

300-135: Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

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

Á

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

Á

QUESTION 3

Refer to the exhibit.

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

Gateway of last resort is 212.50.185.126 to network 0.0.0.0

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

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

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

Correct Answer: D

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

Á
.
.

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

Á
.

QUESTION 6

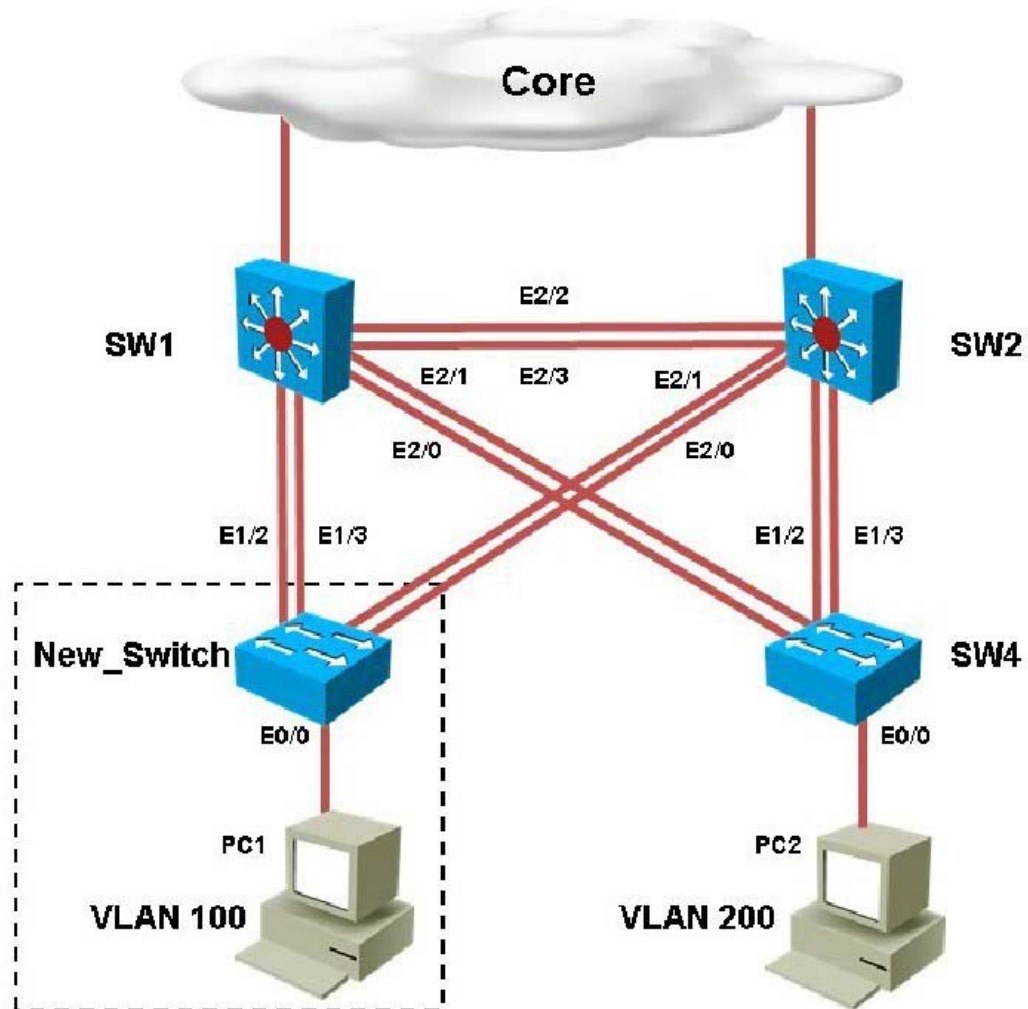
Which statement is true about an IPsec/GRE tunnel?

- 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

QUESTION +

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



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

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

Correct Answer: C

Explanation

Explanation/Reference:

