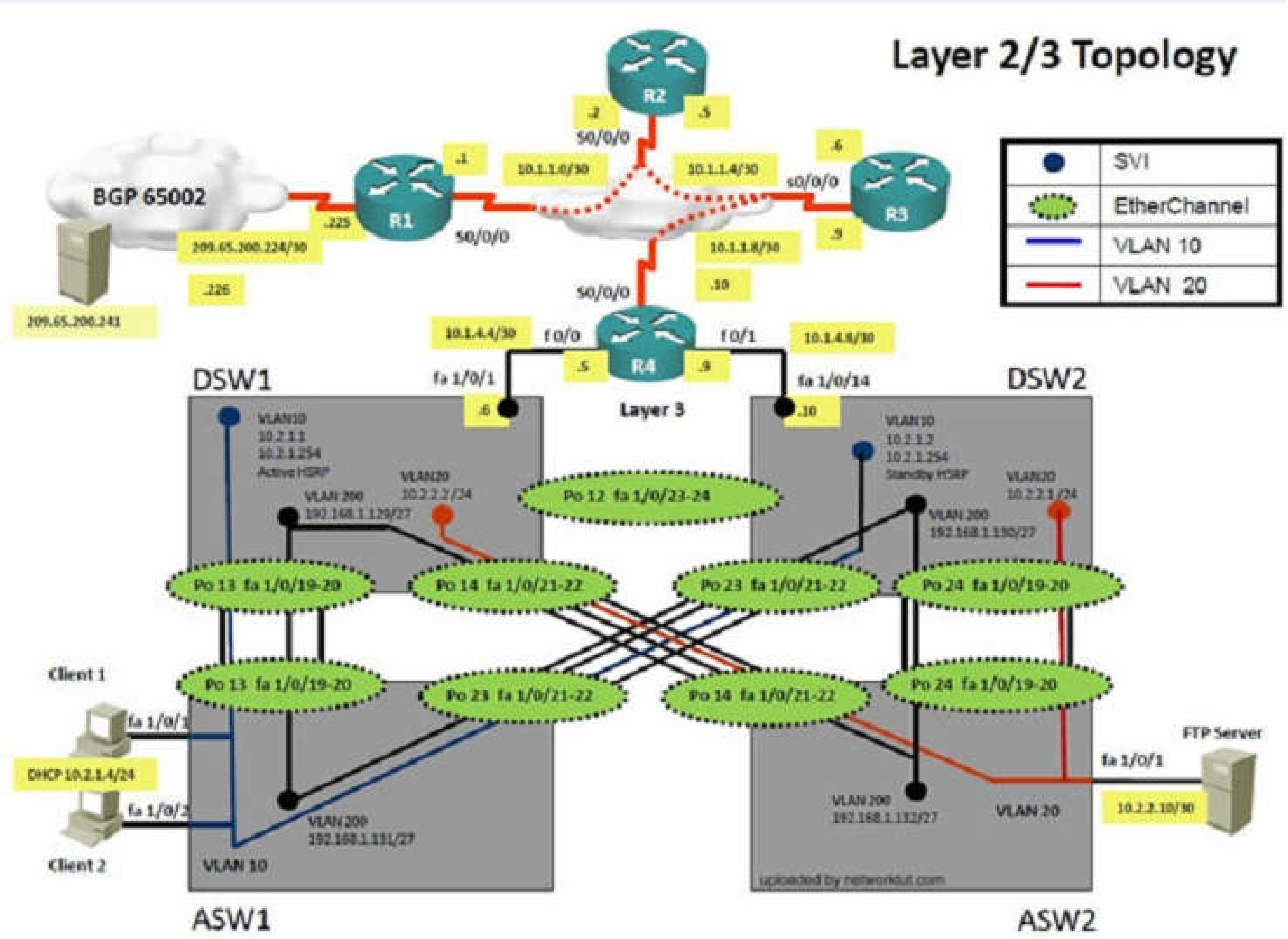
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==


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


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



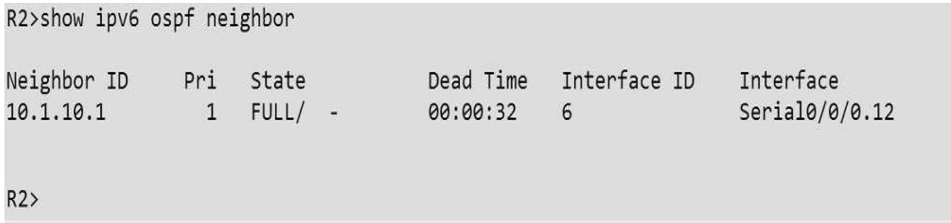
QUESTION 1
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on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

Use the supported commands to isolate the cause of this fault and answer the following question.
On which device is the fault condition located?

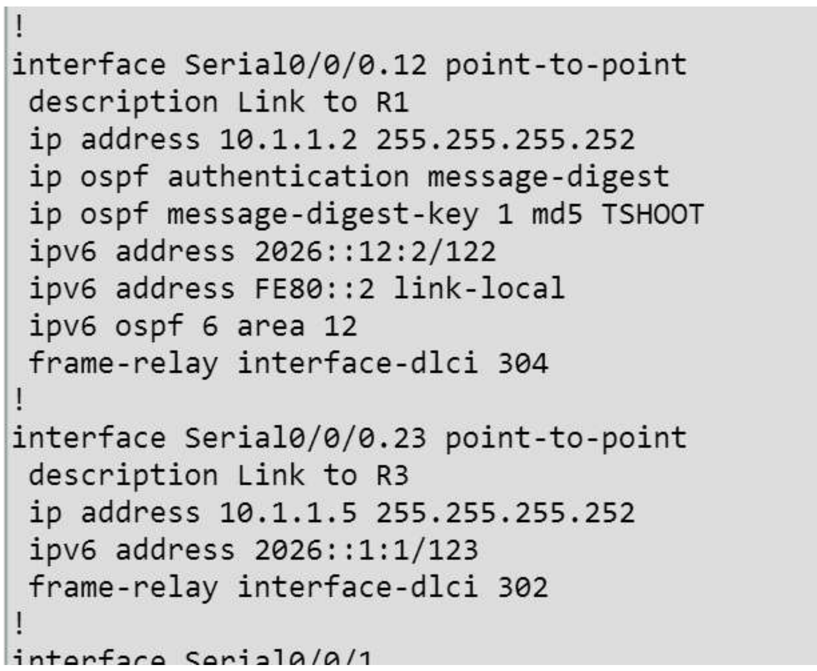
A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Correct Answer: B
Section: [none]
Explanation

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


```
R2>show ipv6 ospf neighbor

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


R2>
```

We can then see that OSPFv3 has not been enabled on the interface to R3:



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

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

QUESTION 2
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Use the supported commands to isolate the cause of this fault and answer the following question.
The fault condition is related to which technology?

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

Correct Answer: B
Section: [none]
Explanation

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

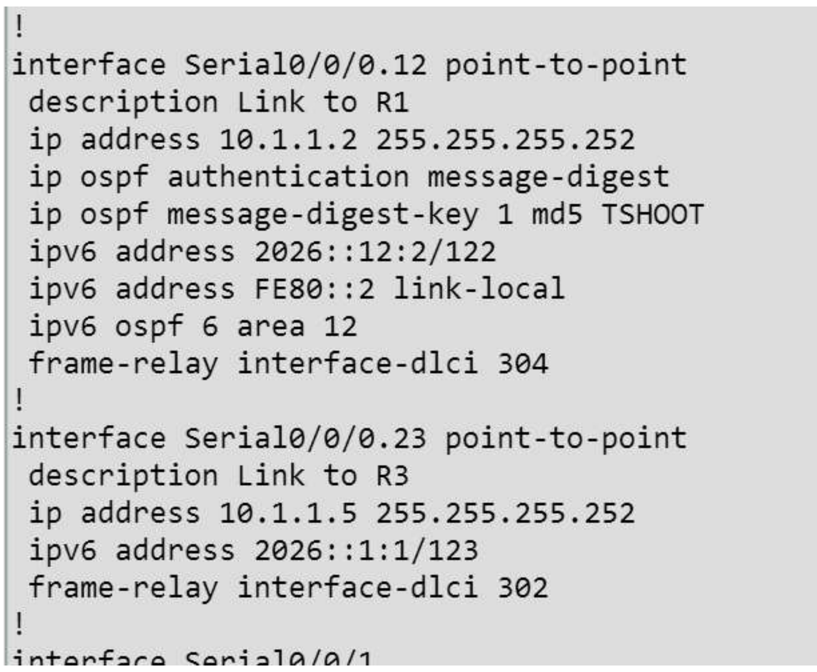
QUESTION 3
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).
Use the supported commands to isolate the cause of this fault and answer the following question.

What is the solution to the fault condition?

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
As explained in question one of this ticket, we can then see that OSPFv3 has not been enabled on the interface to R3:



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

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

Testlet 1

Instructions

The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection

- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation

- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification

- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on “**Next Question**”.
- When you click “**DONE**”, the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the “**Previous Question**” button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click “**DONE**”. This will store your response to the questions. Do not click on “**DONE**” unless you have answered all questions within the ticket.

Item Completion

- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

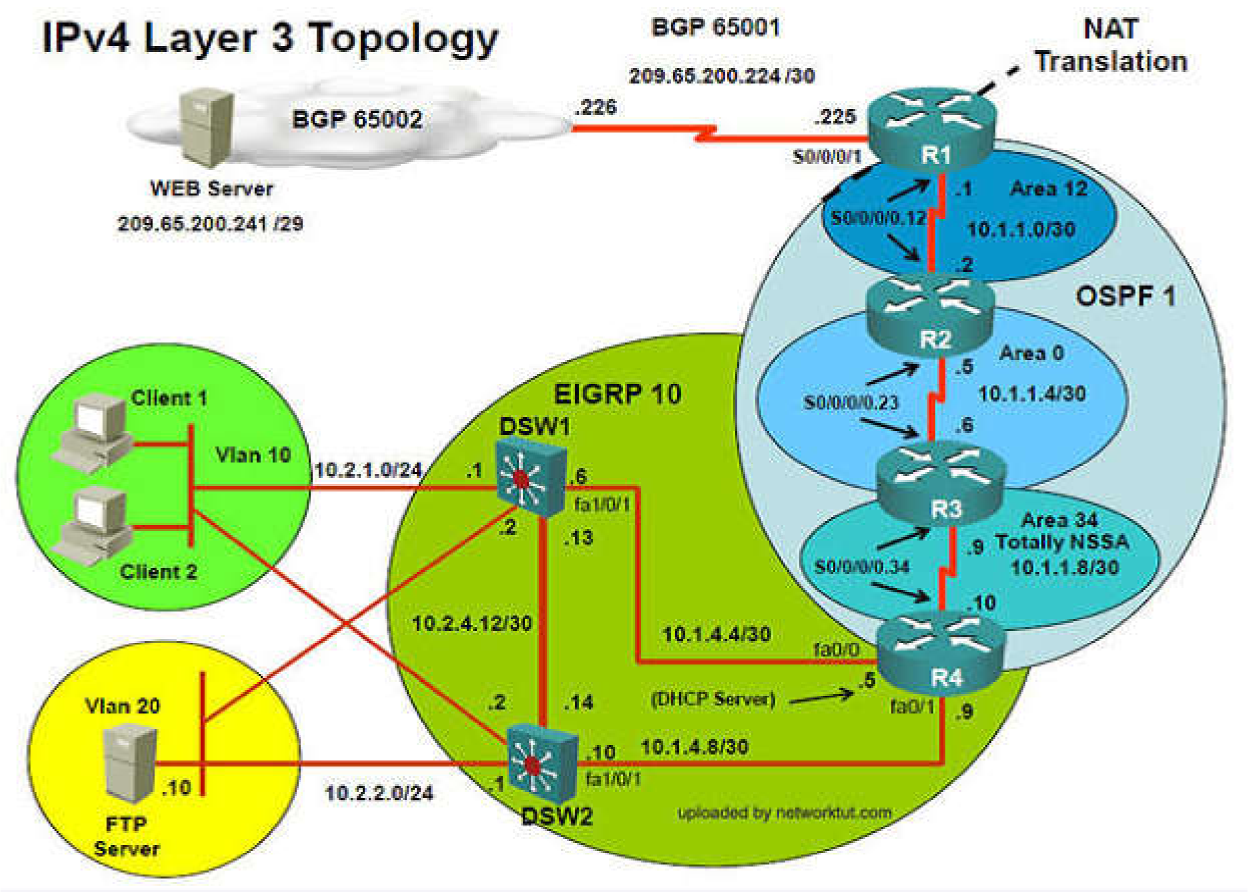
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP’s network. Because the company’s address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4’s DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

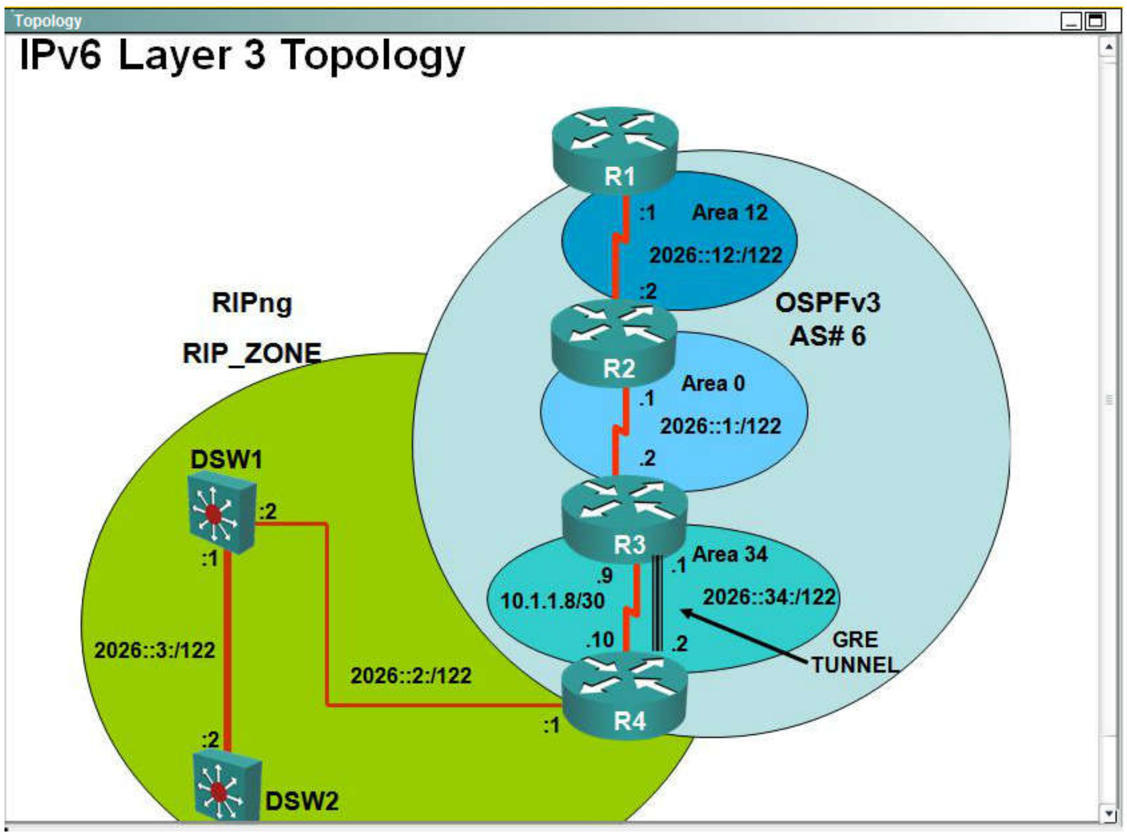
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution is enabled where necessary.

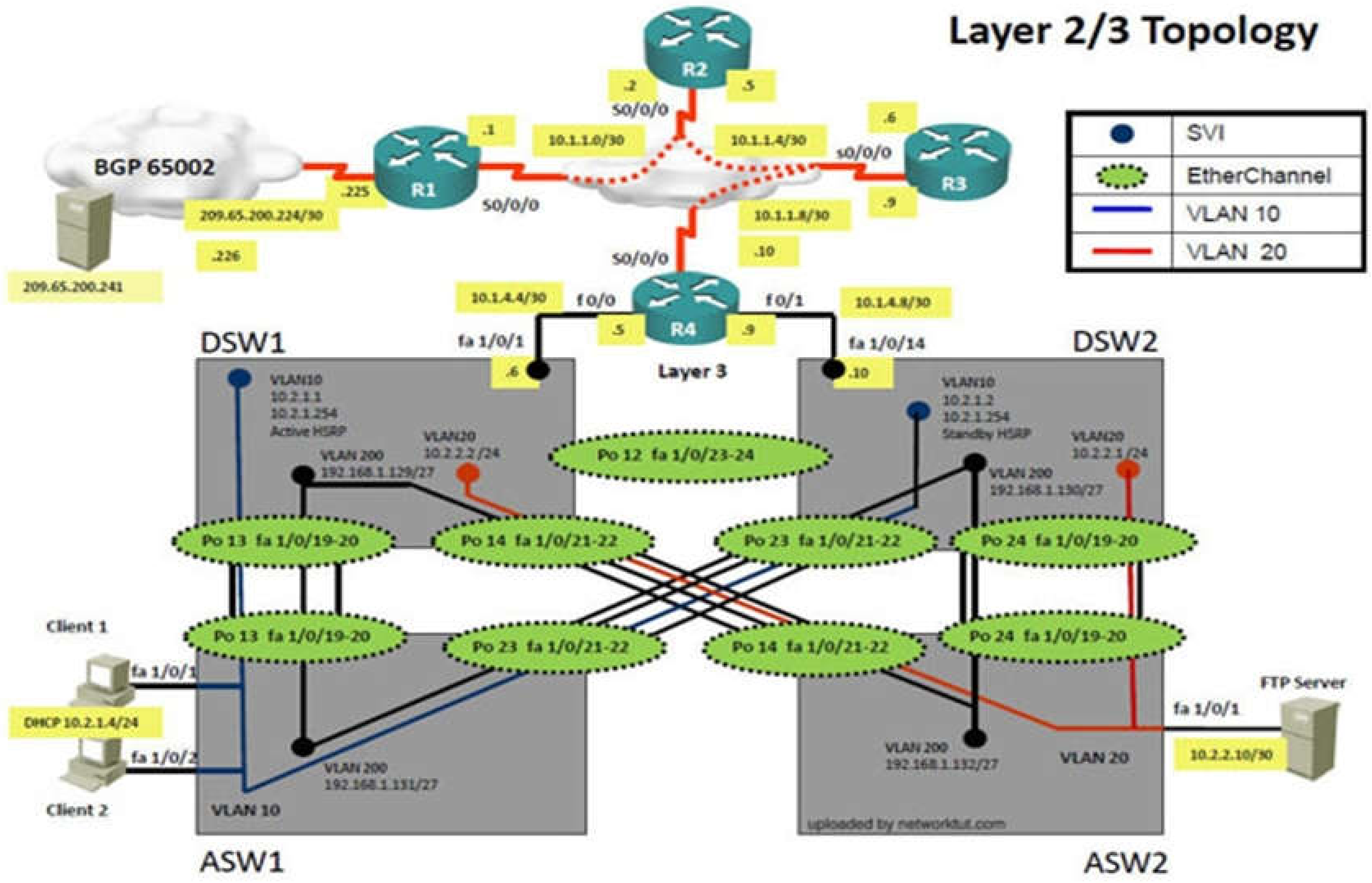
Recently the implementation group has been using the test bed to do a ‘proof-of-concept’ on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution


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
R3
Client 1
Vlan 10
10.2.1.0/24
.1
DSW1
.6
fa1/0/1
.2
.13
Client 2
Area 34
Totally NSSA
.9
S0/0/0/0.34
10.1.1.8/30
.10
10.2.4.12/30
10.1.4.4/30
fa0/0
R4
Vlan 20
.2
.14
(DHCP Server)
.5
fa0/1
.9
.10
10.1.4.8/30
.10
fa1/0/1
FTP Server
10.2.2.0/24
.1
DSW2
uploaded by networktut.com


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

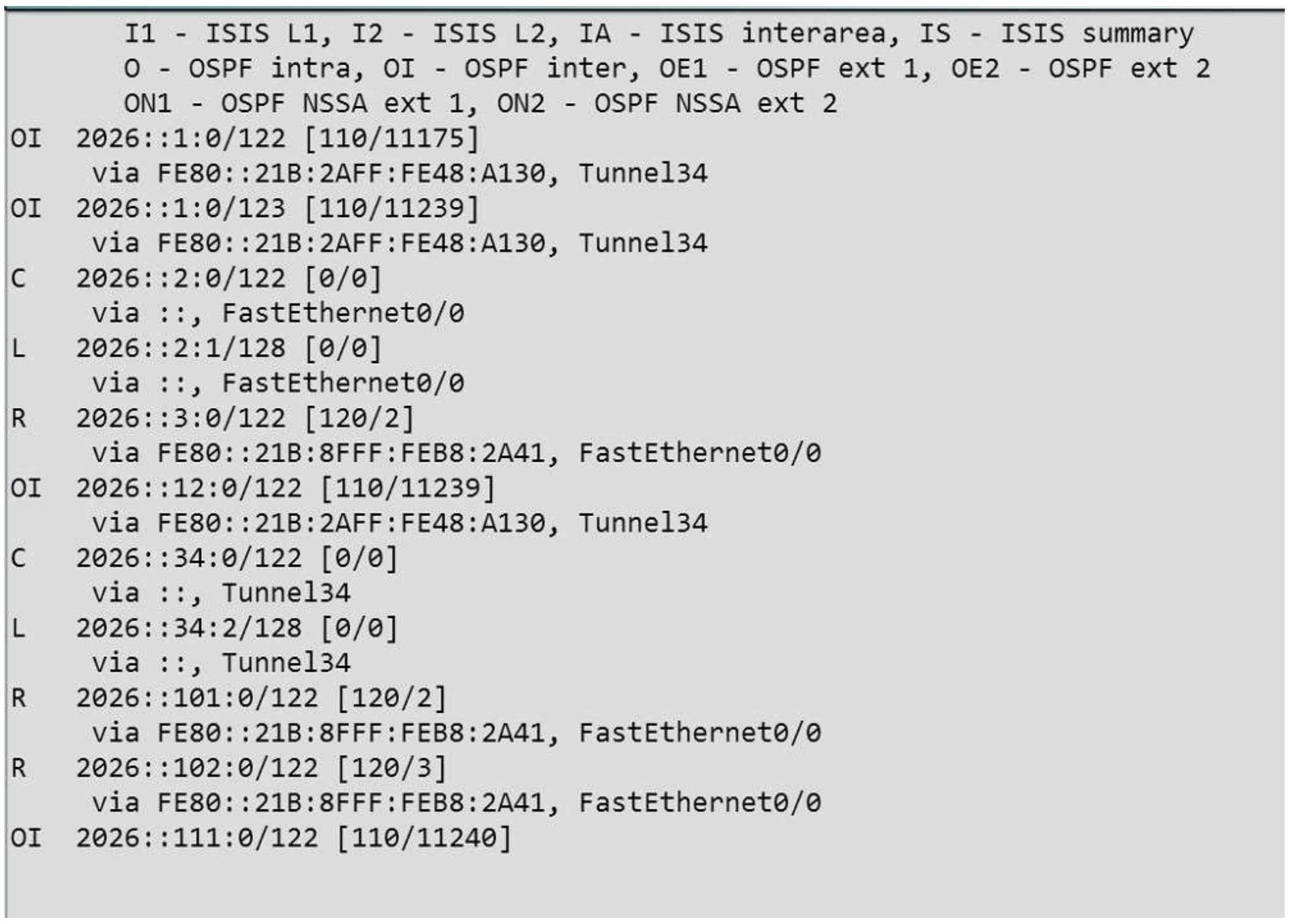


QUESTION 1
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on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

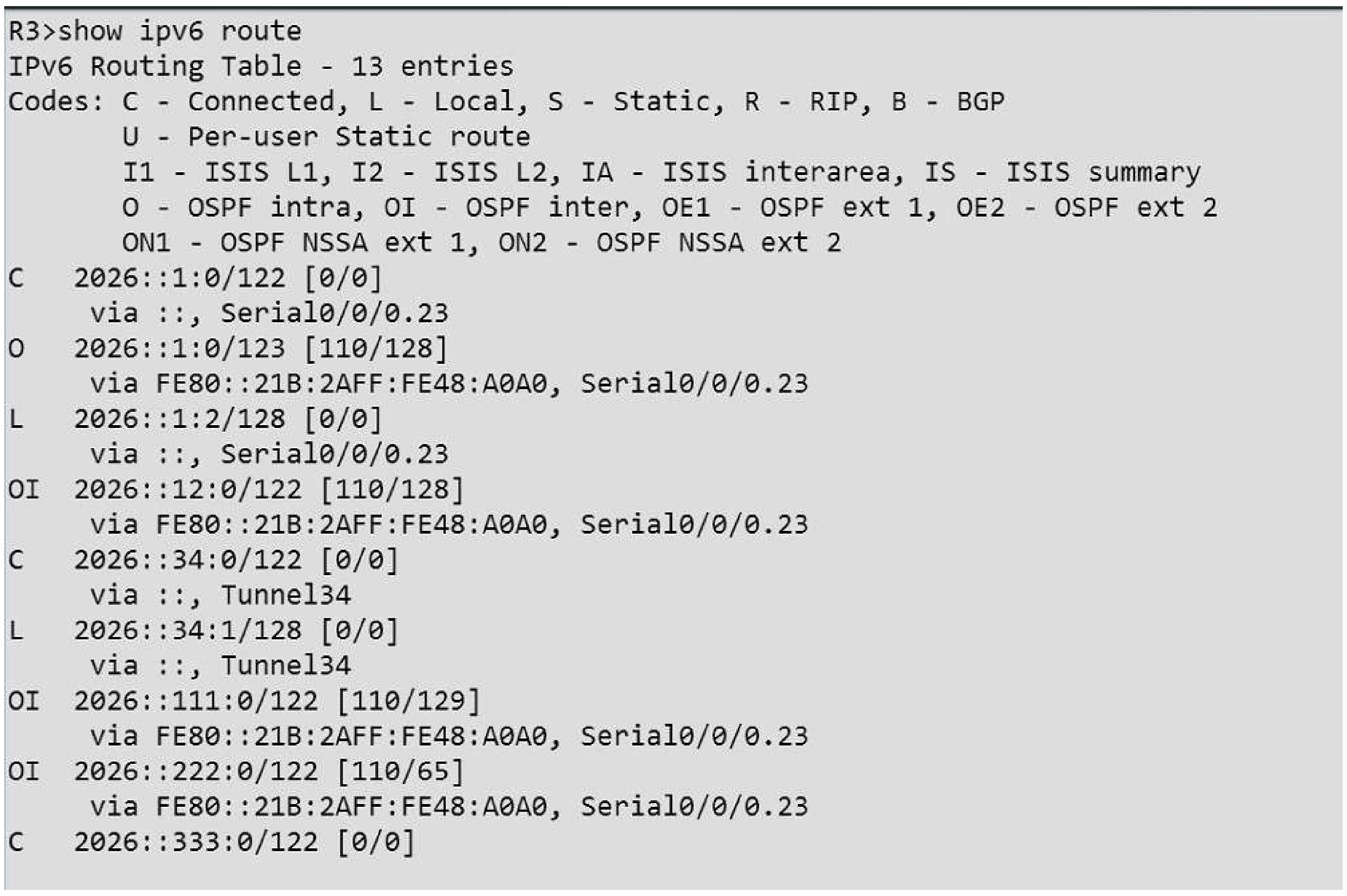
A. R1
B. R2
C. R3
D. R4
E. DSW1
F. DSW2
G. ASW1
H. ASW2

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Start to troubleshoot this by pinging the loopback IPv6 address of DSW2 (2026::102:1). This can be pinged from DSW1, and R4, but not R3 or any other devices past that point. If we look at the diagram, we see that R4 is redistributing the OSPF and RIP IPV6 routes. However, looking at the routing table we see that R4 has the 2026::102 network in the routing table known via RIP, but that R3 does not have the route:

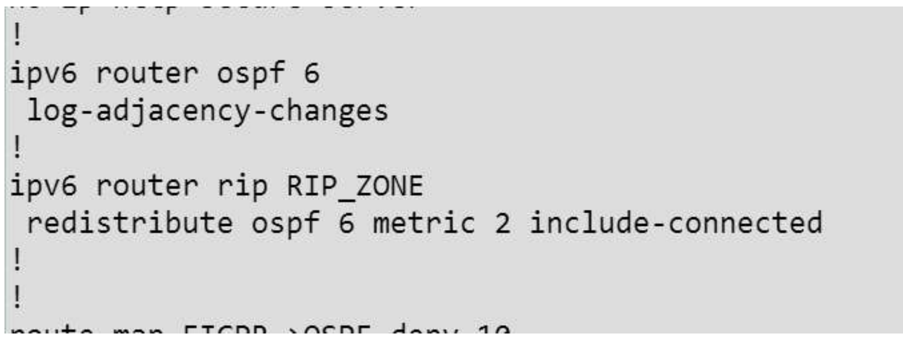


```
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2026::1:0/122 [110/11175]
     via FE80::21B:2AFF:FE48:A130, Tunnel34
OI  2026::1:0/123 [110/11239]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



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

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



```
no ip http secure-server
!
ipv6 router ospf 6
 log-adjacency-changes
!
ipv6 router rip RIP_ZONE
 redistribute ospf 6 metric 2 include-connected
!
!
route-map EIGRP->OSPF deny 10
```

So, problem is with route redistribution on R4.

QUESTION 2

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

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

The fault condition is related to which technology?

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

Correct Answer: G
Section: [none]
Explanation

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

QUESTION 3
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Use the supported commands to isolate the cause of this fault and answer the following question.
What is the solution to the fault condition?

A. Under the interface Tunnel34 configuration enter the **ipv6 ospf 6 area 34** command.
B. Under the interface Loopback6 configuration enter the **ipv6 ospf 6 area 34** command.
C. Under the interface Serial0/0/0.34 configuration enter the **ipv6 ospf 6 area 34** command.
D. Under ipv6 router ospf 6 configuration enter the **redistribute rip RIP_ZONE include-connected** command.

Correct Answer: D
Section: [none]
Explanation

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

Testlet 1

Instructions
The main screen consists of two parts; the Main scenario and the Topology tabs. The main scenario describes TSHOOT.com test bed. The Topology tabs allow you to display the appropriate and select the trouble ticket.
To complete the item, you will first need to familiarize yourself with the TSHOOT.com test bed by clicking on the master scenario first and then the topologies tabs. Once you are familiar with the test bed and the topologies, you should start evaluating the trouble ticket. You will be presented with a Trouble Ticket scenario that will describe the fault condition. You will need to determine on which device the fault condition is located, to which technology the fault condition is related, and the solution to each trouble ticket. This will be done by answering three questions.

Ticket Selection
- To begin, click on the Ticket on the Topology tabs.
- **Please note.** Some of the questions will require you to use the scroll bar to see all options.

Fault Isolation
- Read the ticket scenario to understand the fault condition.
- Open the appropriate topology, based upon the ticket scenario.
- Open the console of the desired device by clicking on that device in the topology, based upon your troubleshooting methodology.
- Use the supported **show, ping** and **trace** commands to begin your fault isolation process.
- Move to other devices as need by clicking on those devices within the topology.

Fault Identification
- The trouble ticket will include three questions that you will need to answer:
  1. Which device contains the fault
  2. Which technology the fault condition is related to
  3. What is the solution to the issue
- To advance to the next question within the ticket click on "**Next Question**".
- When you click "**DONE**", the trouble ticket will turn **RED** and will no longer be accessible.
- You may also use the "**Previous Question**" button to review questions within that specific ticket.
- To complete a trouble ticket, answer all three questions and click "**DONE**". This will store your response to the questions. Do not click on "**DONE**" unless you have answered all questions within the ticket.

Item Completion
- Click the **NEXT** button on the bottom of the screen once a ticket is **RED**. This action moves you to the next item.

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

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

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits.
This network consists of four routers, two layer 3 switches and two layer 2 switches.

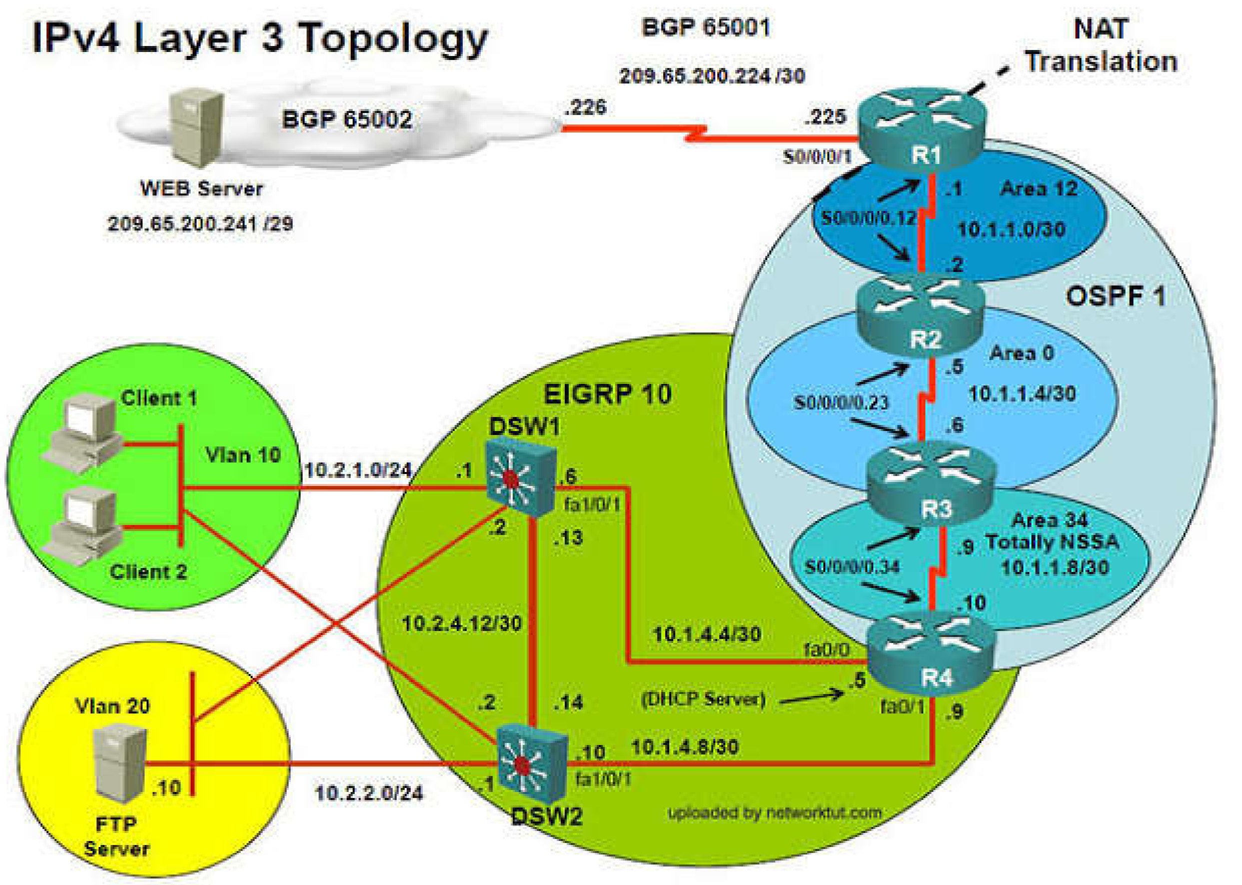
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range.
R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

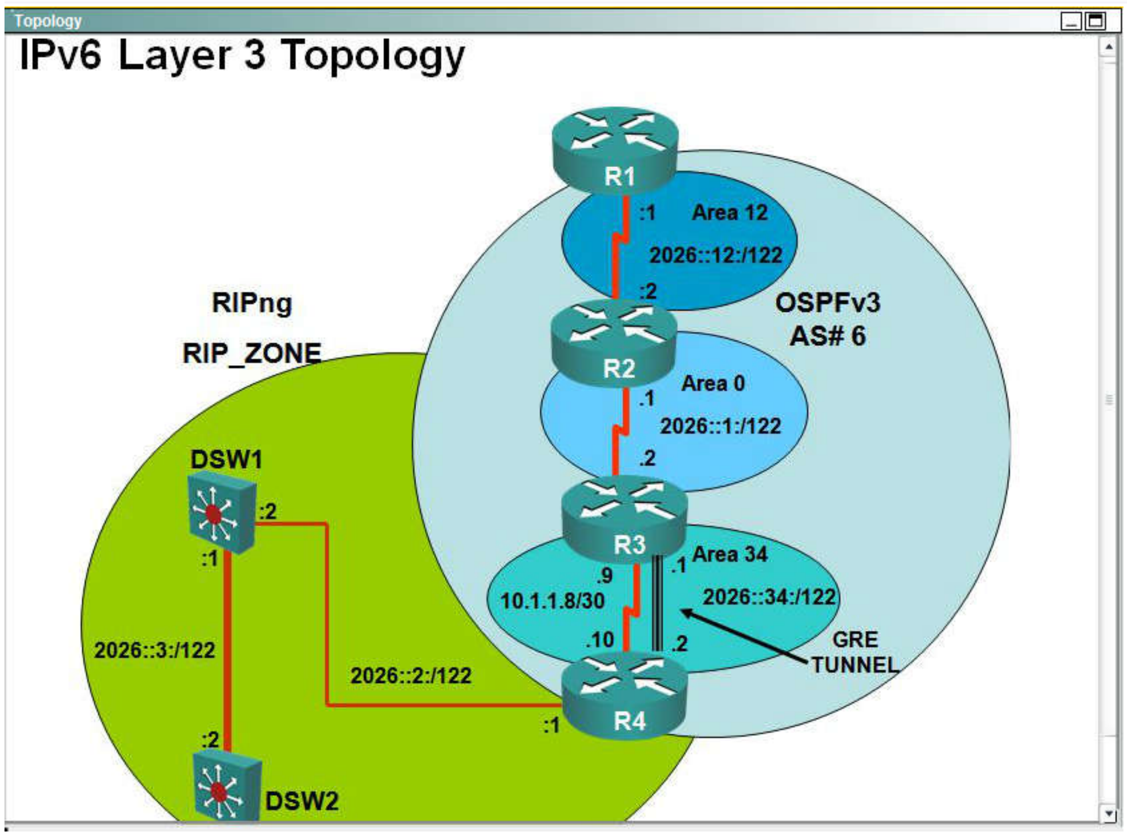
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

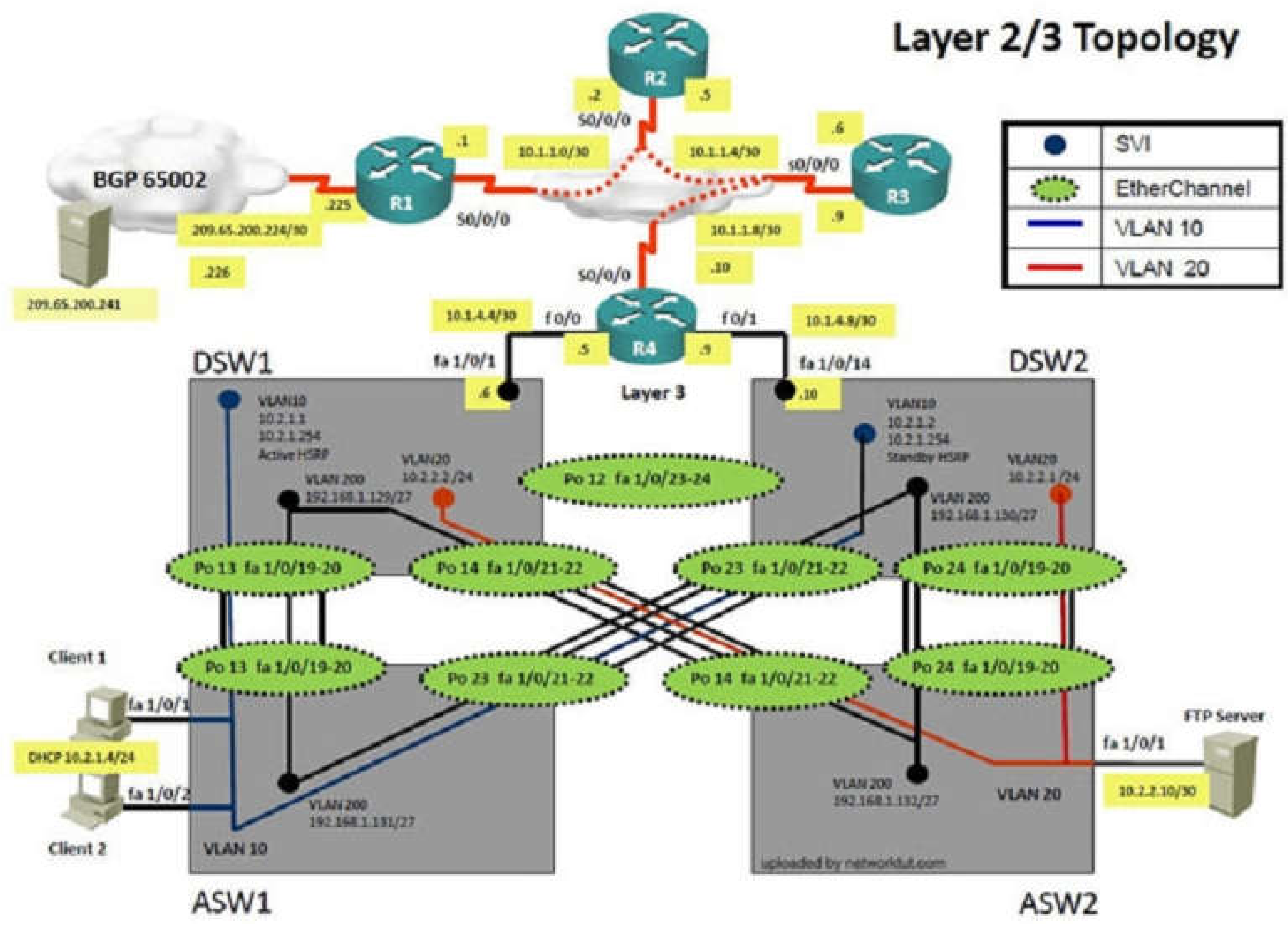
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

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

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==


IPv4 Layer 3 Topology
BGP 65001
209.65.200.224 /30
NAT Translation
BGP 65002
WEB Server
209.65.200.241 /29
.226
.225
S0/0/0/1
R1
.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
fa0/0
.5
fa0/1
.9
(DHCP Server)
EIGRP 10
DSW1
.1
.6
fa1/0/1
.2
.13
10.2.4.12/30
10.1.4.4/30
.2
.14
DSW2
.10
10.1.4.8/30
fa1/0/1
.1
Client 1
Vlan 10
10.2.1.0/24
Client 2
Vlan 20
FTP Server
.10
10.2.2.0/24
uploaded by networktut.com


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

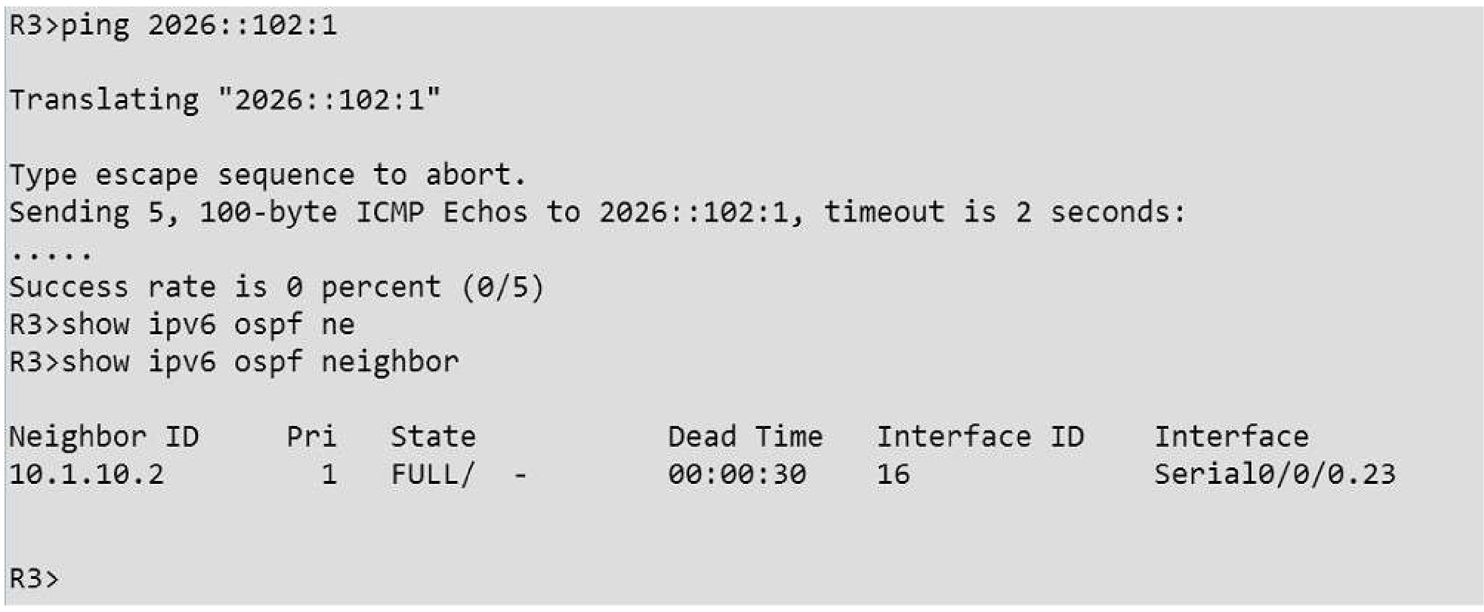


QUESTION 1
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on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

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

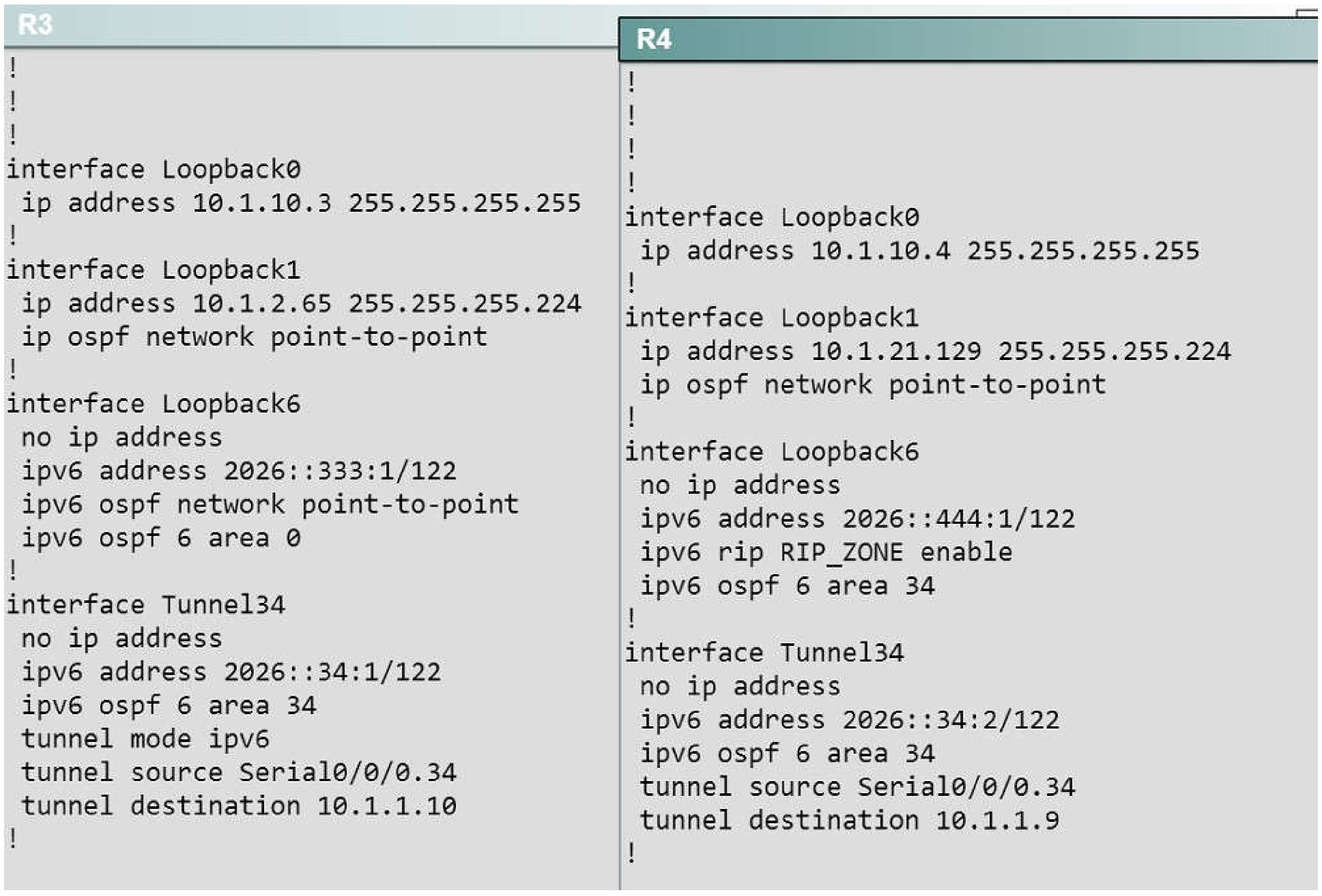
Correct Answer: C
Section: [none]
Explanation

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



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

Translating "2026::102:1"

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

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


R3>
```

This is due to mismatched tunnel modes between R3 and R4:



R3

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

R4

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

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

QUESTION 2
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

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

The fault condition is related to which technology?

A. NTP
B. IPv4 OSPF Routing
C. IPv6 OSPF Routing
D. IPV4 and IPV6 Interoperability
E. IPv4 layer 3 security

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Answer: D
Explanation:
As explained earlier, the problem is with route misconfigured tunnel modes on R3. R3 is using tunnel mode ipv6, while R4 is using the default of GRE.

QUESTION 3
The implementation group has been using the test bed to do an IPv6 'proof-of-concept1. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

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

What is the solution to the fault condition?

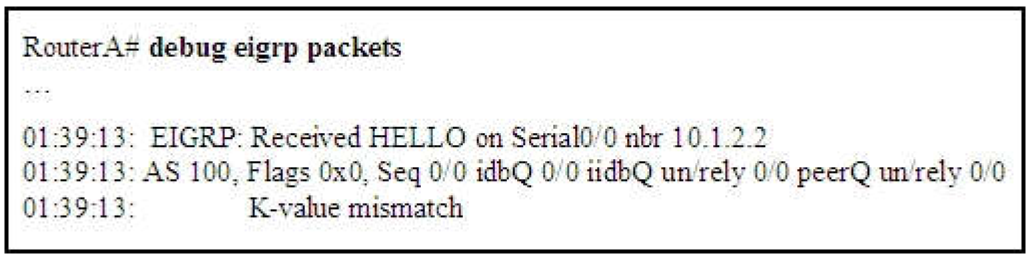
A. Under the interface Tunnel34 configuration delete the tunnel mode ipv6 command.
B. Under the interface Serial0/0/0.34 configuration enter the ipv6 address 2026::34:1/122 command.
C. Under the interface Tunnel34 configuration enter the ip address unnumbered Serial0/0/0.34 command.
D. Under the interface Tunnel34 configuration delete the tunnel source Serial0/0/0.34 command and enter the tunnel source 2026::34:1/122 command.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
As explained earlier, the problem is with route misconfigured tunnel modes on R3. R3 is using tunnel mode ipv6, while R4 is using the default of GRE. We need to remove the “tunnel mode ipv6” command under interface Tunnel34

Question Set 1

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:

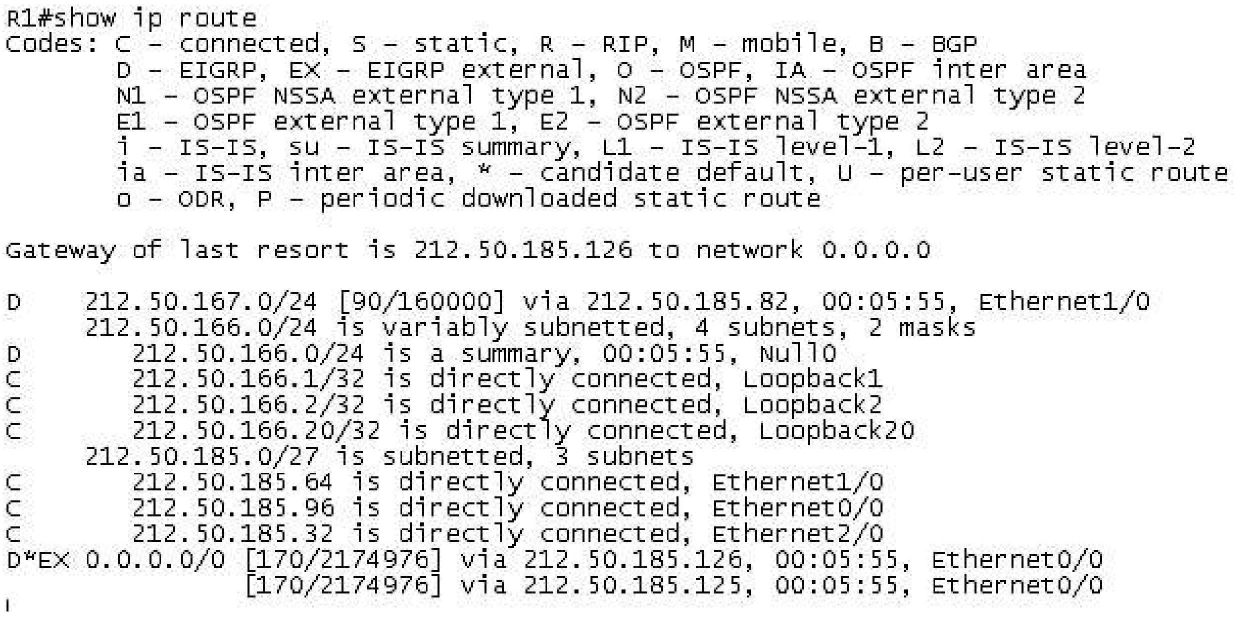
QUESTION 2
When troubleshooting an EIGRP connectivity problem, you notice that two connected EIGRP routers are not becoming EIGRP neighbors. A ping between the two routers was successful. What is the next thing that should be checked?

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:

QUESTION 3
Refer to the exhibit.



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

Gateway of last resort is 212.50.185.126 to network 0.0.0.0

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

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

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

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

A. 3DES

B. multipoint GRE
C. tunnel
D. transport

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
Which three features are benefits of using GRE tunnels in conjunction with IPsec for building site-to-site VPNs? (Choose three.)

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

Correct Answer: ABD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 6
Which statement is true about an IPsec/GRE tunnel?

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

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 7
Which protocol does mGRE use to determine where packets are sent?

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

Correct Answer: A
Section: [none]
Explanation

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

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

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

Correct Answer: BCD
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Currently, MPP controls only the incoming management requests for protocols, such as TFTP, Telnet, Simple Network Management Protocol (SNMP), Secure Shell (SSH), and HTTP.
Following are the management protocols that the MPP feature supports. These management protocols are also the only protocols affected when MPP is enabled.

- Blocks Extensible Exchange Protocol (BEEP)
- FTP
- HTTP
- HTTPS
- SSH, v1 and v2
- SNMP, all versions
- Telnet
- TFTP

Reference: https://www.cisco.com/c/en/us/td/docs/ios/security/configuration/guide/sec_mgmt_plane_prot.html

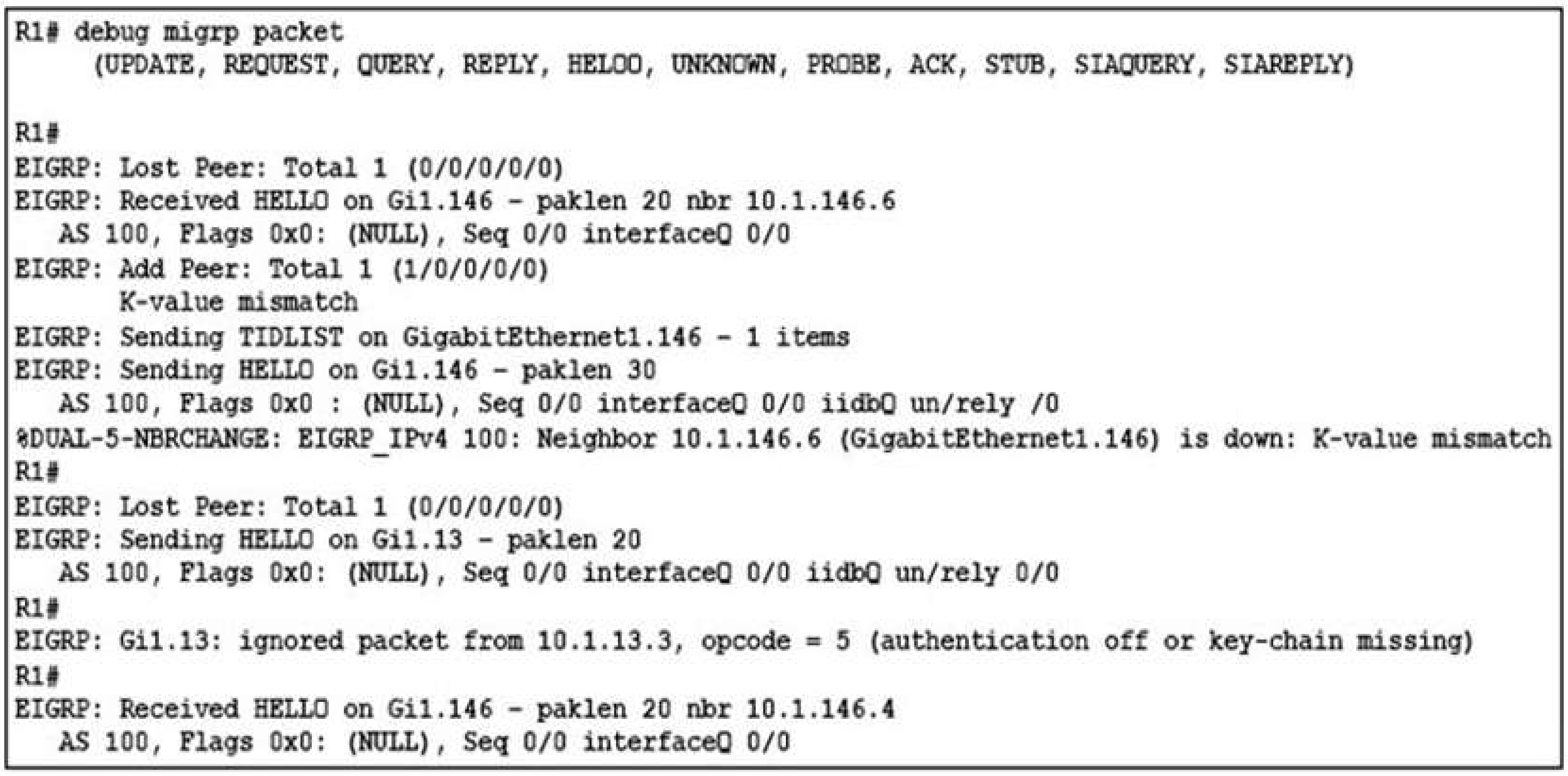
QUESTION 9
Which IPsec mode encrypts a GRE tunnel and adds the least amount of overhead?

A. tunnel
B. transport
C. dynamic
D. transparent

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 10



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

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

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

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

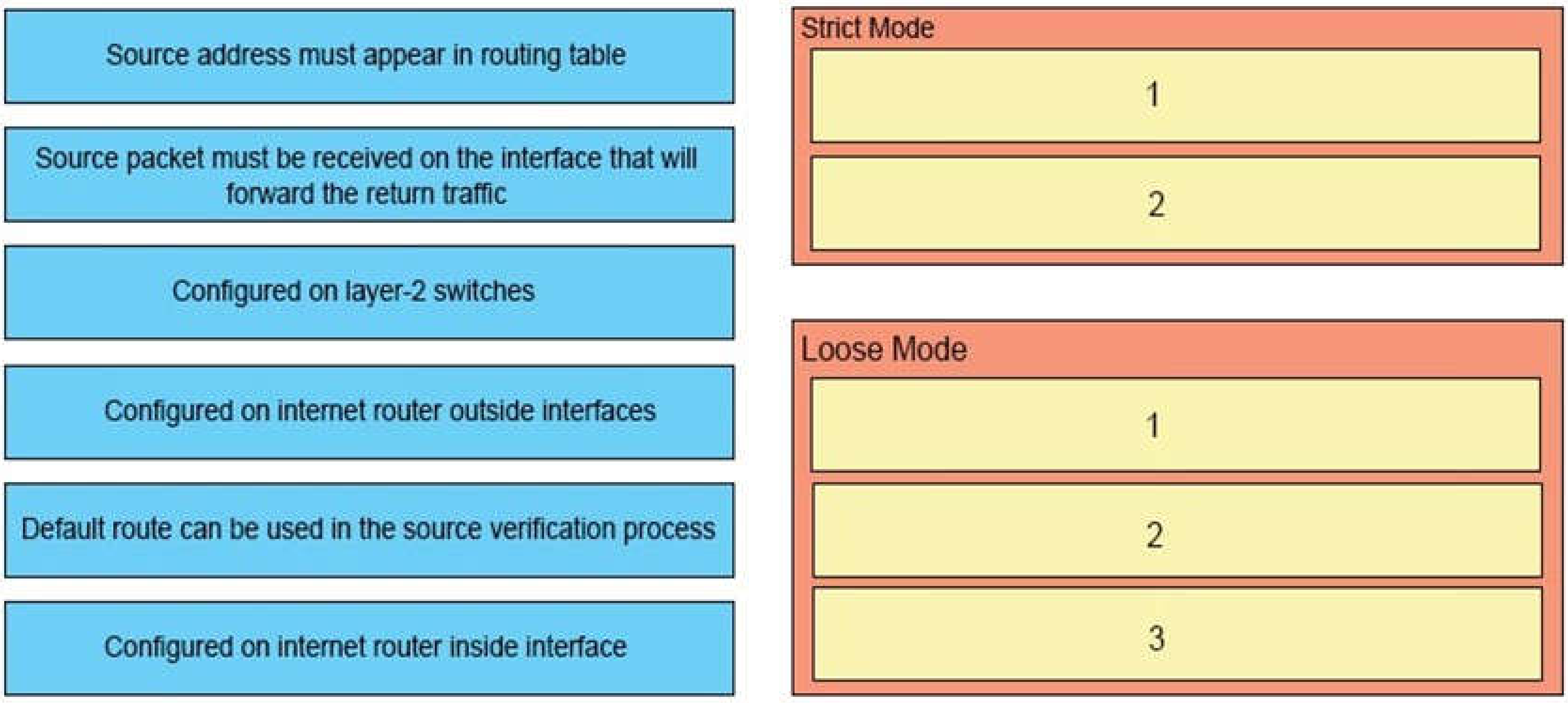
Correct Answer: BD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 11
DRAG DROP

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

Select and Place:



Source address must appear in routing table

Source packet must be received on the interface that will forward the return traffic

Configured on layer-2 switches

Configured on internet router outside interfaces

Default route can be used in the source verification process

Configured on internet router inside interface

Strict Mode

1

2

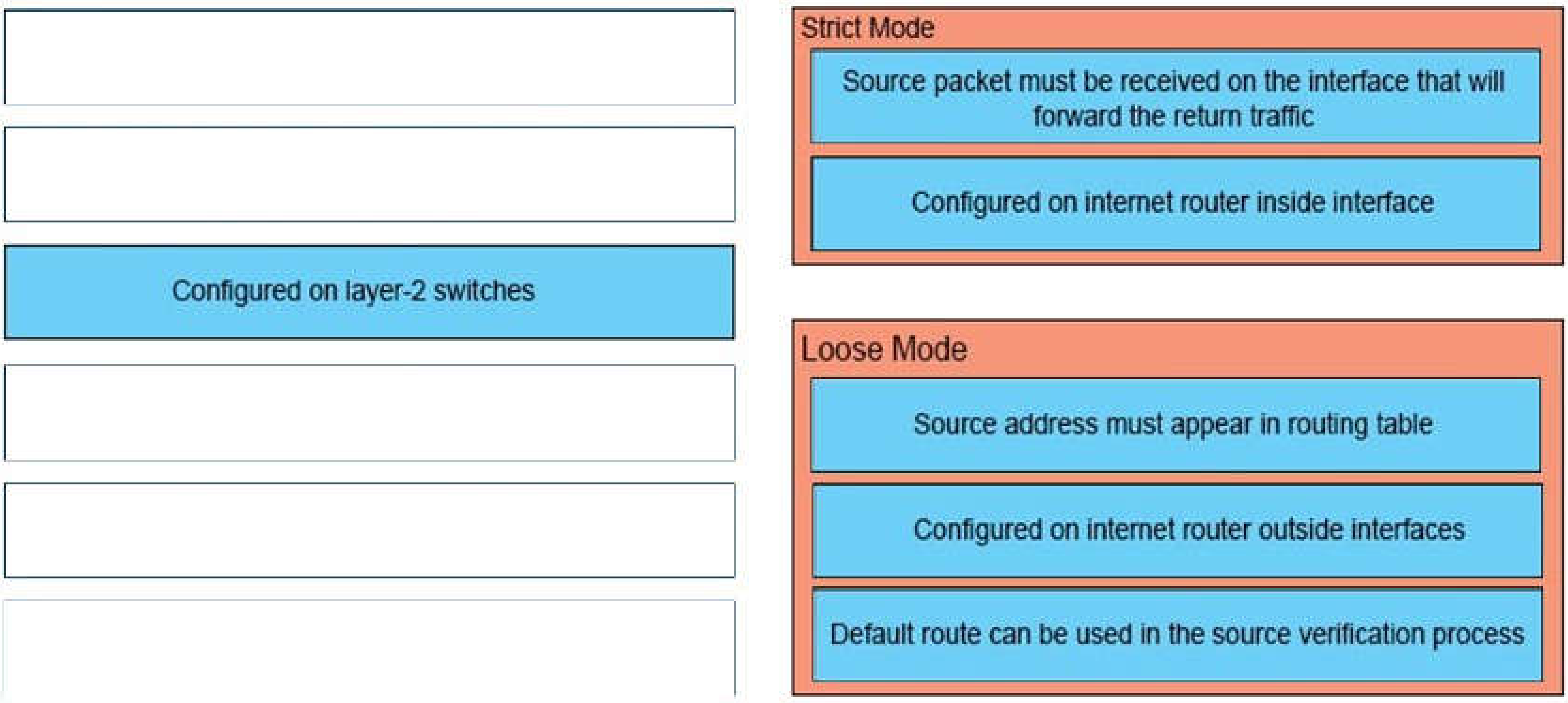
Loose Mode

1

2

3

Correct Answer:



Configured on layer-2 switches

Strict Mode

Source packet must be received on the interface that will forward the return traffic

Configured on internet router inside interface

Loose Mode

Source address must appear in routing table

Configured on internet router outside interfaces

Default route can be used in the source verification process

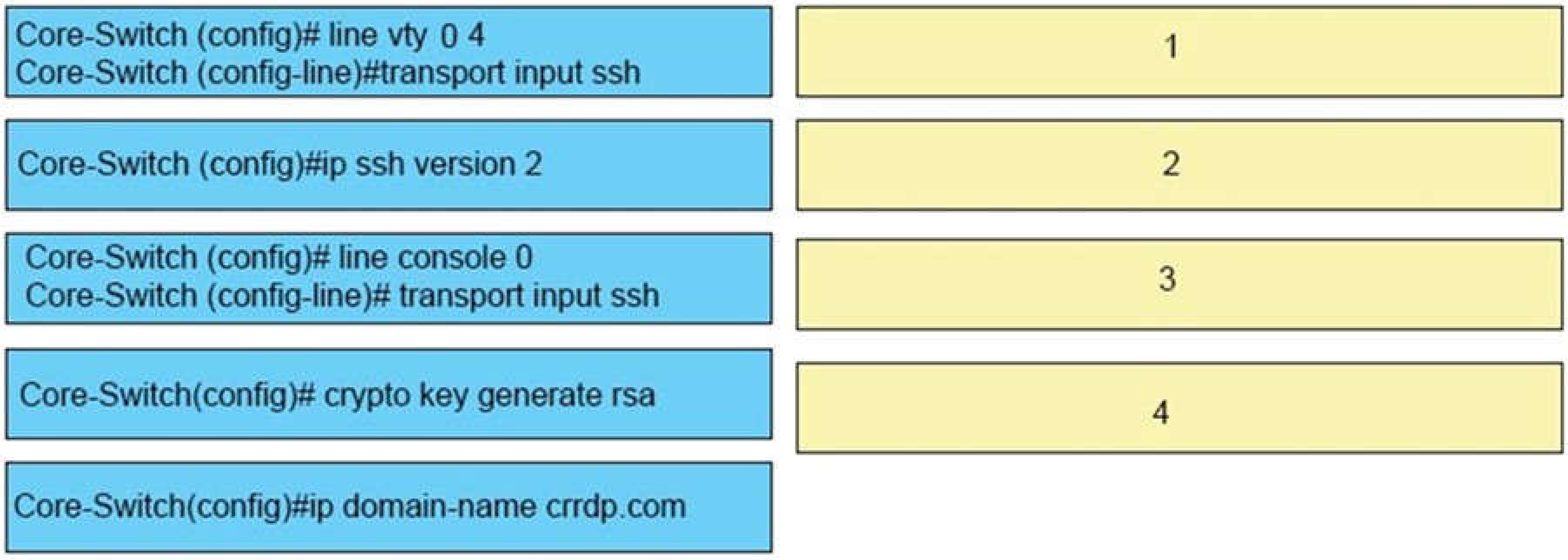
Section: [none]
Explanation

Explanation/Reference:

QUESTION 12
DRAG DROP

Drag the SSH configuration commands in order from the left onto the correct sequence number on the right. Not all commands are used.

Select and Place:



```
Core-Switch (config)# line vty 0 4
Core-Switch (config-line)#transport input ssh
```

```
Core-Switch (config)#ip ssh version 2
```

```
Core-Switch (config)# line console 0
Core-Switch (config-line)# transport input ssh
```

```
Core-Switch(config)# crypto key generate rsa
```

```
Core-Switch(config)#ip domain-name crrdp.com
```

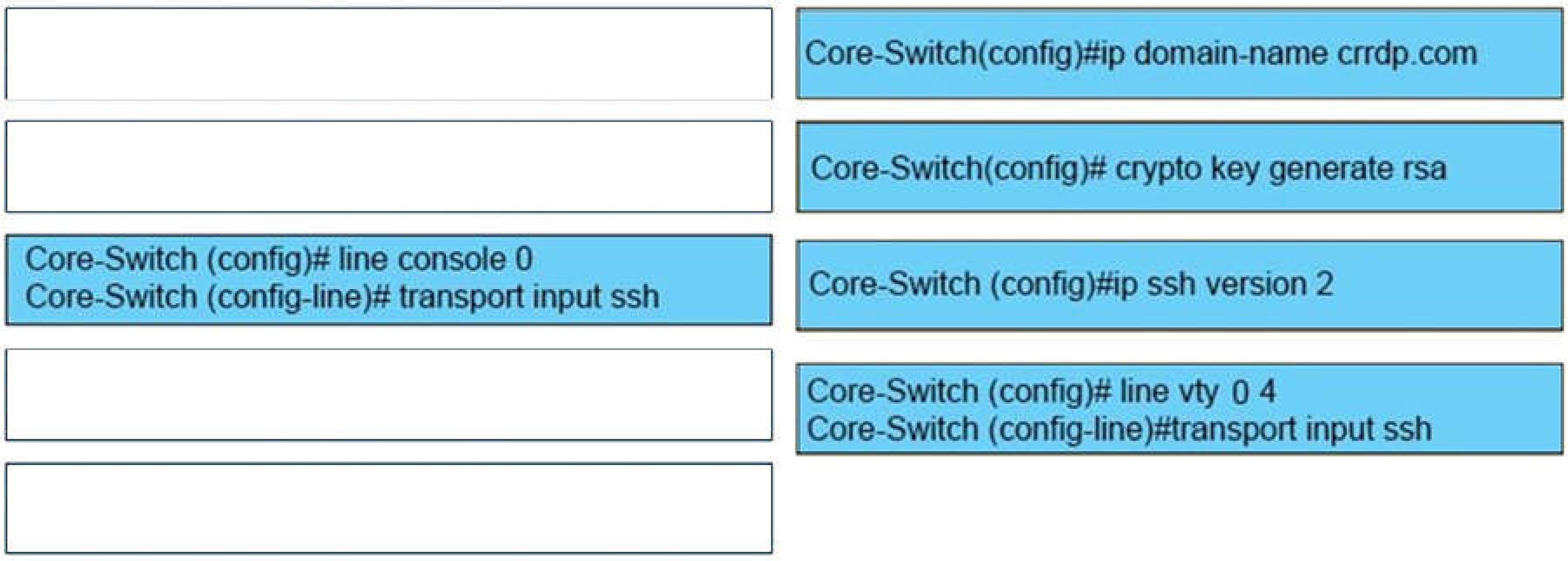
1

2

3

4

Correct Answer:

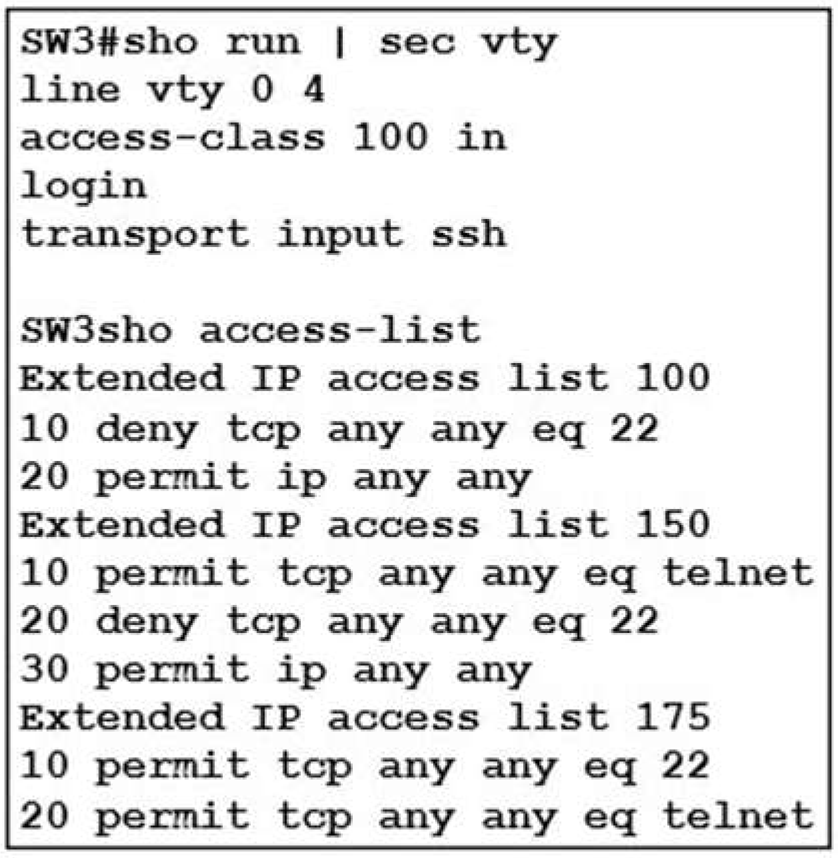


	Core-Switch(config)#ip domain-name crrdp.com
	Core-Switch(config)# crypto key generate rsa
Core-Switch (config)# line console 0 Core-Switch (config-line)# transport input ssh	Core-Switch (config)#ip ssh version 2
	Core-Switch (config)# line vty 0 4 Core-Switch (config-line)#transport input ssh

Section: [none]
Explanation

Explanation/Reference:

QUESTION 13



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

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

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

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 14
On which two topologies can you deploy a point-to-point GRE over IPsec design? (Choose two.)

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

Correct Answer: BC
Section: [none]

Explanation

Explanation/Reference:
Explanation:
In a p2p GRE over IPsec design, the following three topologies can be implemented:

- Hub-and-spoke
- Partial mesh
- Full mesh

Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE/1_p2pGRE_Phase2.html

QUESTION 15
You want to troubleshoot an OSPF adjacency issue. Which two tasks must you perform? (Choose two.)

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

Correct Answer: BD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 16
Which two conditions can you use to filter the output of the **debug condition** command? (Choose two.)

A. interface ID
B. port number
C. packet size
D. protocol
E. username

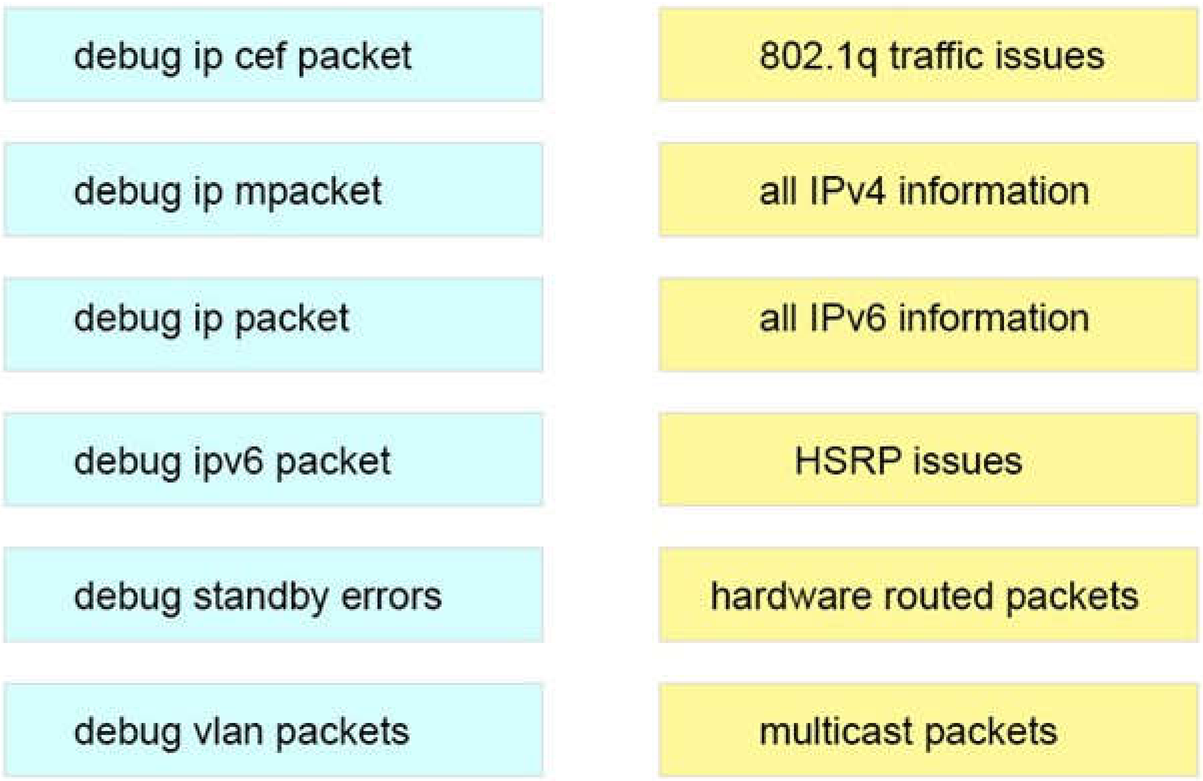
Correct Answer: AE
Section: [none]
Explanation

Explanation/Reference:
Explanation:

```
R1#debug condition ?
  application  Application
  called       called number
  calling      calling
  card         card
  glbp         interface group
  interface    interface
  ip           IP address
  mac-address  MAC address
  match-list   apply the match-list
  standby      interface group
  username     username
  vcid         VC ID
  vlan         vlan
  voice-port   voice-port number
  xconnect     Xconnect conditional debugging on segment pair
```

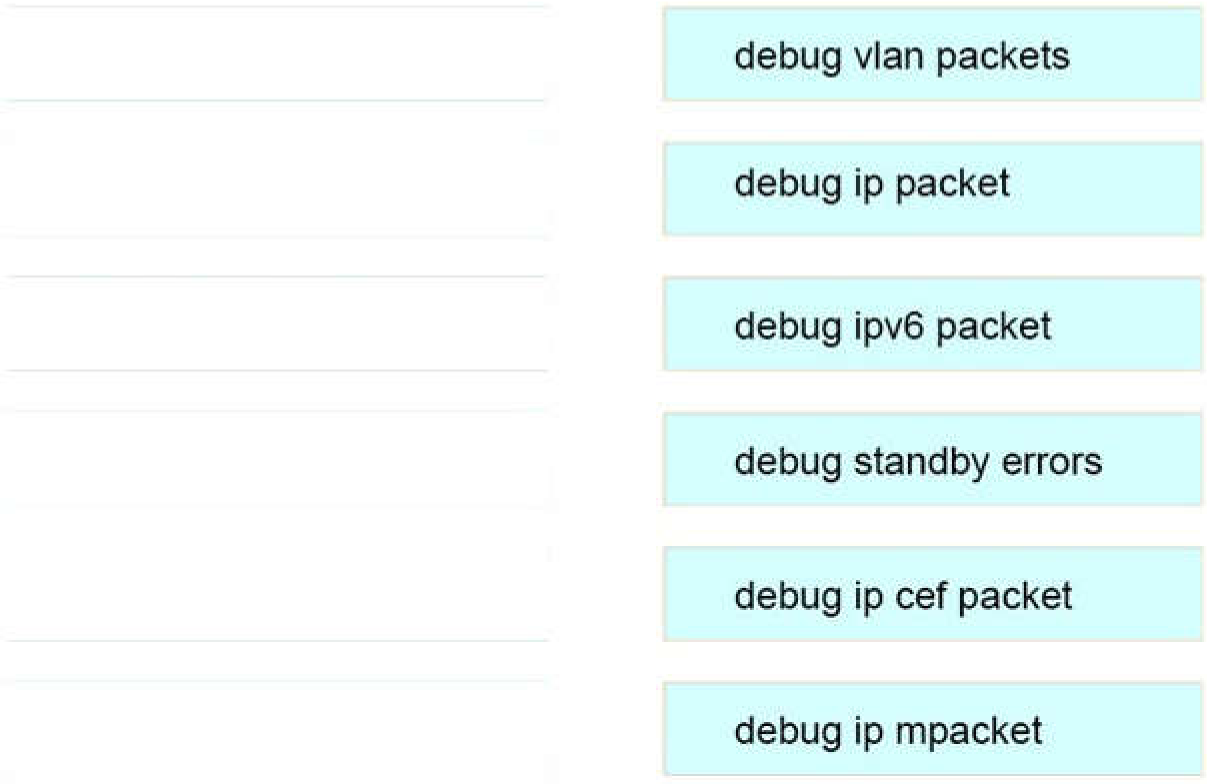
QUESTION 17
DRAG DROP
Drag each debug command on the left to the type of issue it can debug on the right.

Select and Place:



debug ip cef packet	802.1q traffic issues
debug ip mpacket	all IPv4 information
debug ip packet	all IPv6 information
debug ipv6 packet	HSRP issues
debug standby errors	hardware routed packets
debug vlan packets	multicast packets

Correct Answer:



debug vlan packets

debug ip packet

debug ipv6 packet

debug standby errors

debug ip cef packet

debug ip mpacket

Section: [none]
Explanation

Explanation/Reference:

QUESTION 18
Which three keywords are supported in the IP Header Option field of the extended ping command? (Choose three.)

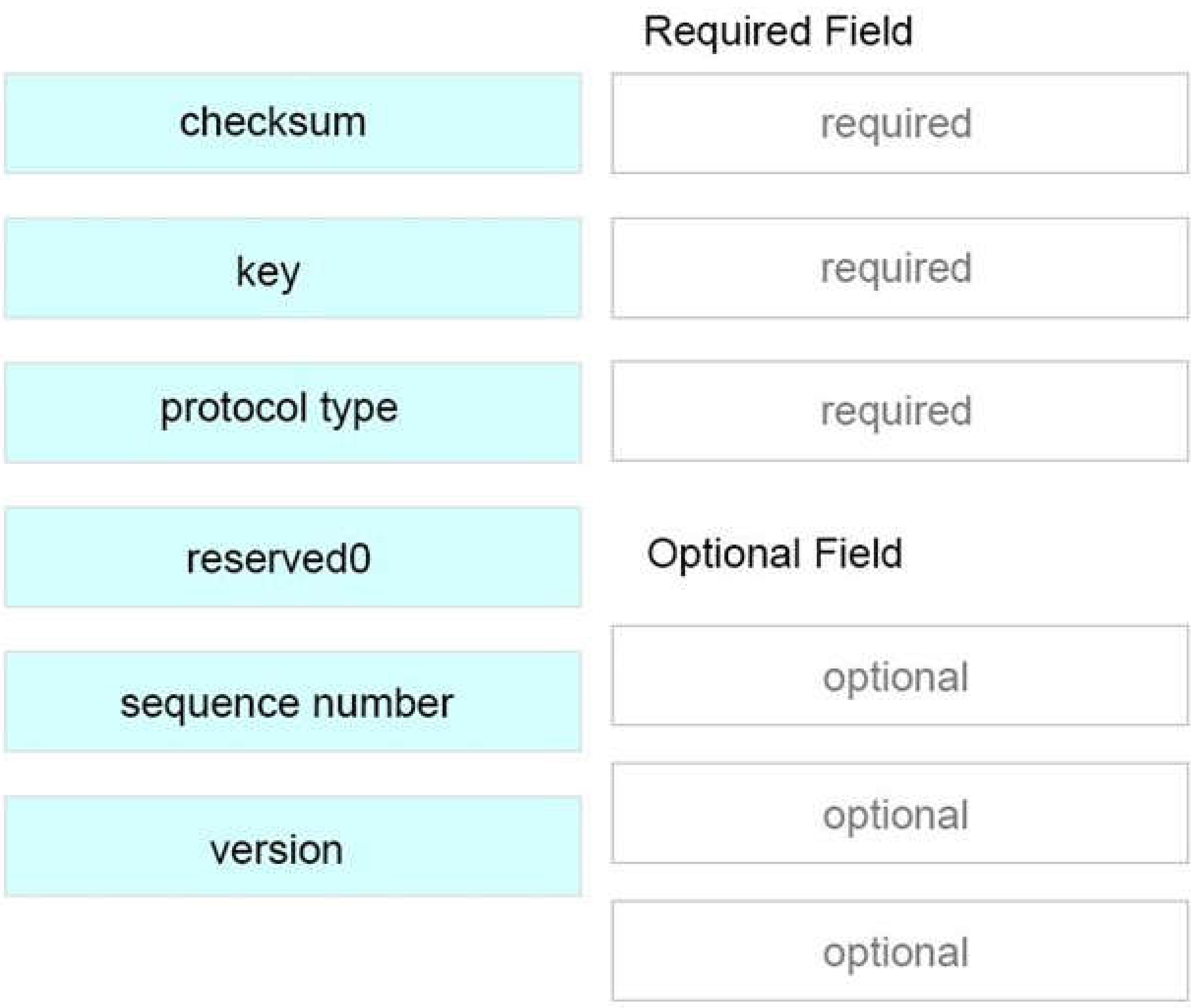
A. Type of Service
B. Timeout
C. Validate
D. Record
E. Strict
F. Timestamp

Correct Answer: DEF
Section: [none]
Explanation

Explanation/Reference:

QUESTION 19
DRAG DROP
Drag and drop the GRE header fields from the left into the Required or Optional categories on the right.

Select and Place:



Required Field

checksum | required

key | required

protocol type | required

reserved0

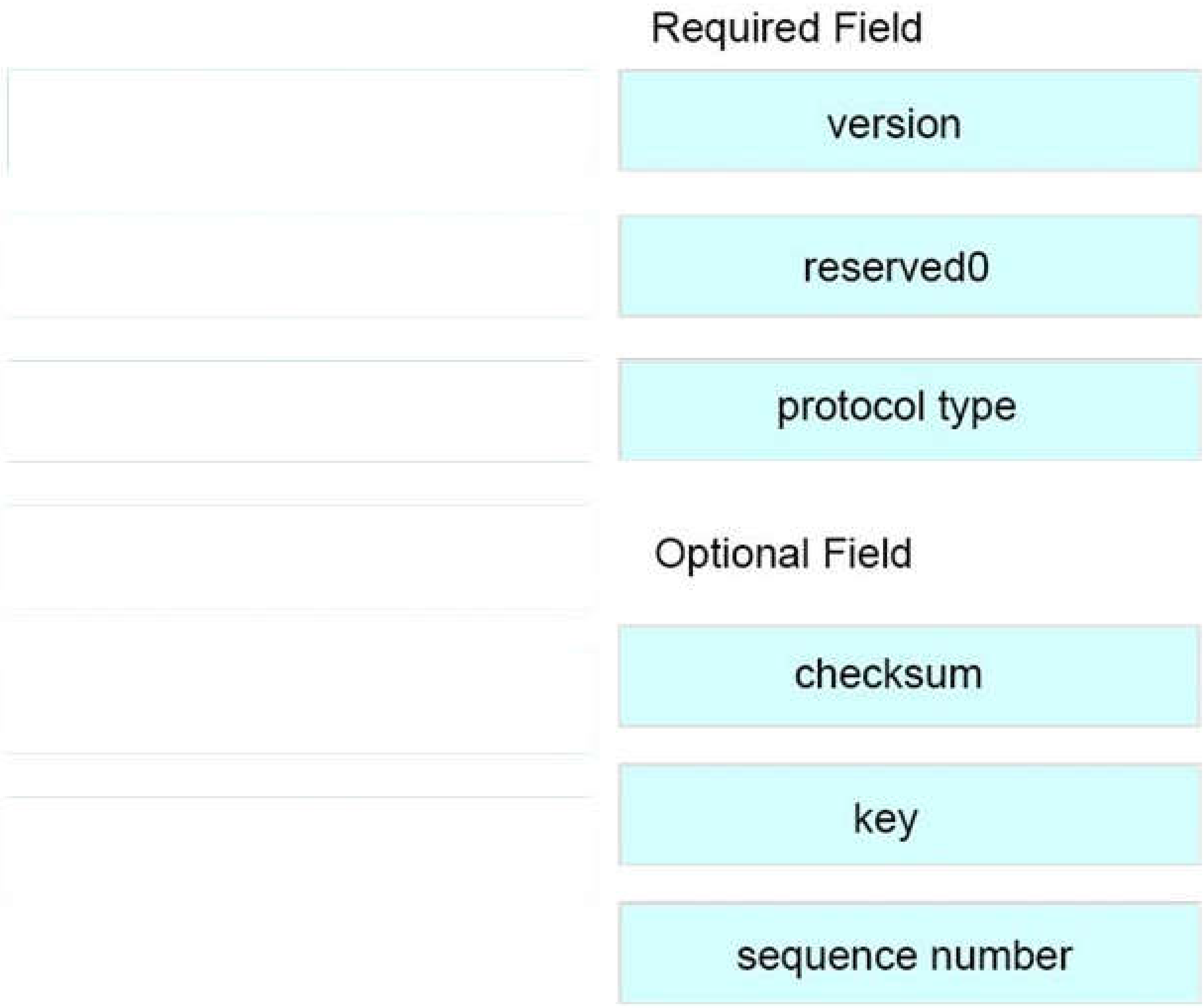
Optional Field

sequence number | optional

version | optional

optional

Correct Answer:



Required Field

version

reserved0

protocol type

Optional Field

checksum

key

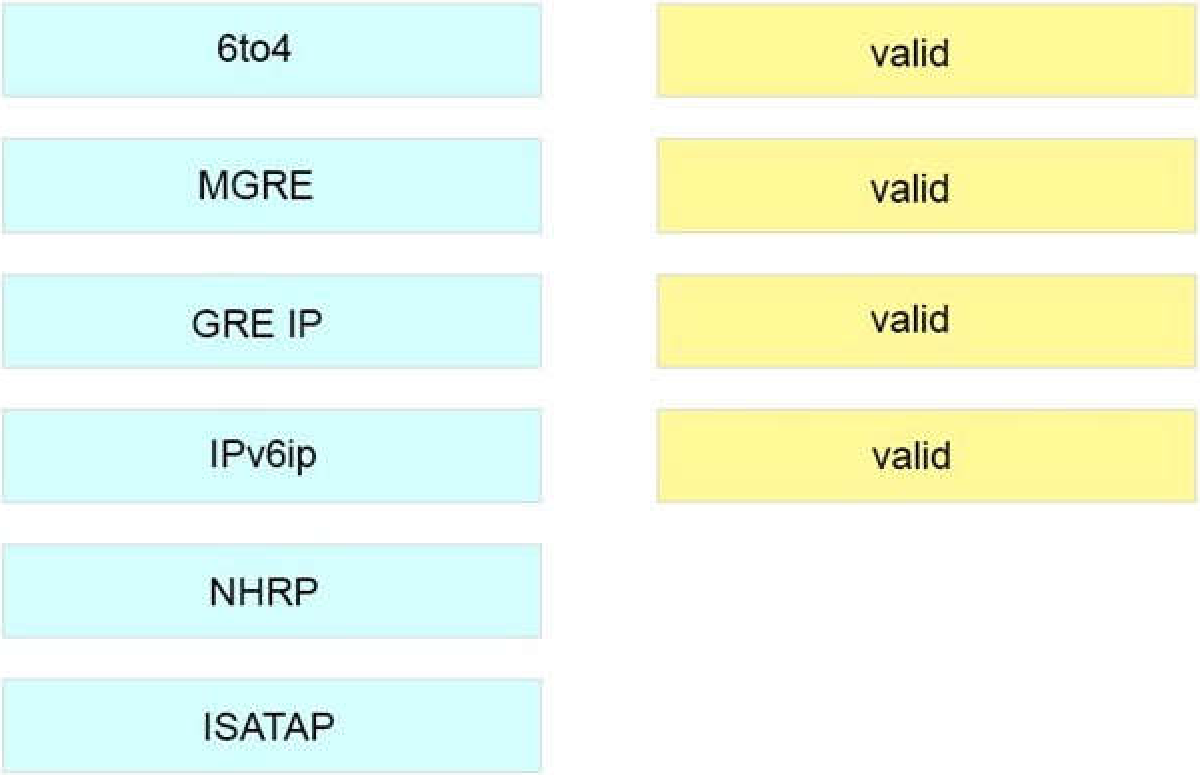
sequence number

Section: [none]
Explanation

Explanation/Reference:

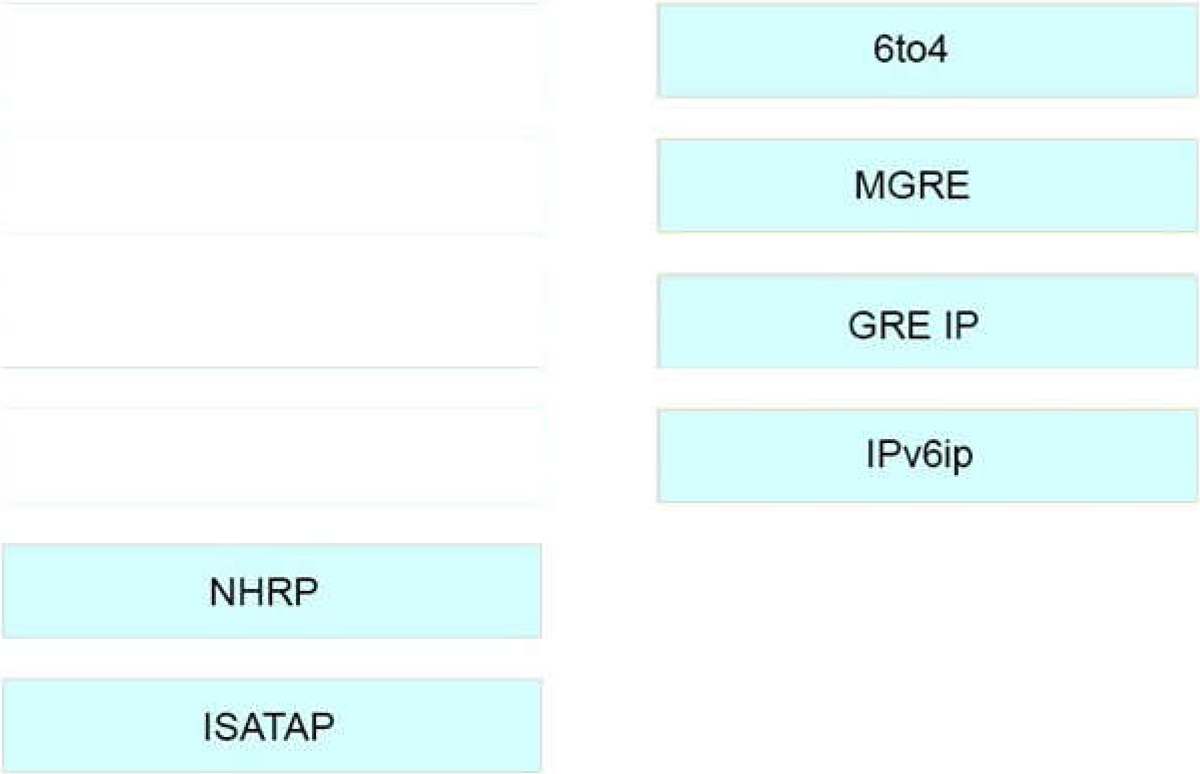
QUESTION 20
DRAG DROP
Drag and drop the valid tunnel modes from the left into the Valid column on the right. Order does not matter and not all options are used.

Select and Place:



6to4	valid
MGRE	valid
GRE IP	valid
IPv6ip	valid
NHRP	
ISATAP	

Correct Answer:



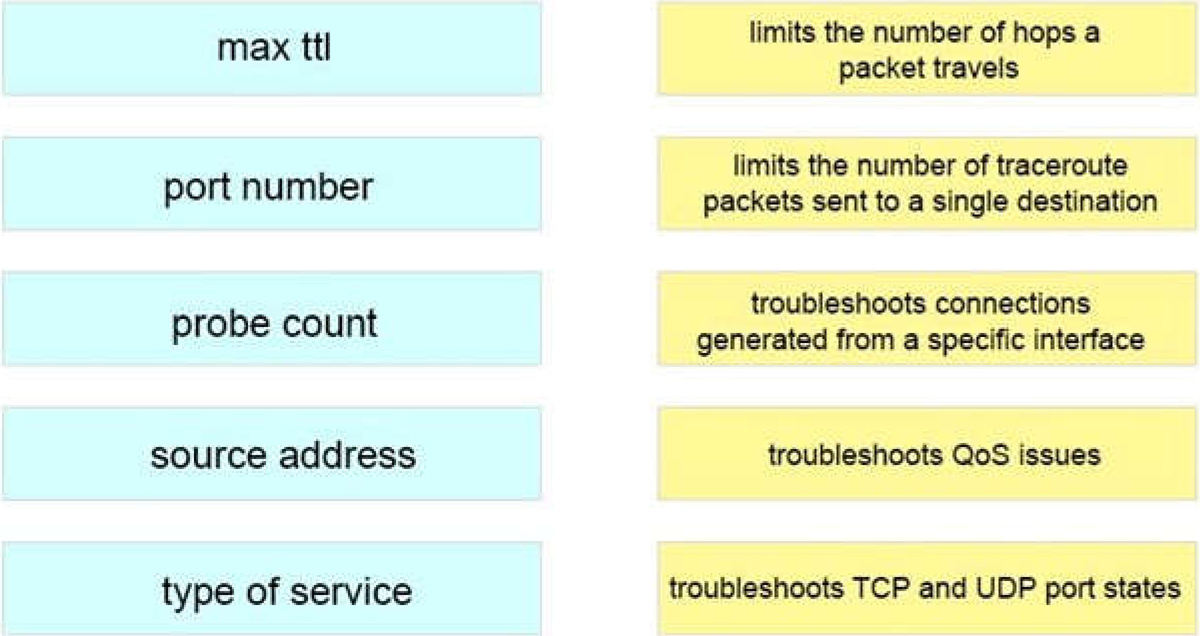
	6to4
	MGRE
	GRE IP
	IPv6ip
NHRP	
ISATAP	

Section: [none]
Explanation

Explanation/Reference:

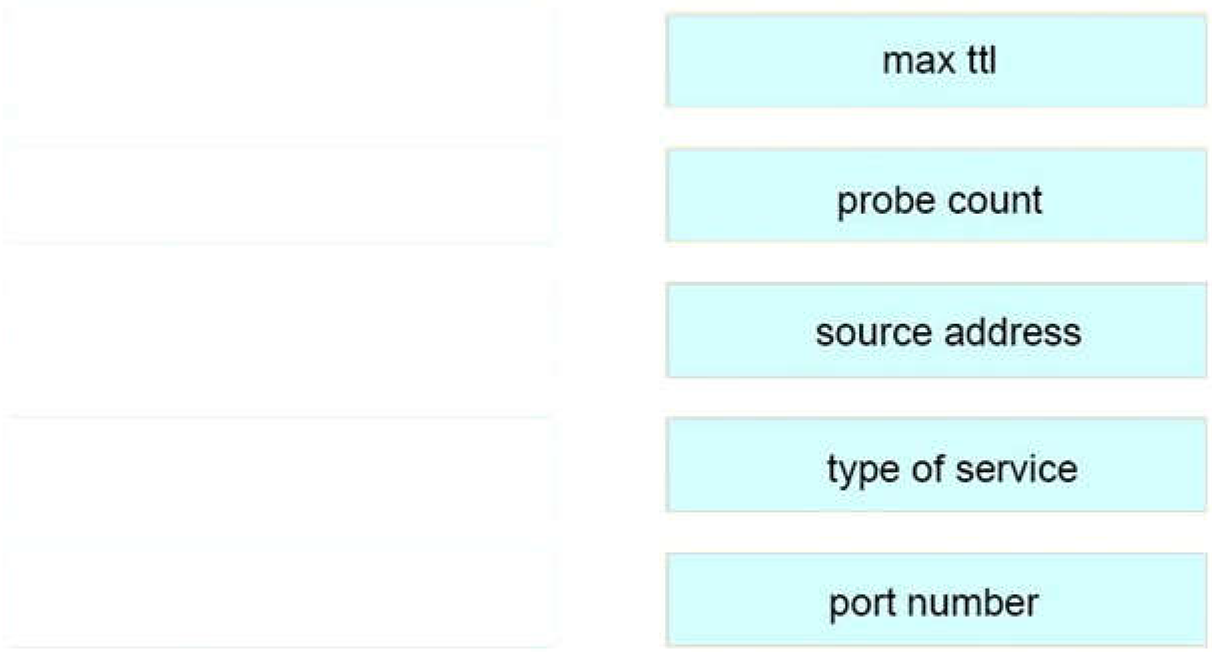
QUESTION 21
DRAG DROP
Drag and drop the extended traceroute options from the left onto the troubleshooting functions they perform on the right.

Select and Place:



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

Correct Answer:

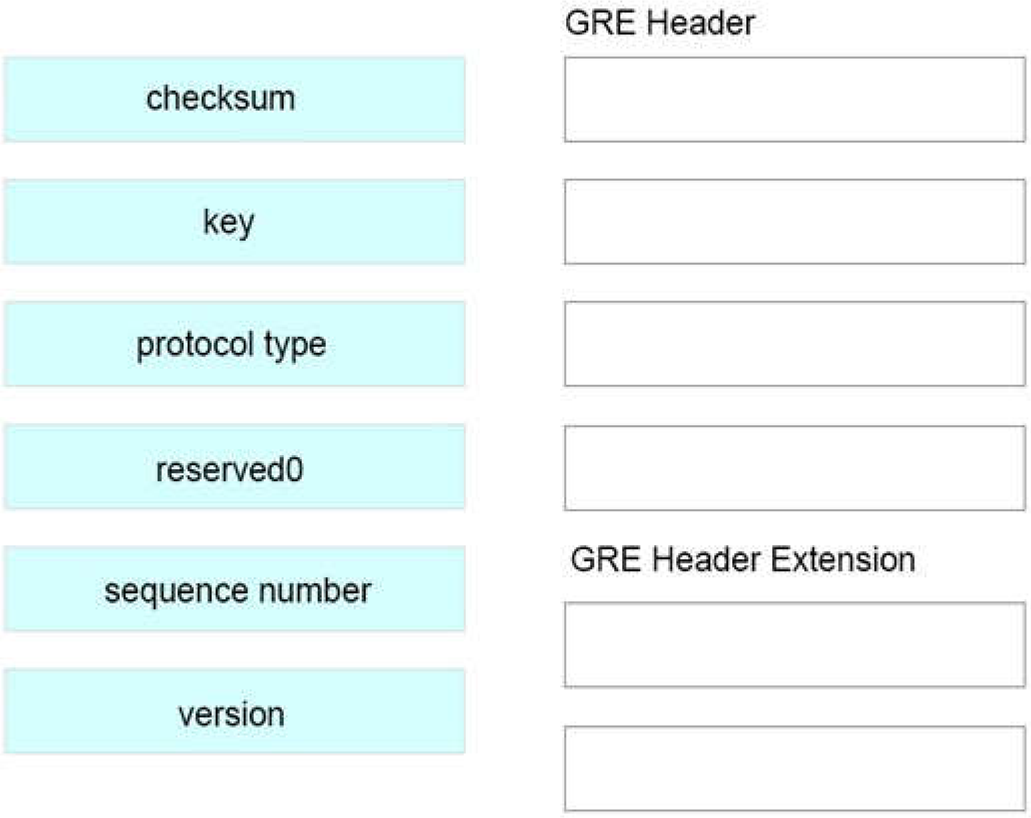


Section: [none]
Explanation

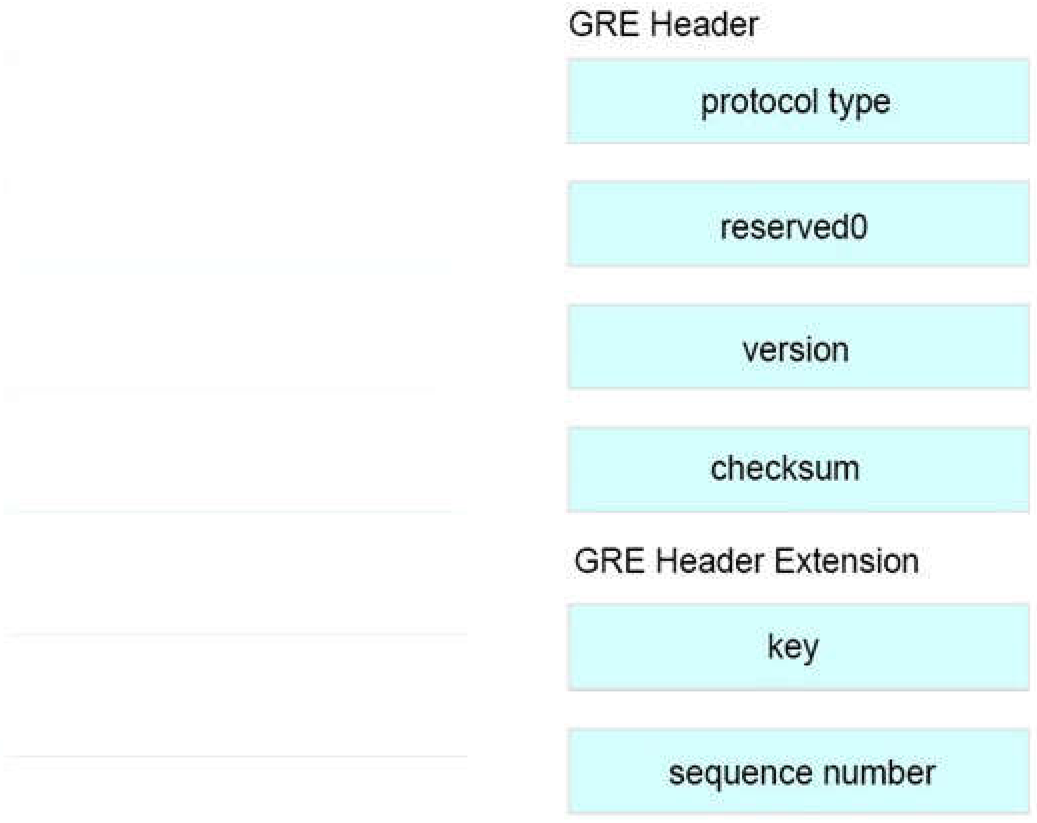
Explanation/Reference:

QUESTION 22
DRAG DROP
Drag and drop the GRE header fields from the left into the correct categories on the right.

Select and Place:



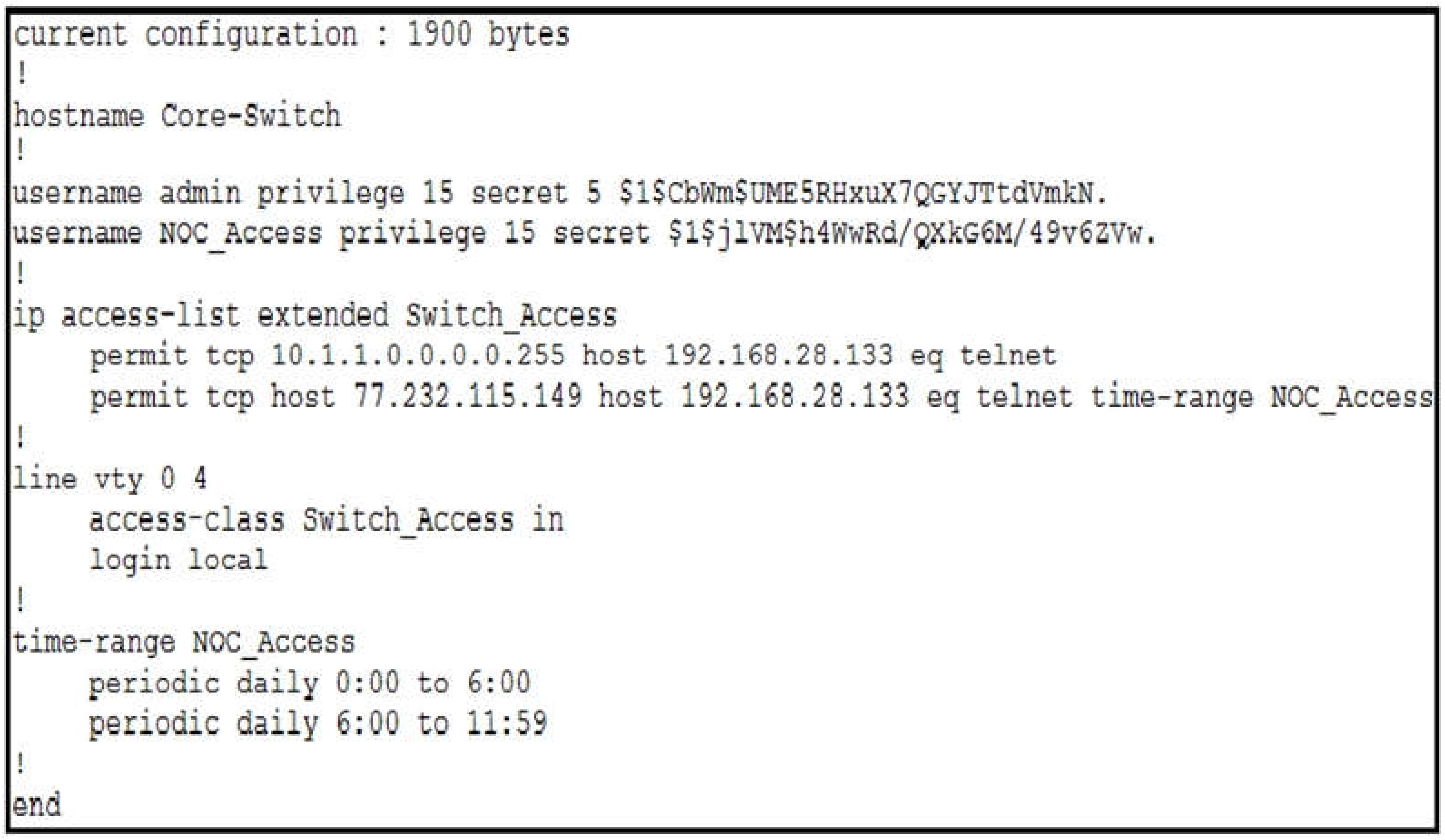
Correct Answer:



Section: [none]
Explanation

Explanation/Reference:

QUESTION 23



```
current configuration : 1900 bytes
!
hostname Core-Switch
!
username admin privilege 15 secret 5 $1$CbWm$UME5RHxuX7QGYJTtdVmkN.
username NOC_Access privilege 15 secret $1$jlVM$h4WwRd/QXkG6M/49v6ZVw.
!
ip access-list extended Switch_Access
    permit tcp 10.1.1.0.0.0.0.255 host 192.168.28.133 eq telnet
    permit tcp host 77.232.115.149 host 192.168.28.133 eq telnet time-range NOC_Access
!
line vty 0 4
    access-class Switch_Access in
    login local
!
time-range NOC_Access
    periodic daily 0:00 to 6:00
    periodic daily 6:00 to 11:59
!
end
```

Refer to the exhibit. The NOC team uses a source address of 77.232.115.149 and requires access only during the hours of 6:00PM through 6:00AM. The configuration is implemented as shown, but the NOC is unable to access the network until midnight. Which configuration is required to fix the problem?

A. **time-range Switch_Access**
periodic daily 18:01 to 5:59

B. **time-range NOC_Access**
periodic daily 0:00 to 6:00
periodic daily 18:00 to 23:59

C. **time-range NOC_Access**
periodic daily 18:01 to 5:59

D. **time-range Switch_Access**
periodic daily 0:00 to 6:00
periodic daily 18:00 to 23:59

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 24

You have configured the **logging console critical** command on a router. Which three alert types display on the console monitor? (Choose three.)

A. warning
B. alert
C. critical
D. debugging
E. notification
F. emergency

Correct Answer: BCF
Section: [none]
Explanation

Explanation/Reference:

QUESTION 25
Which two site-to-site tunnel-based VPN technologies support routing, multicast and private IP addressing? (Choose two.)

A. IPsec VPN
B. GET VPN
C. DMVPN
D. GRE
E. MPLS VPN

Correct Answer: CD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 26
Which type of tunnel supports dynamic routing and carries non-IP traffic?

A. GRE
B. Easy VPN
C. IPsec
D. GET VPN

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 27
You are deploying a new network that requires routing protocols that support TLVs and Fast Reroute. Which two routing protocols must you use? (Choose two.)

A. EIGRP
B. RIPv2
C. OSPF
D. IS-IS
E. RIP

Correct Answer: CD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 28
Which two statements about extended traceroute options are true? (Choose two.)

A. You can change the source port that the UDP probe messages use.
B. You can change the datagram size to troubleshoot clocking problems on serial lines.
C. You can use the Strict IP header option
D. You can change the minimum and maximum TTL
E. You can use the Verbose IP header option to specify the IP address of each hop that the packet takes.

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 29
Which two statements are true regarding login password encryption on Cisco devices? (Choose two.)

A. **enable password** has a higher preference than **enable secret**
B. **enable secret** has a higher preference than **enable password**

C. **enable password** is easy to decipher

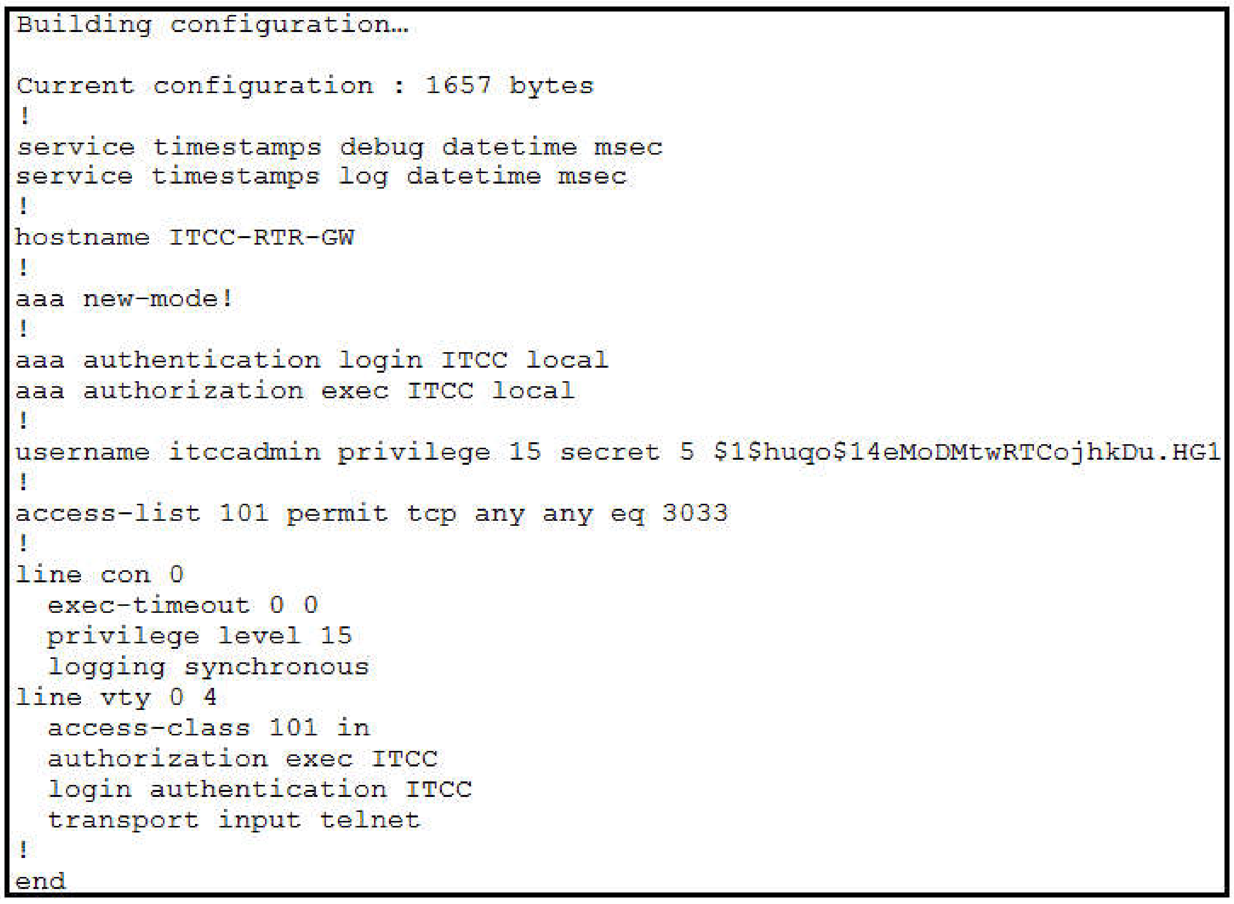
D. **enable password** and **enable secret** cannot be configured together on one device

E. **enable secret** is easy to decipher

Correct Answer: BC
Section: [none]
Explanation

Explanation/Reference:

QUESTION 30



```
Building configuration…

Current configuration : 1657 bytes
!
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname ITCC-RTR-GW
!
aaa new-mode!
!
aaa authentication login ITCC local
aaa authorization exec ITCC local
!
username itccadmin privilege 15 secret 5 $1$huqo$14eMoDMtwRTCojhkDu.HG1
!
access-list 101 permit tcp any any eq 3033
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  access-class 101 in
  authorization exec ITCC
  login authentication ITCC
  transport input telnet
!
end
```

Refer to the exhibit. Your company's security policy requires you to allow telnet access using tcp port 3033 only. You apply the configuration changes as shown and then test. Your telnet attempt fails. Which action would correct the issue?

A. add **rotary 33** to the VTY lines

B. add **access-list 101 deny tcp any any eq 23** to the ACL

C. remove **authorization exec ITCC** from the VTY lines

D. remove **transport input telnet** from the VTY lines

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 31
Which type of system architecture can split point-to-point GRE functions and crypto functions onto separate routing processors?

A. headend

B. client-server

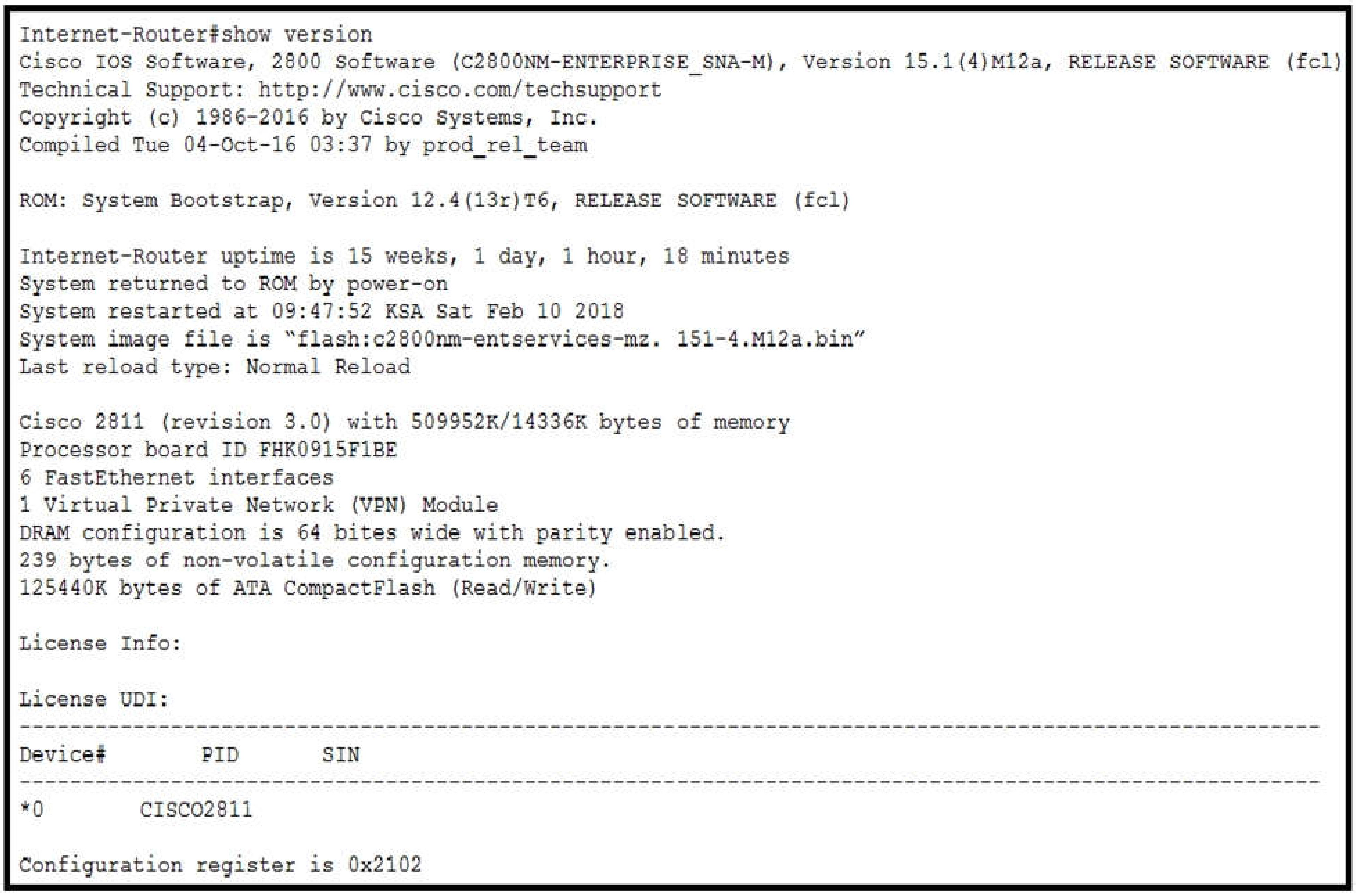
C. backend

D. peer-to-peer

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE/2_p2pGRE_Phase2.html

QUESTION 32



```
Internet-Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ENTERPRISE_SNA-M), Version 15.1(4)M12a, RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 04-Oct-16 03:37 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T6, RELEASE SOFTWARE (fcl)

Internet-Router uptime is 15 weeks, 1 day, 1 hour, 18 minutes
System returned to ROM by power-on
System restarted at 09:47:52 KSA Sat Feb 10 2018
System image file is "flash:c2800nm-entservices-mz. 151-4.M12a.bin"
Last reload type: Normal Reload

Cisco 2811 (revision 3.0) with 509952K/14336K bytes of memory
Processor board ID FHK0915F1BE
6 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bites wide with parity enabled.
239 bytes of non-volatile configuration memory.
125440K bytes of ATA CompactFlash (Read/Write)

License Info:

License UDI:
-------------------------------------------------------------------------------------------------------
Device#       PID       SIN
-------------------------------------------------------------------------------------------------------
*0       CISCO2811

Configuration register is 0x2102
```

Refer to the exhibit. Your client has asked you to replace telnet access with SSH and the configuration has failed. What is the root cause of this issue?

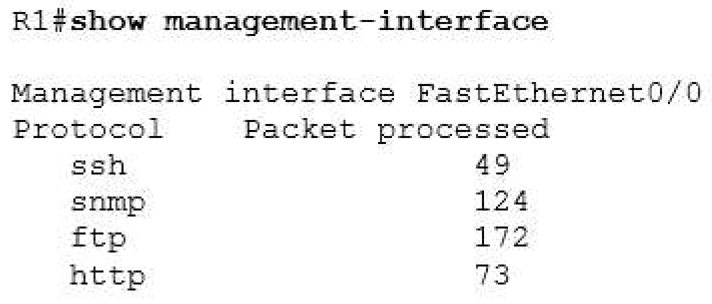
A. The router memory needs to be upgraded
B. The router IOS needs to be updated
C. The Rommon firmware needs to be updated
D. The configuration register is incorrect

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 33
Examine the output from R1. Interface FastEthernet0/0 is used for all management of the device. A client is able to connect to R1 on port 22, however, they are unable to connect on port 23.

What is the cause of the problem?



```
R1#show management-interface

Management interface FastEthernet0/0
Protocol    Packet processed
   ssh                  49
   snmp                 124
   ftp                  172
   http                 73
```

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 34
What are two primary components of a GRE tunnel? (Choose two.)

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

Correct Answer: CE
Section: [none]
Explanation

Explanation/Reference:

QUESTION 35
Which command securely encrypts the enable password on an IOS device?

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 36
Which two statements about extended ping options are true? (Choose two.)

A. You can select the UDP destination port.
B. You can change the minimum and maximum TTL.
C. You can use the Datagram size option to set the size of the ping in bytes.
D. You can use the Data pattern option to troubleshoot framing errors on serial lines.
E. You can use the ToS bit to control fragmentation of the datagram.

Correct Answer: CD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 37
You must connect two remote sites over the public Internet. Multicast support, security, and simplicity are required. Which tunneling technology should you consider?

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 38
You want to troubleshoot a GRE tunnel that is configured with an ACL. Which two tasks must you perform? (Choose two.)

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

Correct Answer: BD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 39
Which command displays the RSA public keys of Cisco router?

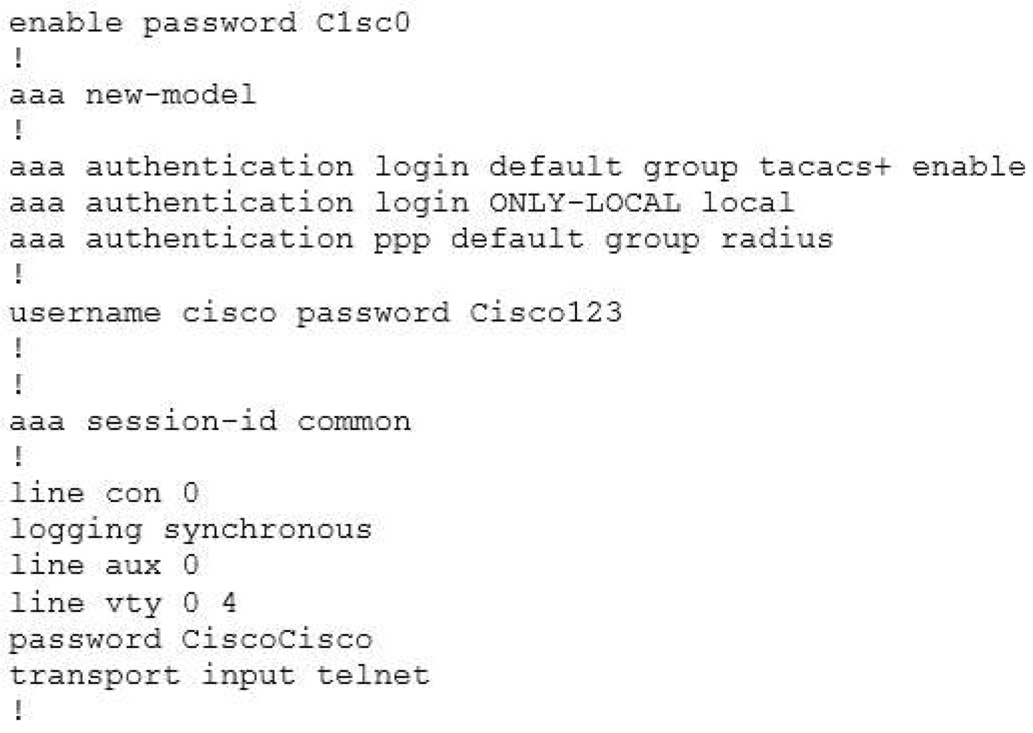
A. **show crypto key mypubkey rsa**
B. **show crypto session local**
C. **show crypto key rsa**

D. **show crypto map**

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/en/US/products/ps6017/products_command_reference_chapter09186a00808ab5a9.html

QUESTION 40
Refer to the configuration. When a user attempts to log in, which authentication method will be used first?



```
enable password C1sc0
!
aaa new-model
!
aaa authentication login default group tacacs+ enable
aaa authentication login ONLY-LOCAL local
aaa authentication ppp default group radius
!
username cisco password Cisco123
!
!
aaa session-id common
!
line con 0
logging synchronous
line aux 0
line vty 0 4
password CiscoCisco
transport input telnet
!
```

A. LOCAL
B. TACACS+
C. RADIUS
D. LINE

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 41
Which two conditions can be used to filter the output of the **debug crypto condition** command? (Choose two.)

A. front-door VRF name
B. routing event filter
C. encryption algorithm
D. ISAKMP profile name
E. destination IP address

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-3s/sec-sec-for-vpns-w-ipsec-xe-3s-book/sec-crypto-debug-sup.pdf

QUESTION 42
Which two features are supported with GRE-based tunnels? (Choose two.)

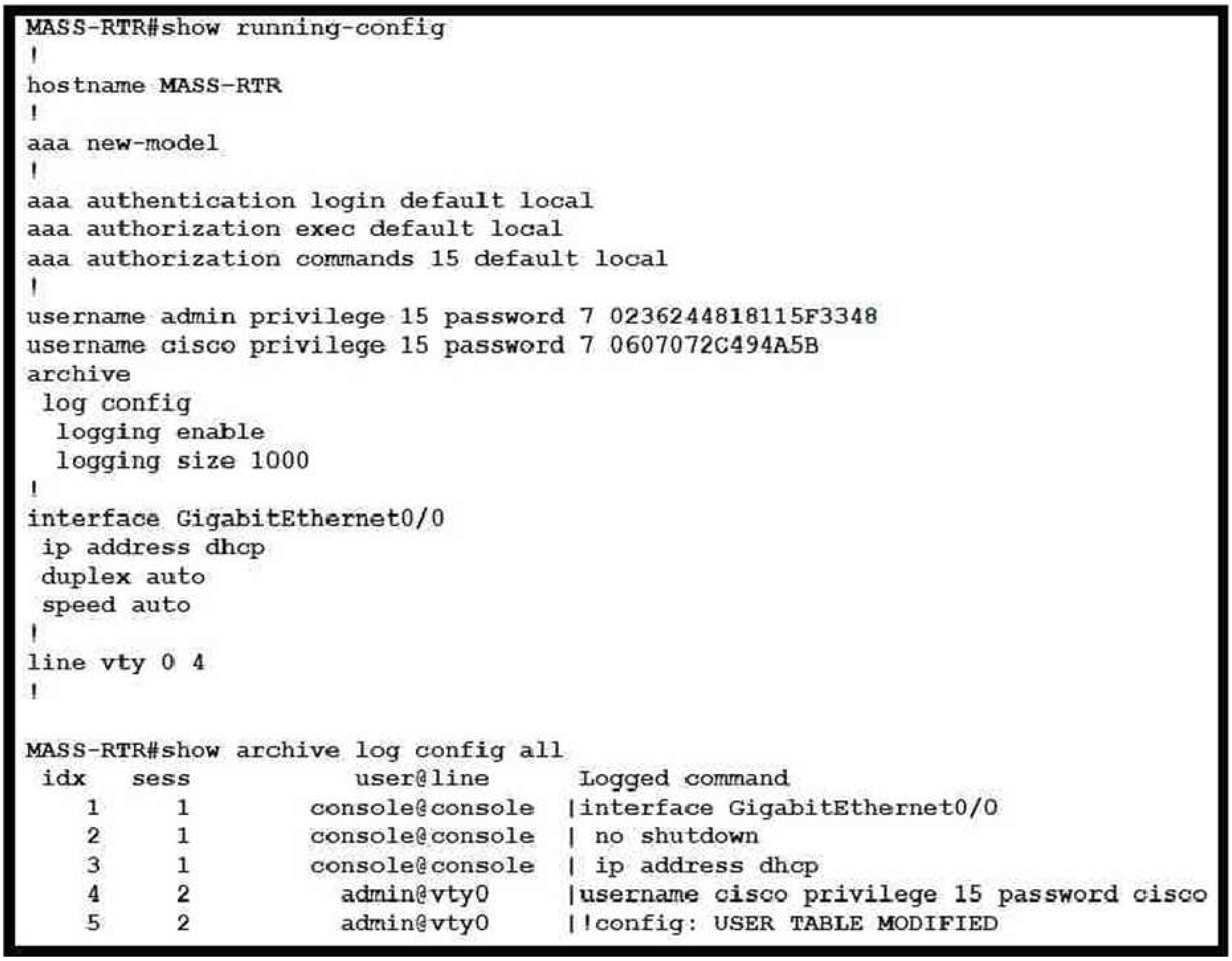
A. any-to-any connectivity
B. encryption
C. multicast traffic forwarding
D. on-demand runnels
E. data encapsulation

Correct Answer: CE
Section: [none]
Explanation

Explanation/Reference:

QUESTION 43
Refer to the exhibit. A client reports that all the password information appears in plain text when the show archive log config all command has been issued.

Which command fixes the issue?



```
MASS-RTR#show running-config
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 0236244818115F3348
username cisco privilege 15 password 7 0607072C494A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

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

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 44
You are troubleshooting a connection between a console port on one router and an AUX port on another router. Which cable type must be used for this connection?

A. Crossover cable
B. Straight cable
C. Rollover cable
D. DB-25 DCE cable

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

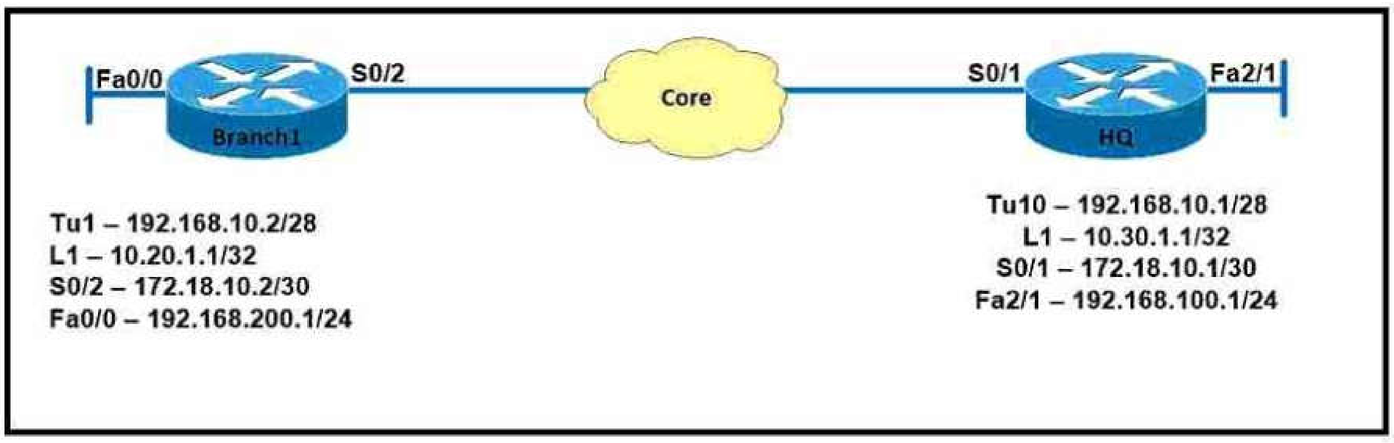
QUESTION 45
Which two statements about GRE tunnels are true? (Choose two.)

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

Correct Answer: AB
Section: [none]
Explanation

Explanation/Reference:

QUESTION 46
Refer to the exhibit. Which IP address should be configured as the tunnel source on the HQ router for maximum resiliency?



A. 10.20.1.1
B. 10.30.1.1
C. 172.18.10.2
D. 192.168.10.1

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

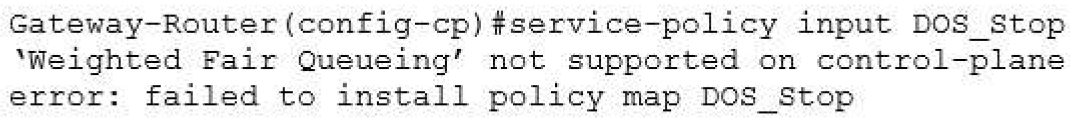
QUESTION 47
What is the ping response to a transmitted echo that needed to be fragmented and fragmentation was not allowed?

A. U
B. M
C. …
D. D

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 48
Refer to the exhibit. A large number of TCP sessions attempting to connect to a router cause memory leakage and the router to hang. During troubleshooting the client configures a service policy and applies it to the control plane in the error shown. What is the root cause of this error message?



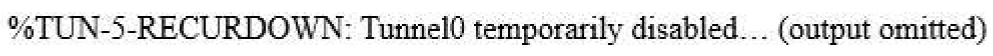
```
Gateway-Router(config-cp)#service-policy input DOS_Stop
'Weighted Fair Queueing' not supported on control-plane
error: failed to install policy map DOS_Stop
```

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

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 49
Refer to the exhibit. Which statement indicates a cause for Tunnel0's connection failure?



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

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 50
When troubleshooting recursive routing issues with GRE tunnels, which three actions resolve the issue? (Choose three.)

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

Correct Answer: CDE
Section: [none]
Explanation

Explanation/Reference:

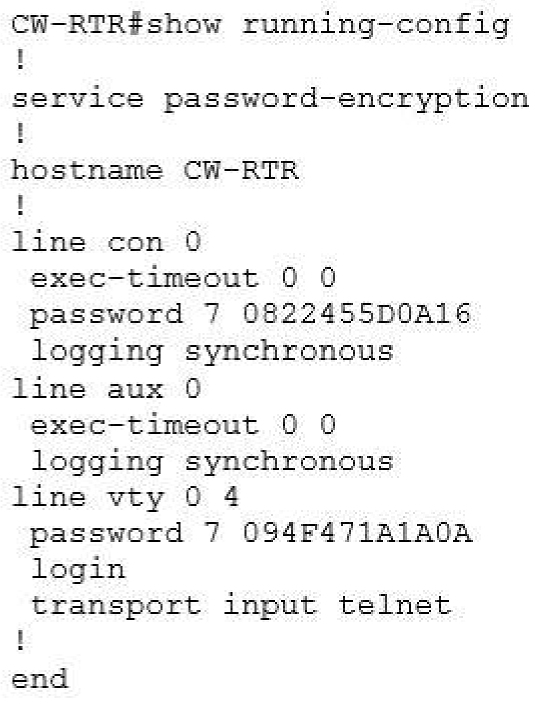
QUESTION 51
What debug command is used to identify and troubleshoot IP Fragmentation and Path Maximum Transmission Unit Discovery issues?

A. debug ip icmp
B. debug ip packet
C. debug ip policy
D. debug ip routing

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 52
Refer to the exhibit. Which outcome regarding a telnet connection to the router is valid?



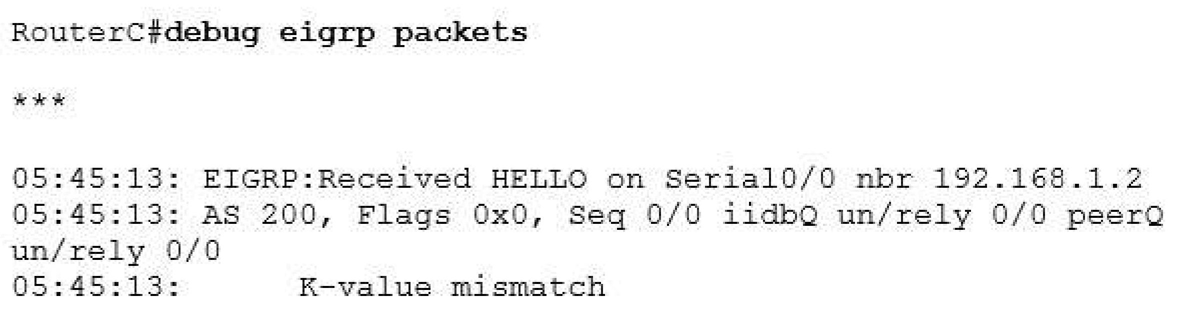
```
CW-RTR#show running-config
!
service password-encryption
!
hostname CW-RTR
!
line con 0
 exec-timeout 0 0
 password 7 0822455D0A16
 logging synchronous
line aux 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password 7 094F471A1A0A
 login
 transport input telnet
!
end
```

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

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 53
Refer to the exhibit. A NOC technician is troubleshooting an EIGRP connection between RouterC, IP address 192.168.1.1, and RouterD, IP address 192.168.1.2. Given the debug output on RouterC, which outcome is valid?



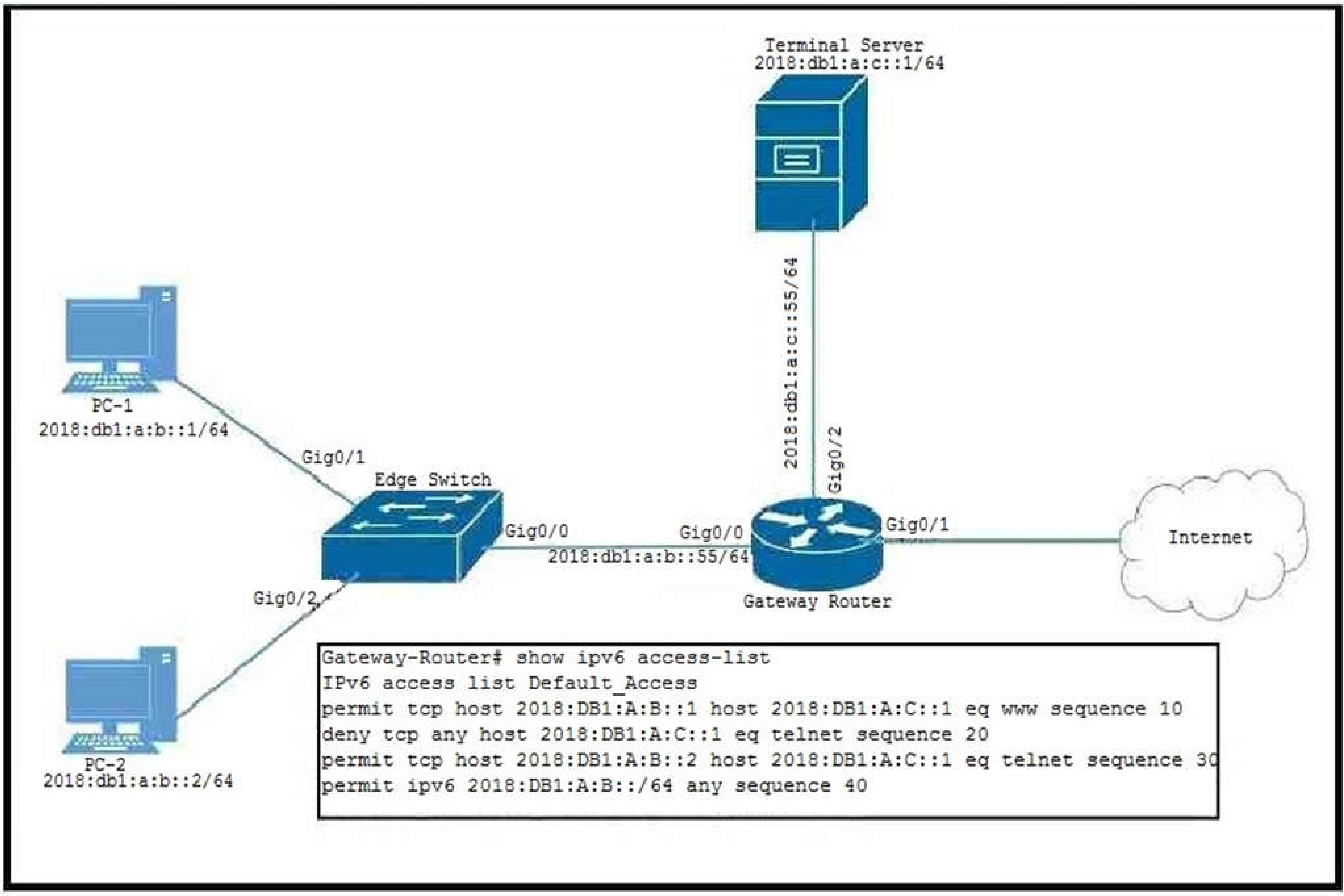
```
RouterC#debug eigrp packets

***

05:45:13: EIGRP:Received HELLO on Serial0/0 nbr 192.168.1.2
05:45:13: AS 200, Flags 0x0, Seq 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
05:45:13:      K-value mismatch
```

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 54
Refer to the exhibit. PC-2 failed to establish a Telnet connection to the Terminal Server. Which solution allows PC-2 to establish the Telnet connection?



```
Gateway-Router# show ipv6 access-list
IPv6 access list Default_Access
permit tcp host 2018:DB1:A:B::1 host 2018:DB1:A:C::1 eq www sequence 10
deny tcp any host 2018:DB1:A:C::1 eq telnet sequence 20
permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet sequence 30
permit ipv6 2018:DB1:A:B::/64 any sequence 40
```

A. Gateway-Router(config)#**ipv6 access-list Default_Access**
   Gateway-Router(config-ipv6-acl)#**no sequence 20**
   Gateway-Router(config-ipv6-acl)#**sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**
B. Gateway-Router(config)#**ipv6 access-list Default_Access**
   Gateway-Router(config-ipv6-acl)#**permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**
C. Gateway-Router(config)#**ipv6 access-list Default_Access**
   Gateway-Router(config-ipv6-acl)#**sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**
D. Gateway-Router(config)#**ipv6 access-list Default_Access**
   Gateway-Router(config-ipv6-acl)#**sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

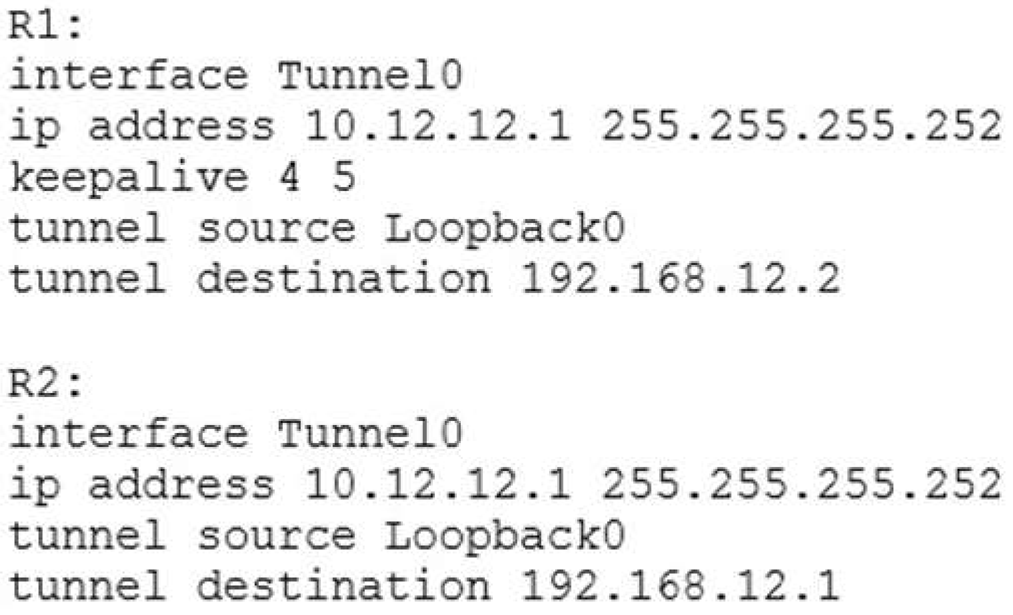
QUESTION 55
Which scenario would cause the tunnel interface on a router to show a status of down/down?

A. The source physical interface is in a down/down state
B. The destination router's physical interface is shut down
C. The **shutdown** command has been issued on the virtual interface
D. The destination address is missing on the tunnel configuration

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 56
Refer to the exhibit. How does the GRE keepalive configuration affect tunnel operation on these two routers?



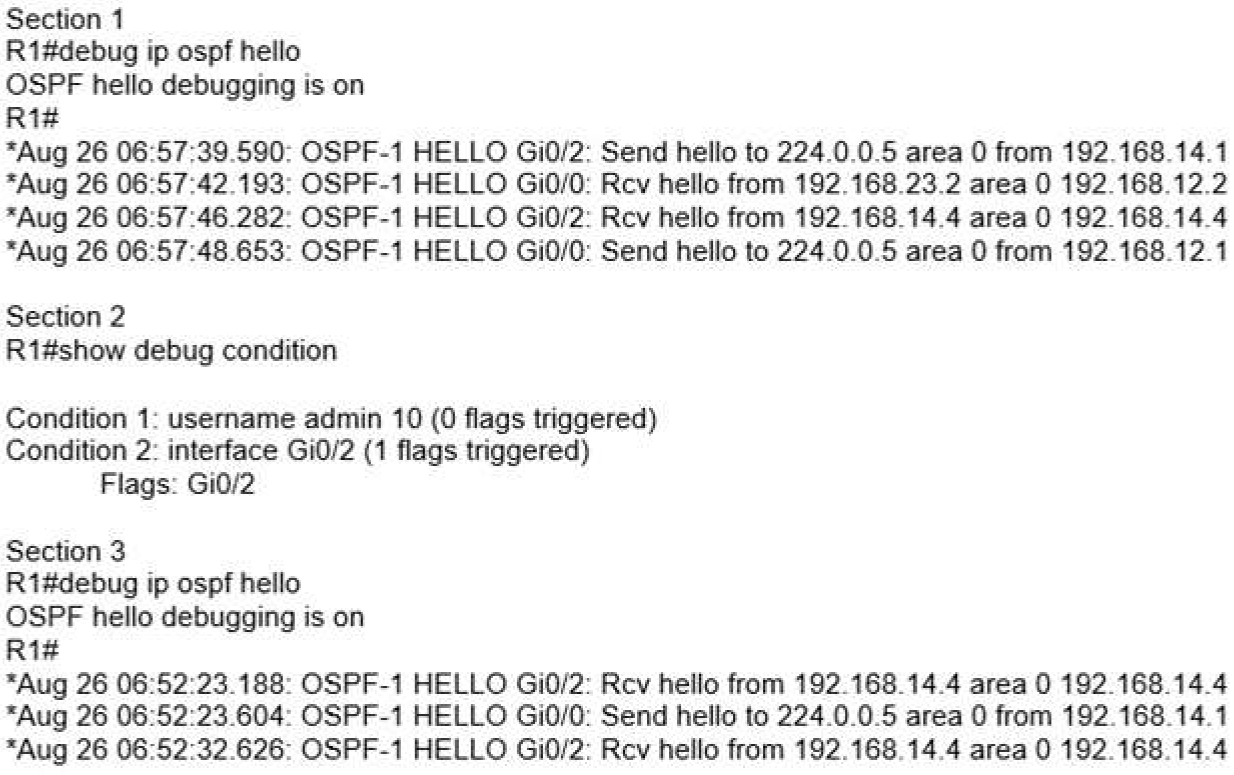
```
R1:
interface Tunnel0
ip address 10.12.12.1 255.255.255.252
keepalive 4 5
tunnel source Loopback0
tunnel destination 192.168.12.2

R2:
interface Tunnel0
ip address 10.12.12.1 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.12.1
```

A. R1 will not send keepalives until keepalives are configured on R2
B. R1 will detect tunnel failures within 5 seconds
C. R1 will detect tunnel failures within 20 seconds
D. R1 will send keepalives, but R2 will not return them

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 57
Refer to the exhibit. Which command will limit the output of the debug ospf hello command as shown in Section 3?



```
Section 1
R1#debug ip ospf hello
OSPF hello debugging is on
R1#
*Aug 26 06:57:39.590: OSPF-1 HELLO Gi0/2: Send hello to 224.0.0.5 area 0 from 192.168.14.1
*Aug 26 06:57:42.193: OSPF-1 HELLO Gi0/0: Rcv hello from 192.168.23.2 area 0 192.168.12.2
*Aug 26 06:57:46.282: OSPF-1 HELLO Gi0/2: Rcv hello from 192.168.14.4 area 0 192.168.14.4
*Aug 26 06:57:48.653: OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 192.168.12.1

Section 2
R1#show debug condition

Condition 1: username admin 10 (0 flags triggered)
Condition 2: interface Gi0/2 (1 flags triggered)
        Flags: Gi0/2

Section 3
R1#debug ip ospf hello
OSPF hello debugging is on
R1#
*Aug 26 06:52:23.188: OSPF-1 HELLO Gi0/2: Rcv hello from 192.168.14.4 area 0 192.168.14.4
*Aug 26 06:52:23.604: OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 192.168.14.1
*Aug 26 06:52:32.626: OSPF-1 HELLO Gi0/2: Rcv hello from 192.168.14.4 area 0 192.168.14.4
```

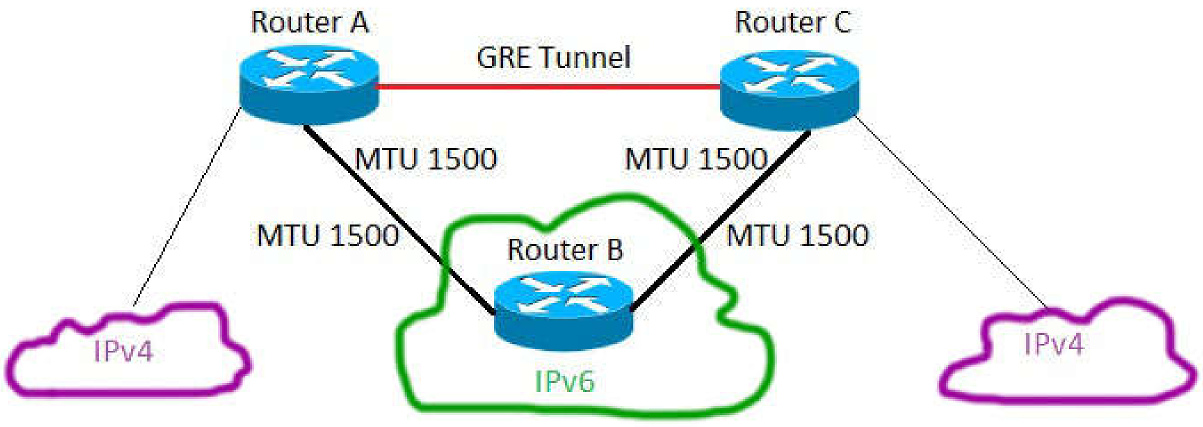
A. debug condition interface Gi0/0
B. debug condition interface Gi0/2
C. debug condition ip 224.0.0.5
D. no debug condition ip 192.168.13.3

Correct Answer: B

Section: [none]
Explanation

Explanation/Reference:

QUESTION 58
Refer to the exhibit. MTU has been configured as shown, and no MTU command has been configured on the tunnel interfaces. It has been found that fragmentation is occurring when tunneled packets are placed onto the IPv6 underlay network. Which configuration change will resolve this problem?

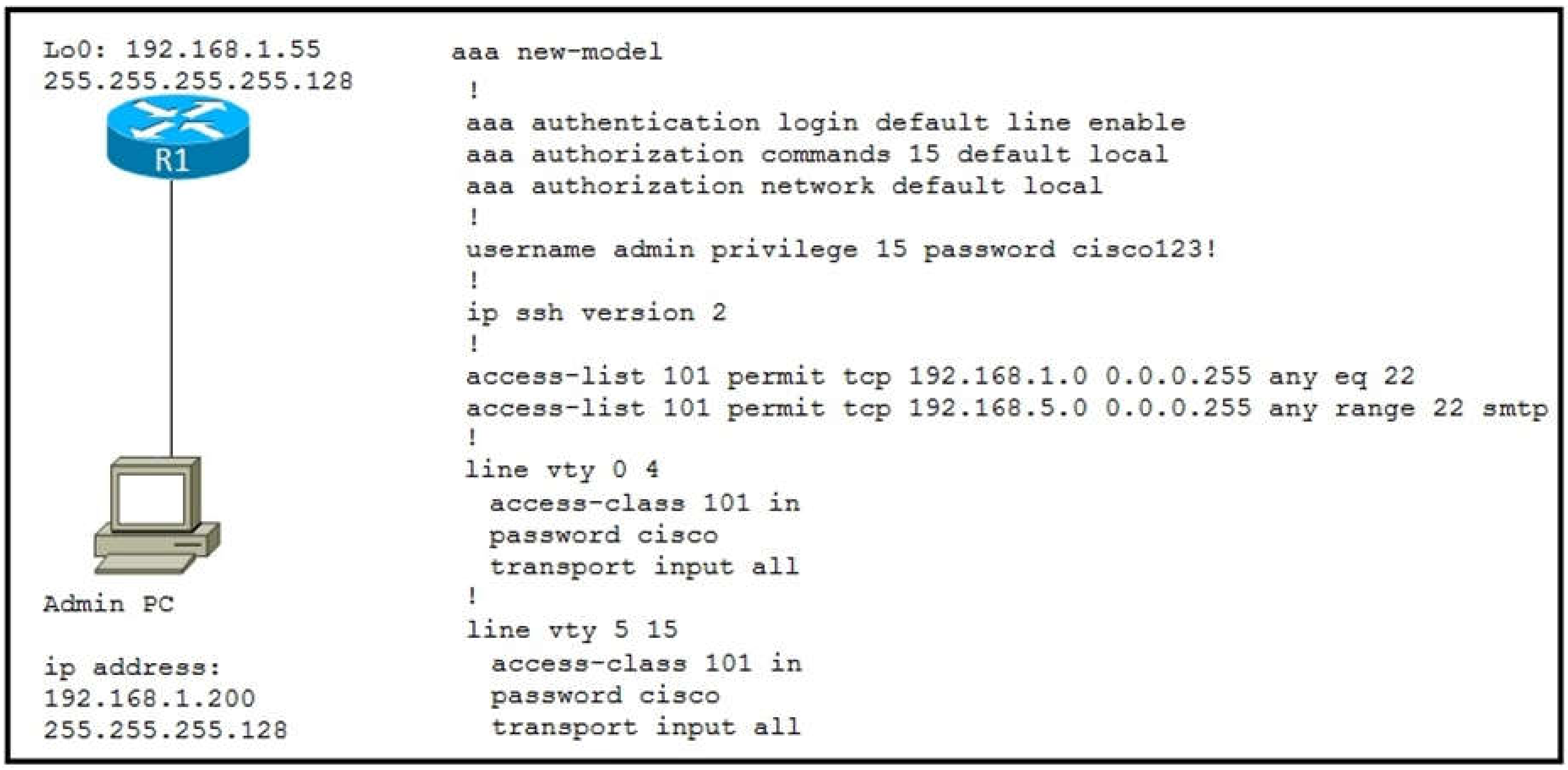


A. Set the MTU to 1476 on the tunnel interfaces
B. Increase the MTU on the IPv6 network
C. Set the MTU to 1500 on the tunnel interfaces
D. Increase the MTU on the IPv4 networks

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 59
Refer to the exhibit. Which command will allow the administrator to log in using the device database authentication?



```
Lo0: 192.168.1.55
255.255.255.255.128

Admin PC

ip address:
192.168.1.200
255.255.255.128
```

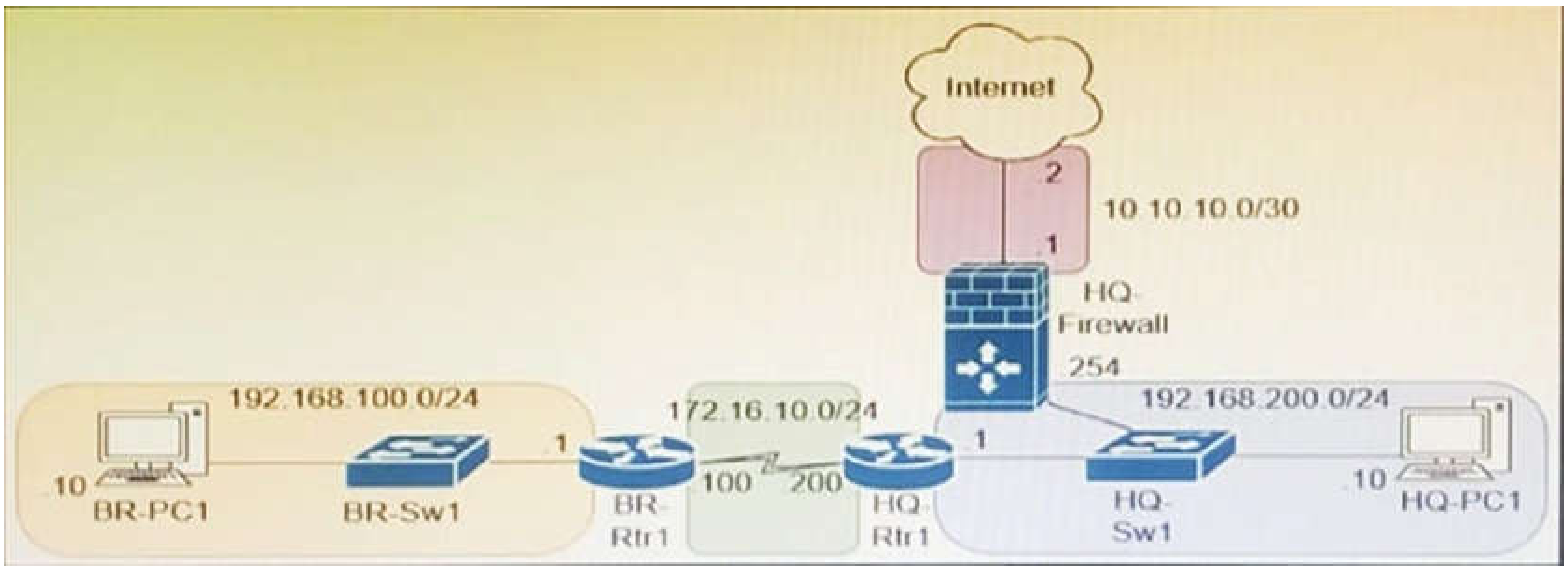
```
aaa new-model
 !
 aaa authentication login default line enable
 aaa authorization commands 15 default local
 aaa authorization network default local
 !
 username admin privilege 15 password cisco123!
 !
 ip ssh version 2
 !
 access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 22
 access-list 101 permit tcp 192.168.5.0 0.0.0.255 any range 22 smtp
 !
 line vty 0 4
  access-class 101 in
  password cisco
  transport input all
 !
 line vty 5 15
  access-class 101 in
  password cisco
  transport input all
```

A. aaa authentication login default local
B. aaa authorization network default local
C. aaa authentication login default enable
D. aaa authorization exec default local

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 60
Refer to the exhibit. BR-PC1 (192.168.100.10) is unable to reach the Internet. Access to the Internet is routed through the HQ site and all NAT configurations have been applied and verified. The user on BR-PC1 has attempted to ping www.cisco.com and did not receive any responses. Which troubleshooting step will assist with root cause analysis by displaying a series of upstream connected devices?



A. Check the physical link from HQ-Firewall to HQ-Sw1
B. Run an nslookup to www.cisco.com
C. Check HQ-Firewall to see if it's blocking HTTP traffic
D. Run a traceroute to www.cisco.com

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

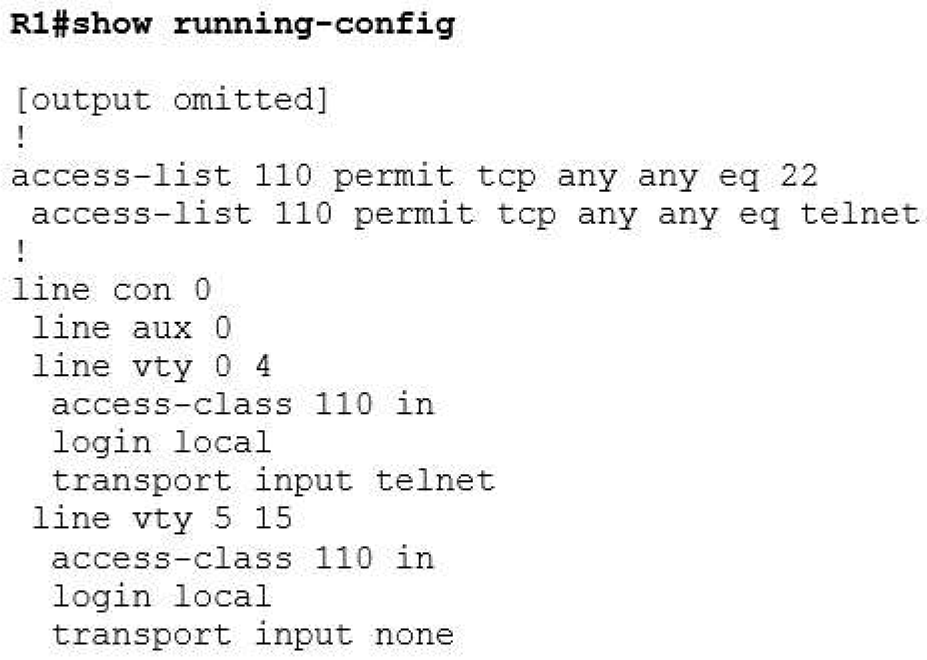
QUESTION 61
A syslog message from a router with a GRE tunnel reads: "%TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing". Which scenario would cause this error?

A. The remote router's tunnel interface is not participating in the routing process.
B. The local tunnel mode does not match the tunnel mode configured on the remote router.
C. The **shutdown** command has been issued on the source physical interface.
D. The installed route to the tunnel destination has been learned via the tunnel interface.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 62
Refer to the exhibit. All routing has been confirmed working as expected. The network administrator is unable to log into router R1 via SSH. Which statement describes the issue?



```
R1#show running-config

[output omitted]
!
access-list 110 permit tcp any any eq 22
 access-list 110 permit tcp any any eq telnet
!
line con 0
 line aux 0
 line vty 0 4
  access-class 110 in
  login local
  transport input telnet
 line vty 5 15
  access-class 110 in
  login local
  transport input none
```

A. Access-list 110 is not applied in the correct direction on the VTY interfaces.
B. The **transport input** command on VTY 0-4 is only allowing telnet.
C. The **access-group** command should be used on VTY lines.
D. Access-list 110 is implicitly denying the authentication attempt.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 63
An engineer is attempting to configure a secure connection to a device. During testing, the login is not working. Which statement describes the root cause?

A. Only SSHv1 is allowed and you are trying to configure SSHv2
B. Domain name has been configured
C. The **transport input ssh** command is missing
D. The old RSA key pair needs to be deleted first

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 64
Which technology is used to monitor and collect the utilization statistics of Cisco IOS devices to determine the overall health of those devices?

A. ICMP
B. LLDP
C. HSRP
D. SNMP

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

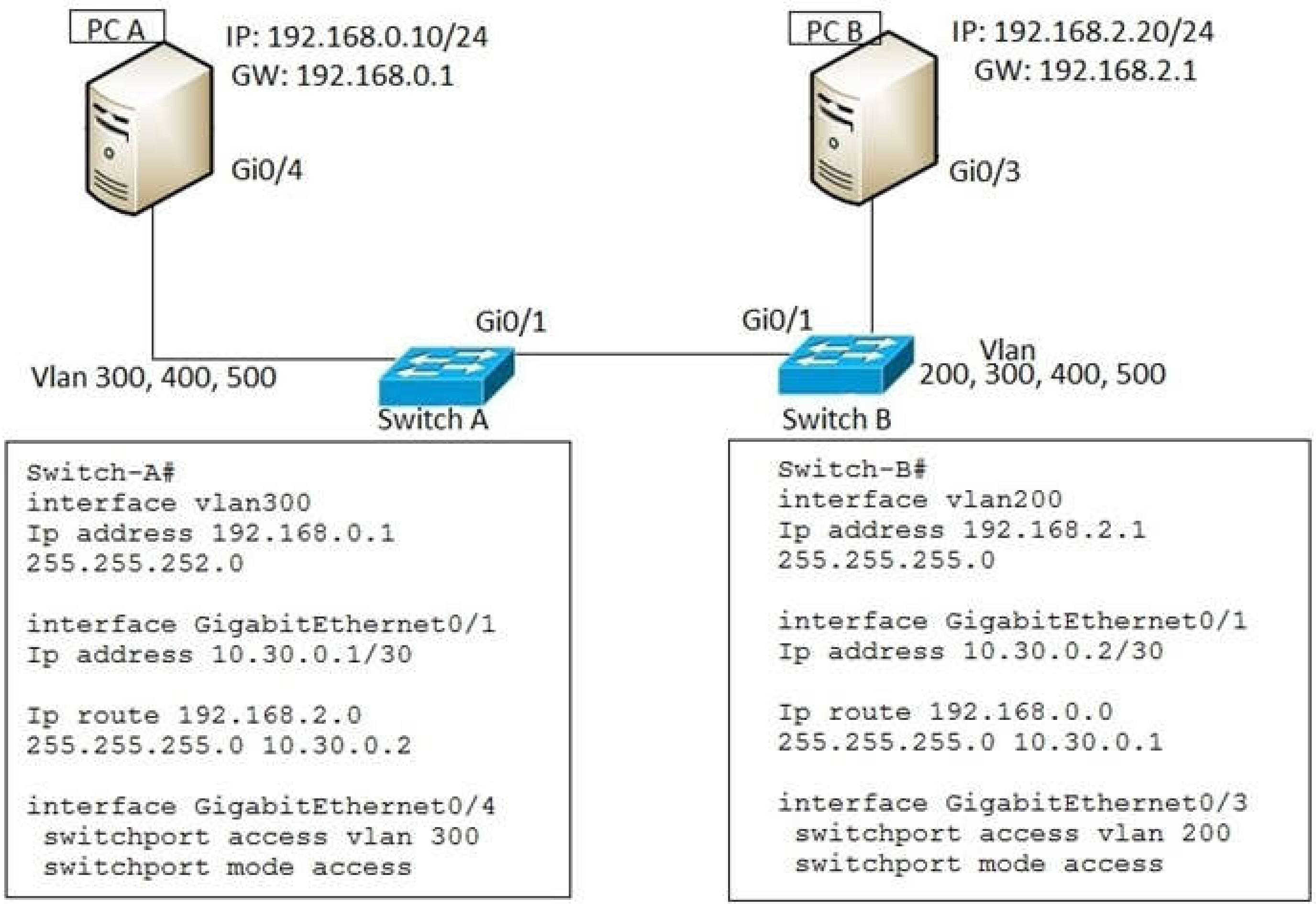
QUESTION 65
An engineer wants to verify the access control lists that are applied on interface gigabitethernet0/0. Which command provides the desired output?

A. show ip access lists applied
B. show interface gigabitethernet 0/0
C. show ip access-lists interface gigabitethernet 0/0
D. show interface gigabitethernet 0/0 stats

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 66
Refer to the exhibit. PC A is able to ping its gateway but is unable to access resources in VLAN 200. Which statement describes the root cause?



```
Switch-A#
interface vlan300
Ip address 192.168.0.1
255.255.252.0

interface GigabitEthernet0/1
Ip address 10.30.0.1/30

Ip route 192.168.2.0
255.255.255.0 10.30.0.2

interface GigabitEthernet0/4
 switchport access vlan 300
 switchport mode access
```

```
Switch-B#
interface vlan200
Ip address 192.168.2.1
255.255.255.0

interface GigabitEthernet0/1
Ip address 10.30.0.2/30

Ip route 192.168.0.0
255.255.255.0 10.30.0.1

interface GigabitEthernet0/3
 switchport access vlan 200
 switchport mode access
```

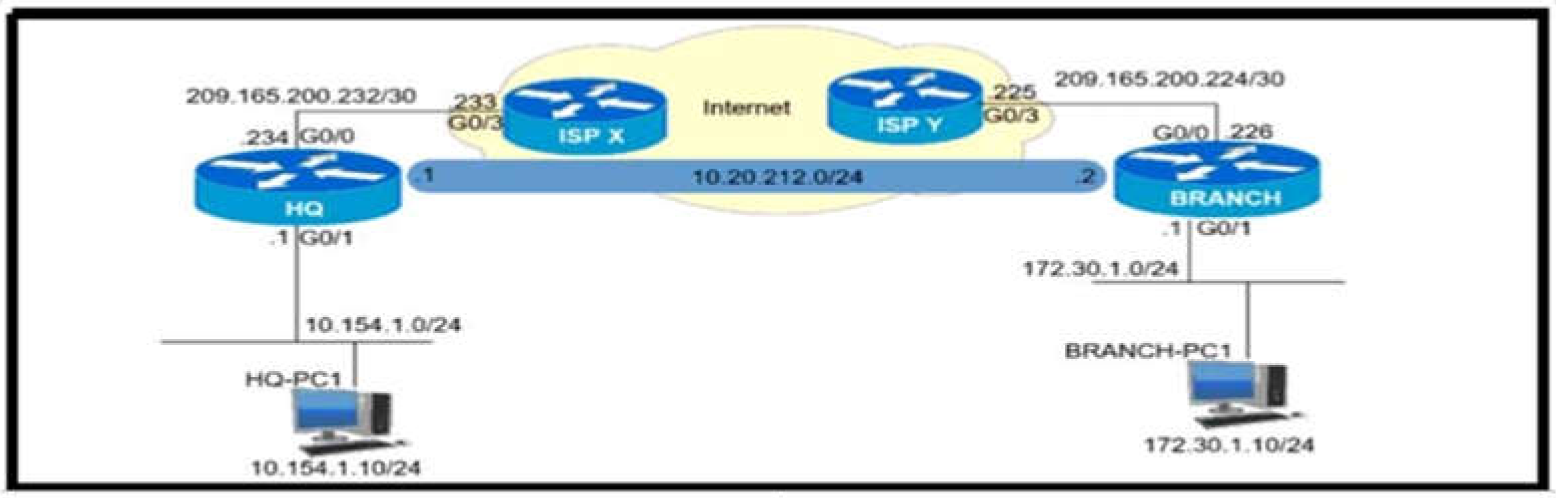
A. Interface VLAN 300 needs also to be configured on Switch B.
B. An ACL is needed on Switch A Gi0/1 to allow traffic to pass.
C. The subnet mask for interface VLAN 300 does not match the subnet mask for PC A.
D. There needs to be a port channel between Switch A and Switch B to communicate properly.

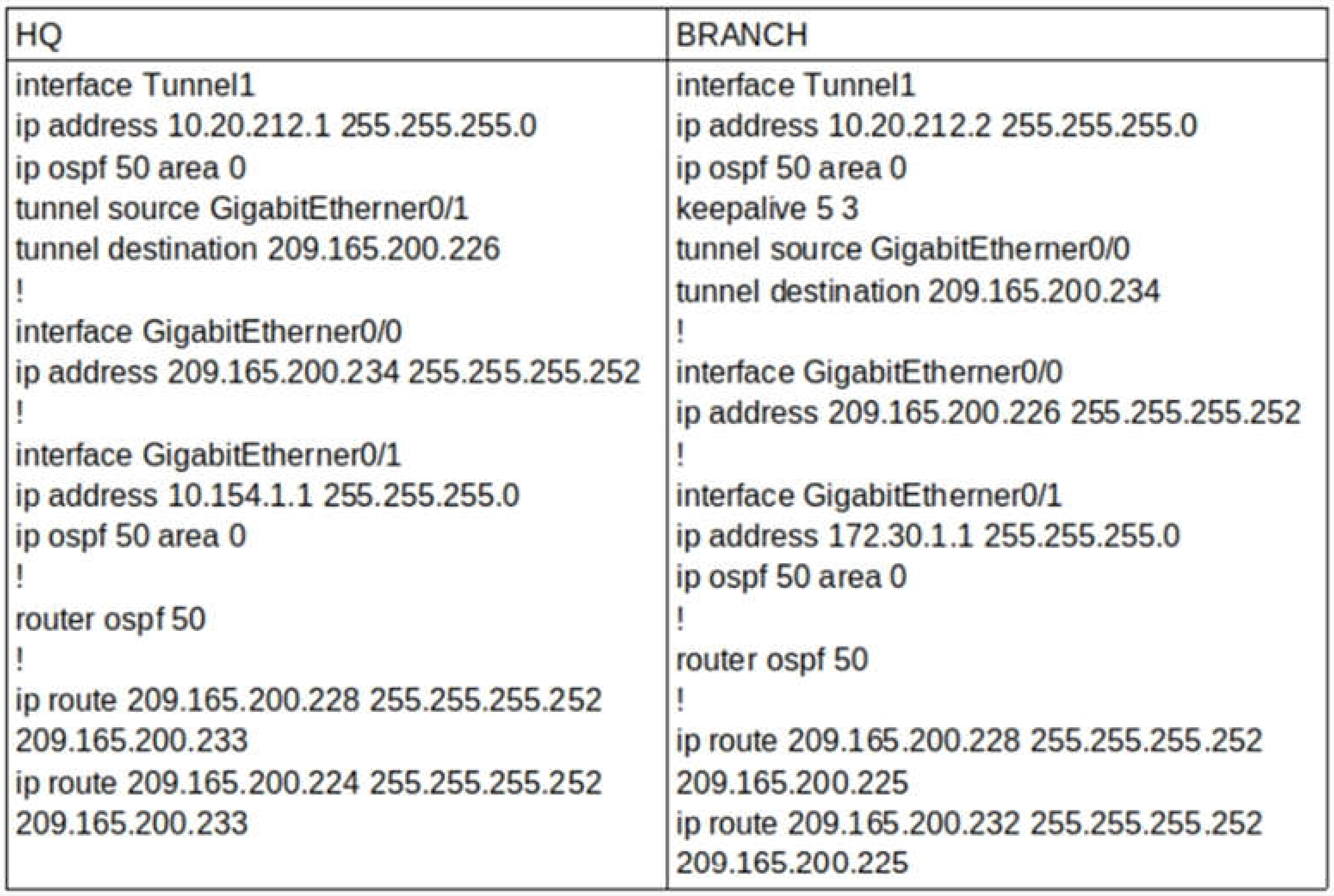
Correct Answer: C

Section: [none]
Explanation

Explanation/Reference:

QUESTION 67
Refer to the exhibit.





HQ	BRANCH
interface Tunnel1 ip address 10.20.212.1 255.255.255.0 ip ospf 50 area 0 tunnel source GigabitEtherner0/1 tunnel destination 209.165.200.226 ! interface GigabitEtherner0/0 ip address 209.165.200.234 255.255.255.252 ! interface GigabitEtherner0/1 ip address 10.154.1.1 255.255.255.0 ip ospf 50 area 0 ! router ospf 50 ! ip route 209.165.200.228 255.255.255.252 209.165.200.233 ip route 209.165.200.224 255.255.255.252 209.165.200.233	interface Tunnel1 ip address 10.20.212.2 255.255.255.0 ip ospf 50 area 0 keepalive 5 3 tunnel source GigabitEtherner0/0 tunnel destination 209.165.200.234 ! interface GigabitEtherner0/0 ip address 209.165.200.226 255.255.255.252 ! interface GigabitEtherner0/1 ip address 172.30.1.1 255.255.255.0 ip ospf 50 area 0 ! router ospf 50 ! ip route 209.165.200.228 255.255.255.252 209.165.200.225 ip route 209.165.200.232 255.255.255.252 209.165.200.225

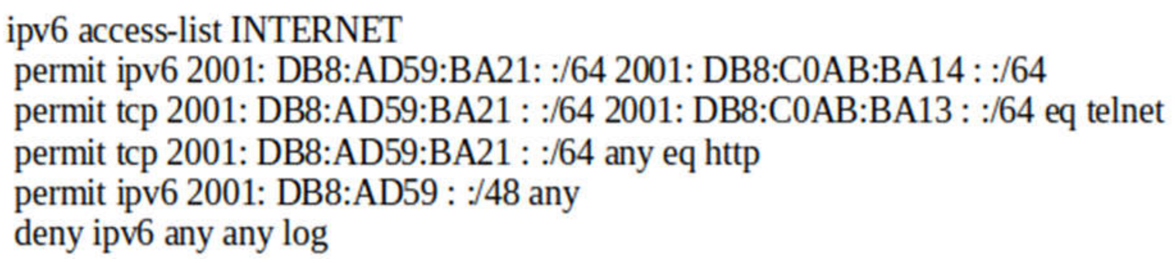
A network engineer is tasked with setting up a GRE tunnel between the HQ and BRANCH offices. All devices need to be accessible between the sites. BRANCH-PC1 is unable to ping HQ-PC1. Which action resolves the issue?

A. Change the destination IP on HQ to 10.20.212.2
B. Change the source tunnel interface on BRANCH to G0/1.
C. Change the source tunnel interface on HQ to G0/0.
D. Change the destination IP on BRANCH to 10.20.212.1

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 68
Refer to the exhibit.



```
ipv6 access-list INTERNET
 permit ipv6 2001: DB8:AD59:BA21: :/64 2001: DB8:C0AB:BA14 : :/64
 permit tcp 2001: DB8:AD59:BA21 : :/64 2001: DB8:C0AB:BA13 : :/64 eq telnet
 permit tcp 2001: DB8:AD59:BA21 : :/64 any eq http
 permit ipv6 2001: DB8:AD59 : :/48 any
 deny ipv6 any any log
```

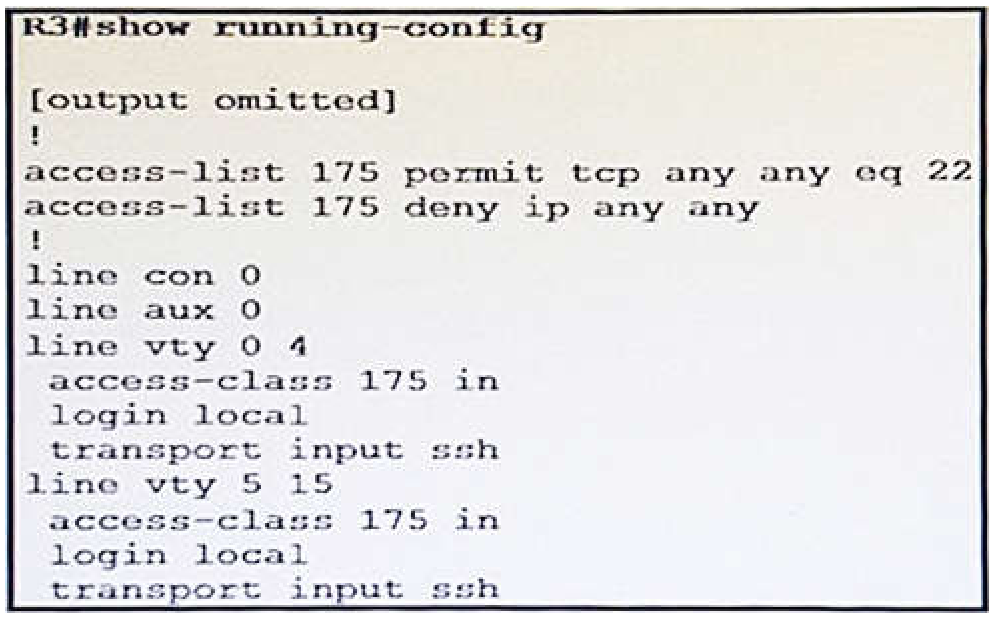
Which statement about the INTERNET ACL is true?

A. The denied entries will be logged because of the explicit deny ipv6 any any log line.
B. A packet with a source address of 2001:DB8:AD59:ACC0:2020:882:DB8:1125 will be denied.
C. HTTPS traffic from the 2001:DB8:AD59:BA21::/64 subnet will automatically be permitted along with HTTP traffic.
D. A packet with a source address of 2001:DB80:AD59:BA21:101:CAB:64:38 destined to port 80 will be permitted.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 69
Refer to the exhibit.



```
R3#show running-config

[output omitted]
!
access-list 175 permit tcp any any eq 22
access-list 175 deny ip any any
!
line con 0
line aux 0
line vty 0 4
 access-class 175 in
 login local
 transport input ssh
line vty 5 15
 access-class 175 in
 login local
 transport input ssh
```

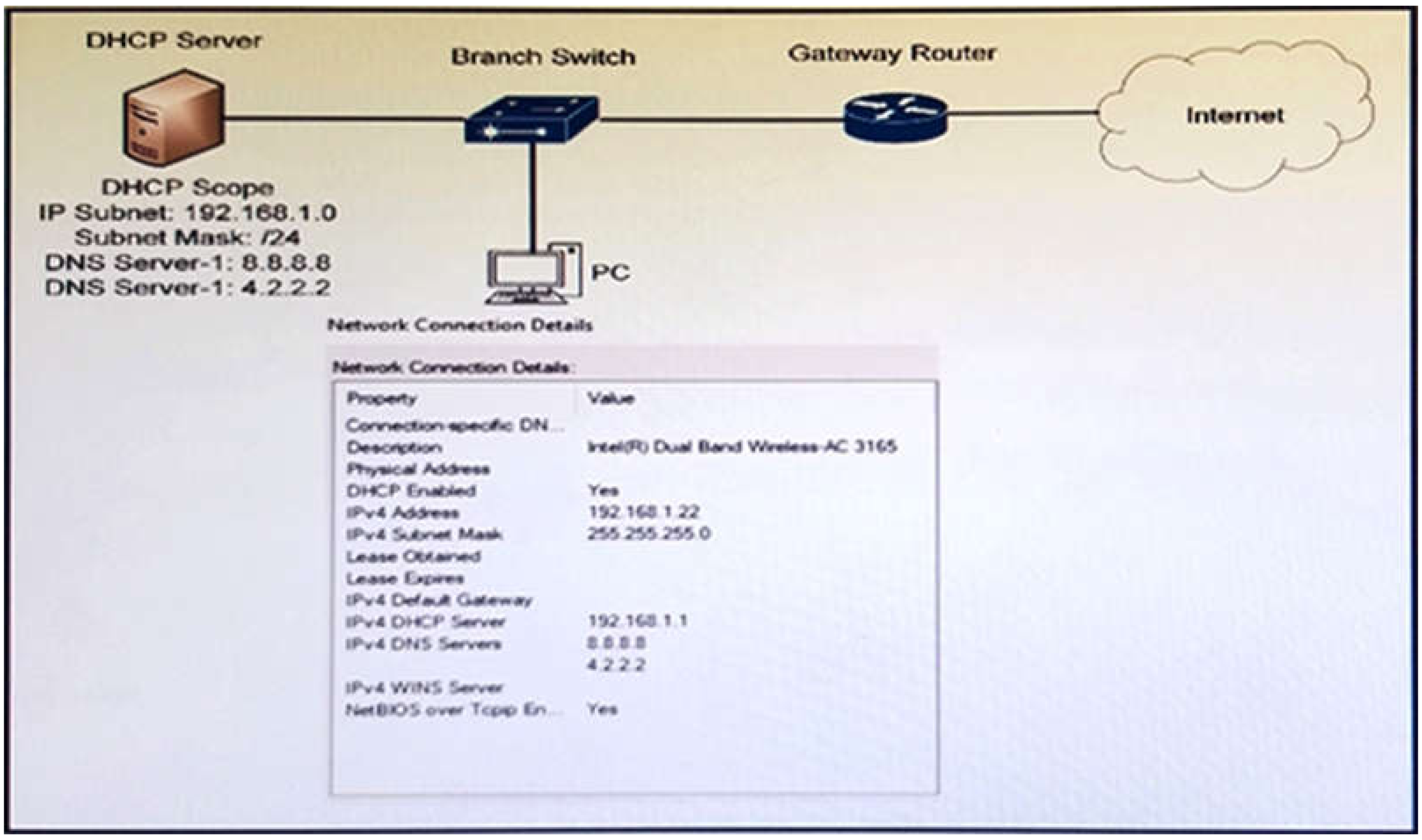
Multiple users are logging into R3 via Telnet and making changes at the same time. Which action will restrict the number of users logging into R3 simultaneously?

A. Apply the session-limit command to the VTY lines.
B. Add the aaa authorization command to the global configuration.
C. Apply the access-class 175 in command on line con 0.
D. Remove all configured usernames other than the admin account.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 70
Refer to the exhibit.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) Dual Band Wireless-AC 3165
Physical Address	
DHCP Enabled	Yes
IPv4 Address	192.168.1.22
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	
Lease Expires	
IPv4 Default Gateway	
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Servers	8.8.8.8 4.2.2.2
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

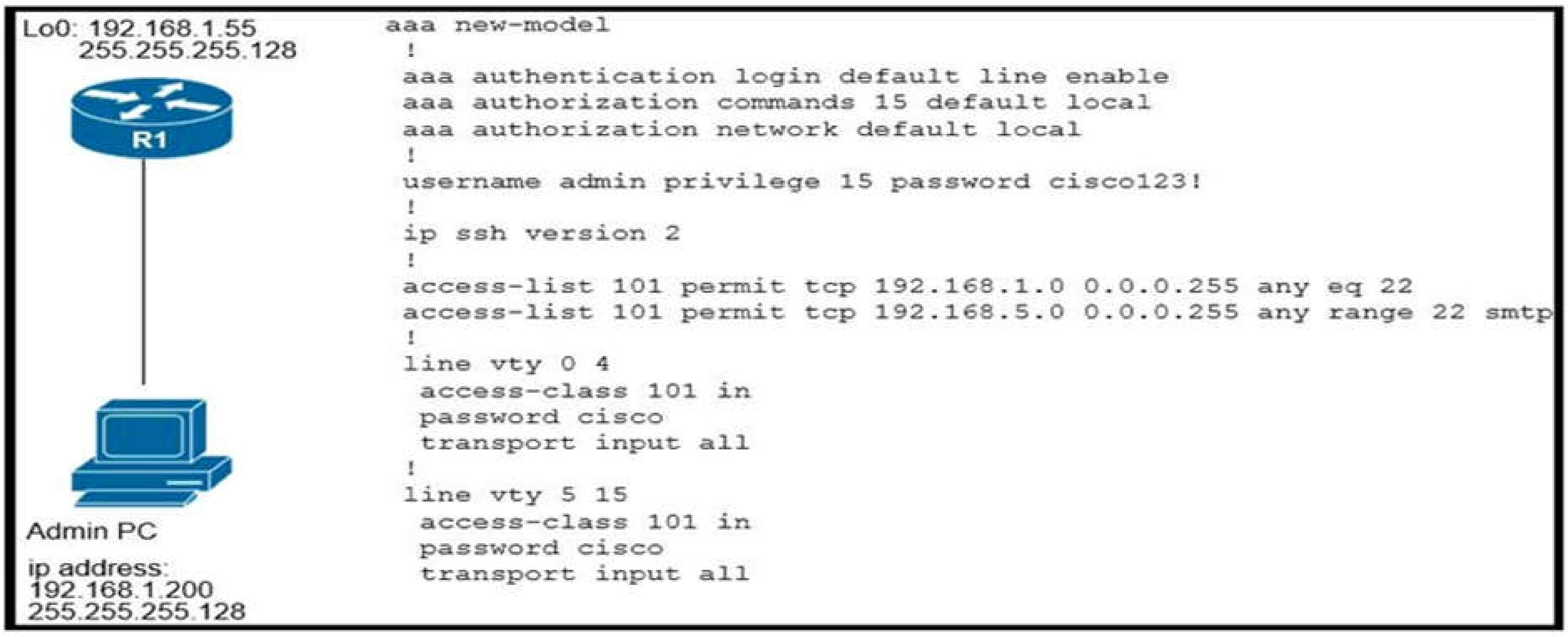
The PC is unable to connect to the Internet. You have determined that the DHCP server has not issued a default gateway to the PC. Which configuration mechanism will resolve this issue?

A. Configure proxy ARP on the gateway router
B. Configure static ARP on the gateway router
C. Configure DHCP snooping on the gateway router
D. Configure reverse ARP on the gateway router

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 71
Refer to the exhibit.



```
aaa new-model
 !
 aaa authentication login default line enable
 aaa authorization commands 15 default local
 aaa authorization network default local
 !
 username admin privilege 15 password cisco123!
 !
 ip ssh version 2
 !
 access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 22
 access-list 101 permit tcp 192.168.5.0 0.0.0.255 any range 22 smtp
 !
 line vty 0 4
  access-class 101 in
  password cisco
  transport input all
 !
 line vty 5 15
  access-class 101 in
  password cisco
  transport input all
```

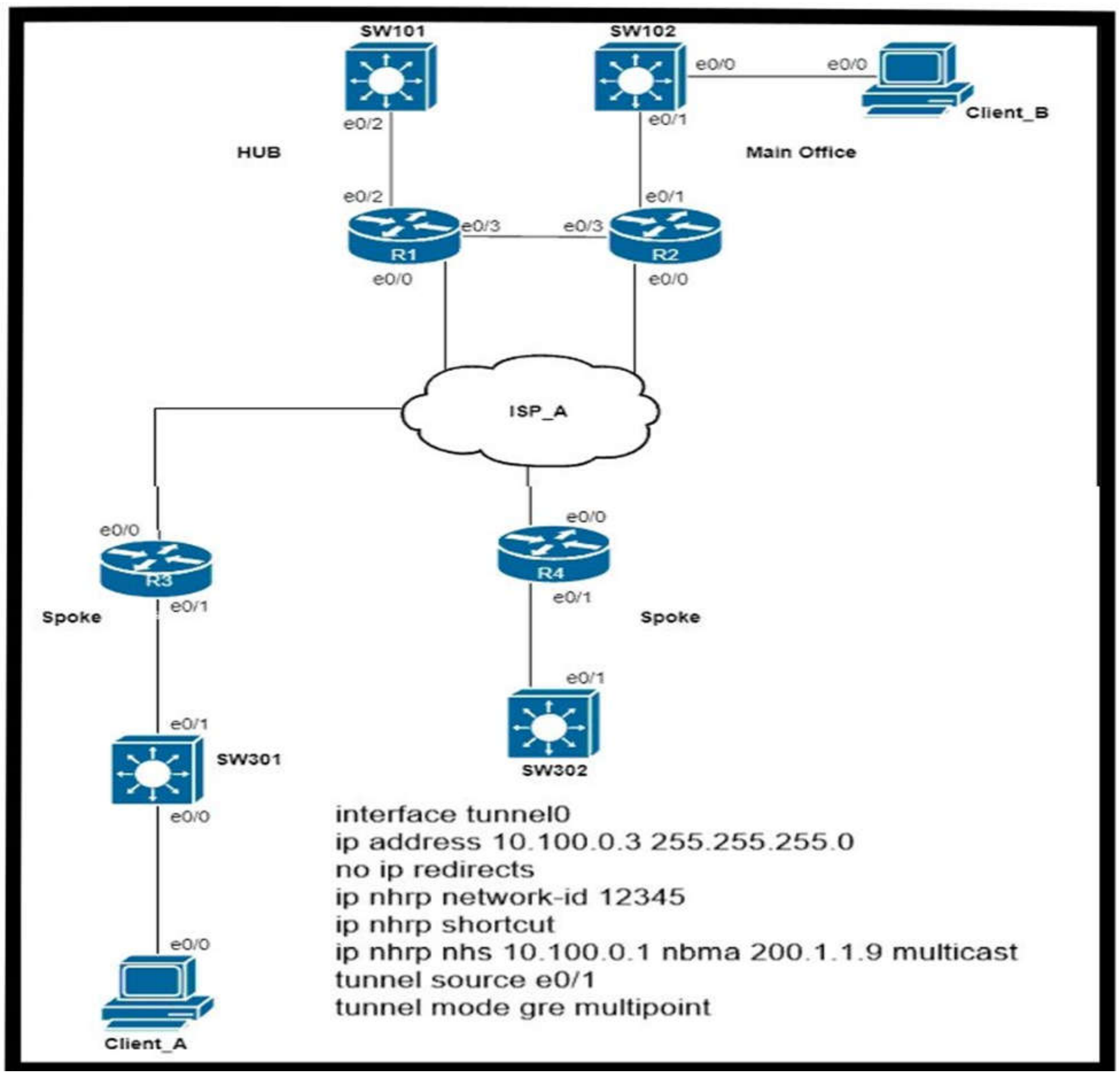
The administrator has successfully logged into R1 but is unable to access privileged mode commands. Which configuration is causing the problem?

A. The aaa authorization reverse-access command is missing.
B. The username command uses password, not secret.
C. Enable secret or enable password must be configured.
D. The password on the VTY does not match the username password.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 72
Refer to the exhibit.



```
interface tunnel0
ip address 10.100.0.3 255.255.255.0
no ip redirects
ip nhrp network-id 12345
ip nhrp shortcut
ip nhrp nhs 10.100.0.1 nbma 200.1.1.9 multicast
tunnel source e0/1
tunnel mode gre multipoint
```

Client A cannot reach client B while other users from other spoke routers can reach Client B. Which command provides the output necessary to troubleshoot the issue?

A. show ip route

B. show ip interface brief

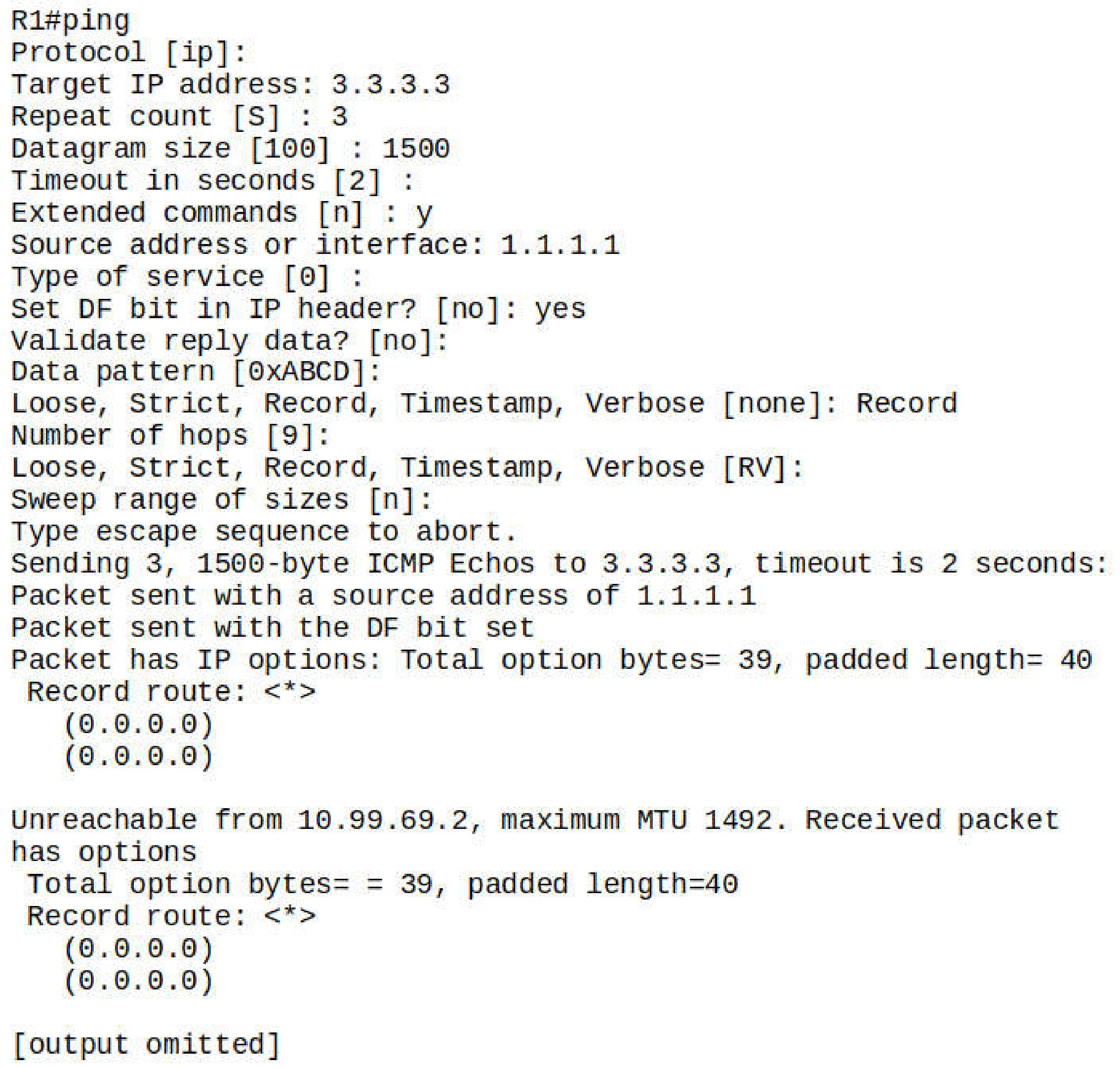
C. show dmvpn

D. show ip bgp sum

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 73
Refer to the exhibit.



```
R1#ping
Protocol [ip]:
Target IP address: 3.3.3.3
Repeat count [S] : 3
Datagram size [100] : 1500
Timeout in seconds [2] :
Extended commands [n] : y
Source address or interface: 1.1.1.1
Type of service [0] :
Set DF bit in IP header? [no]: yes
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose [none]: Record
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose [RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 3, 1500-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
Packet sent with the DF bit set
Packet has IP options: Total option bytes= 39, padded length= 40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)

Unreachable from 10.99.69.2, maximum MTU 1492. Received packet
has options
 Total option bytes= = 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)

[output omitted]
```

R1 can ping the R3 fa0/1 interface. Why do the extended pings fail?

A. The maximum packet size accepted by the command is 1476 bytes.
B. R3 is missing a return route to 10.99.69.0/30.
C. The DF bit has been set.
D. R2 and R3 do not have an OSPF adjacency.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 74
Routes are not being shared dynamically over a functional GRE tunnel. Which scenario is causing the issue?

A. MTU is configured at 1500 on the tunnel interface.
B. An ACL is blocking the data plane traffic between the remote devices.
C. The tunnel mode is mismatched between the two routers.
D. The tunnel interface is not participating in the dynamic routing process.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 75
DRAG DROP

Drag the ping and traceroute extended command from the left onto the corresponding purpose on the right.

Select and Place:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 76
Which two statements about troubleshooting with Unicast reverse Path Forwarding are true? (Choose two.)

A. uRPF allows packets with source 0.0.0.0 and destination 255.255.255.255 to pass.
B. uRPF drops packets with source 0.0.0.0 and destination 255.255.255.255.
C. Cisco Express Forwarding must be enabled for uRPF to work.

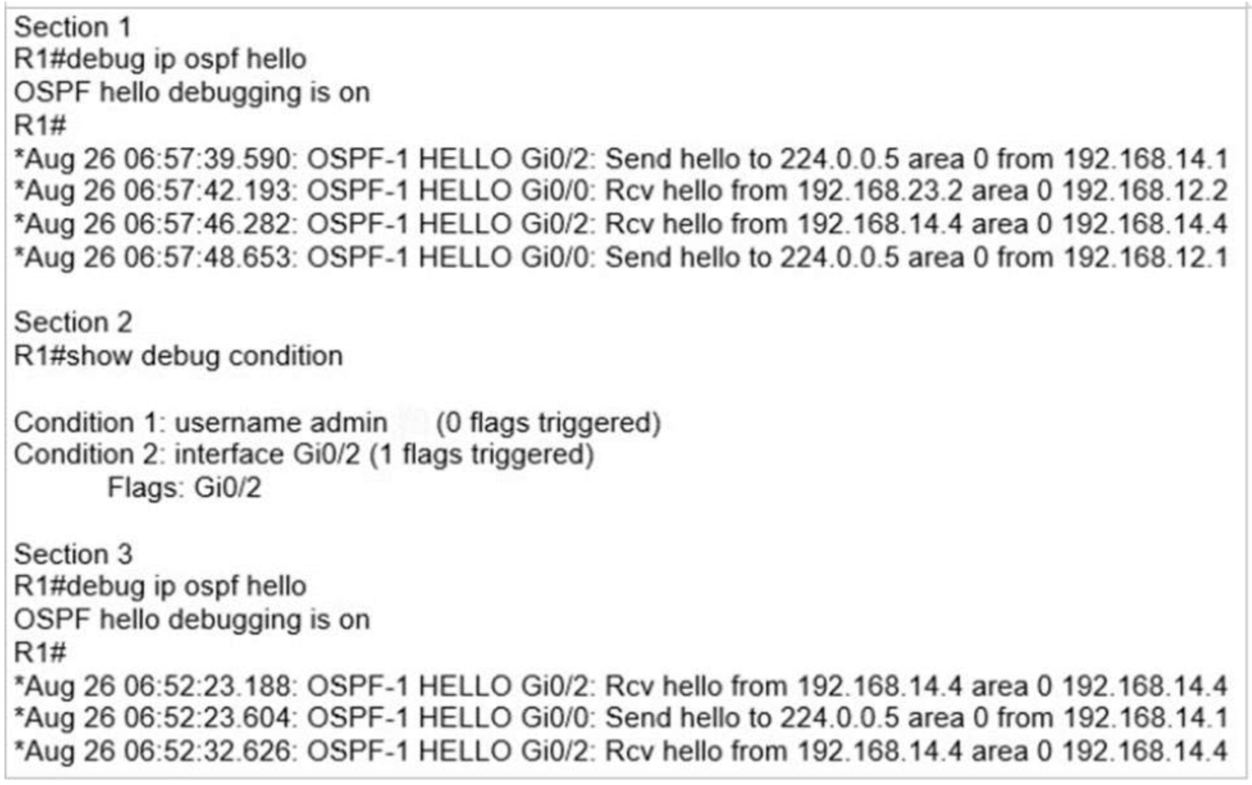
D. Cisco Express Forwarding must be disabled for uRPF to work.

E. uRPF configuration is supported on Layer 2 and Layer 3 Cisco devices.

Correct Answer: AC
Section: [none]
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfrpf.pdf

QUESTION 77
Refer to the exhibit.



```
Section 1
R1#debug ip ospf hello
OSPF hello debugging is on
R1#
*Aug 26 06:57:39.590: OSPF-1 HELLO Gi0/2: Send hello to 224.0.0.5 area 0 from 192.168.14.1
*Aug 26 06:57:42.193: OSPF-1 HELLO Gi0/0: Rcv hello from 192.168.23.2 area 0 192.168.12.2
*Aug 26 06:57:46.282: OSPF-1 HELLO Gi0/2: Rcv hello from 192.168.14.4 area 0 192.168.14.4
*Aug 26 06:57:48.653: OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 192.168.12.1

Section 2
R1#show debug condition

Condition 1: username admin      (0 flags triggered)
Condition 2: interface Gi0/2 (1 flags triggered)
         Flags: Gi0/2

Section 3
R1#debug ip ospf hello
OSPF hello debugging is on
R1#
*Aug 26 06:52:23.188: OSPF-1 HELLO Gi0/2: Rcv hello from 192.168.14.4 area 0 192.168.14.4
*Aug 26 06:52:23.604: OSPF-1 HELLO Gi0/0: Send hello to 224.0.0.5 area 0 from 192.168.14.1
*Aug 26 06:52:32.626: OSPF-1 HELLO Gi0/2: Rcv hello from 192.168.14.4 area 0 192.168.14.4
```

Which output will be displayed for Section 2 when the command no debug condition 1 is entered on the router R1?

A. R1#show debug condition 1
   Condition 2: username admin (0 flags triggered)

B. R1#show debug condition 1
   Condition 1: interface Gi0/2 (1 flags triggered)
   Flags: Gi0/2

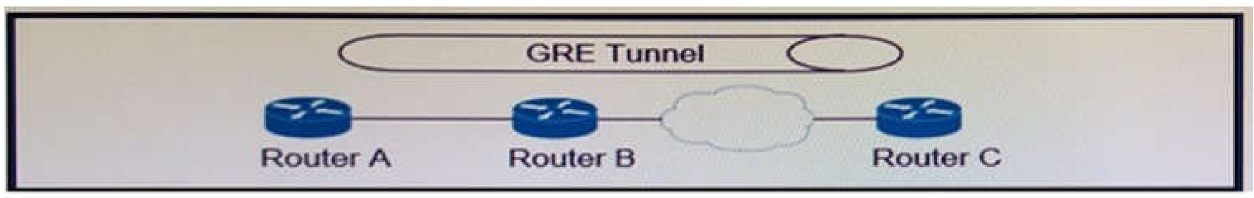
C. R1#show debug condition 1
   Condition 2: interface Gi0/2 (1 flag triggered)
   Flags: Gi0/2

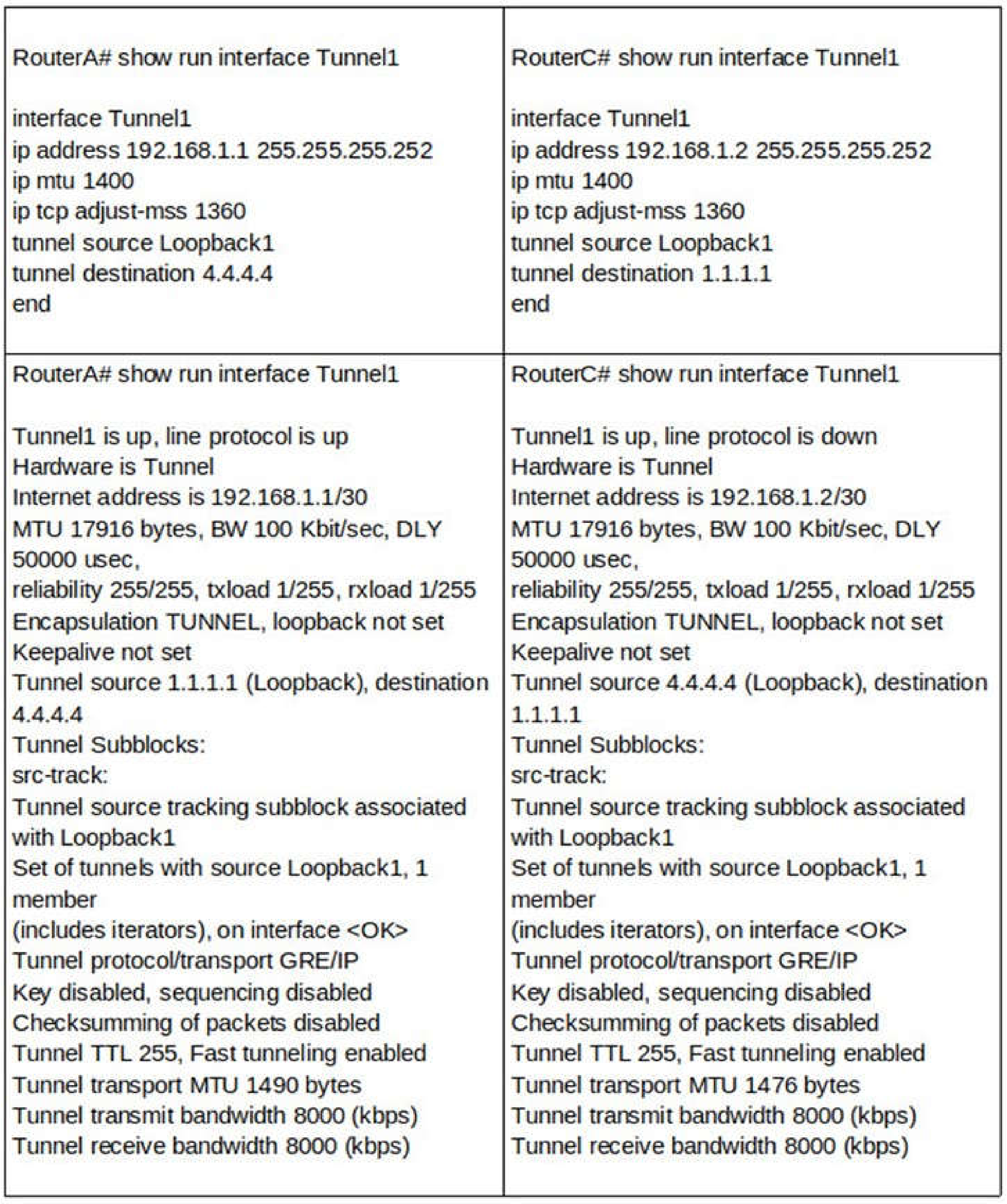
D. R1#show debug condition 1
   Condition 1: username admin (0 flags triggered)
   Condition 2: interface Gi0/2 (1 flag triggered)
   Flags: Gi0/2

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 78
Refer to the exhibit.





```
RouterA# show run interface Tunnel1

interface Tunnel1
ip address 192.168.1.1 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source Loopback1
tunnel destination 4.4.4.4
end
```

```
RouterC# show run interface Tunnel1

interface Tunnel1
ip address 192.168.1.2 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source Loopback1
tunnel destination 1.1.1.1
end
```

```
RouterA# show run interface Tunnel1

Tunnel1 is up, line protocol is up
Hardware is Tunnel
Internet address is 192.168.1.1/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY
50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 1.1.1.1 (Loopback), destination
4.4.4.4
Tunnel Subblocks:
src-track:
Tunnel source tracking subblock associated
with Loopback1
Set of tunnels with source Loopback1, 1
member
(includes iterators), on interface <OK>
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1490 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

```
RouterC# show run interface Tunnel1

Tunnel1 is up, line protocol is down
Hardware is Tunnel
Internet address is 192.168.1.2/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY
50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 4.4.4.4 (Loopback), destination
1.1.1.1
Tunnel Subblocks:
src-track:
Tunnel source tracking subblock associated
with Loopback1
Set of tunnels with source Loopback1, 1
member
(includes iterators), on interface <OK>
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
```

An engineer has set up a GRE tunnel between Router A and Router C. Router A can reach the Router C Loopback 1 interface but the tunneled traffic is not working. What is the cause of this issue?

A. Router A does not have a route to 4.4.4.4
B. Router B has a routing problem.
C. Router C does not have a route to 1.1.1.1
D. Router C has the wrong tunnel MTU

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference: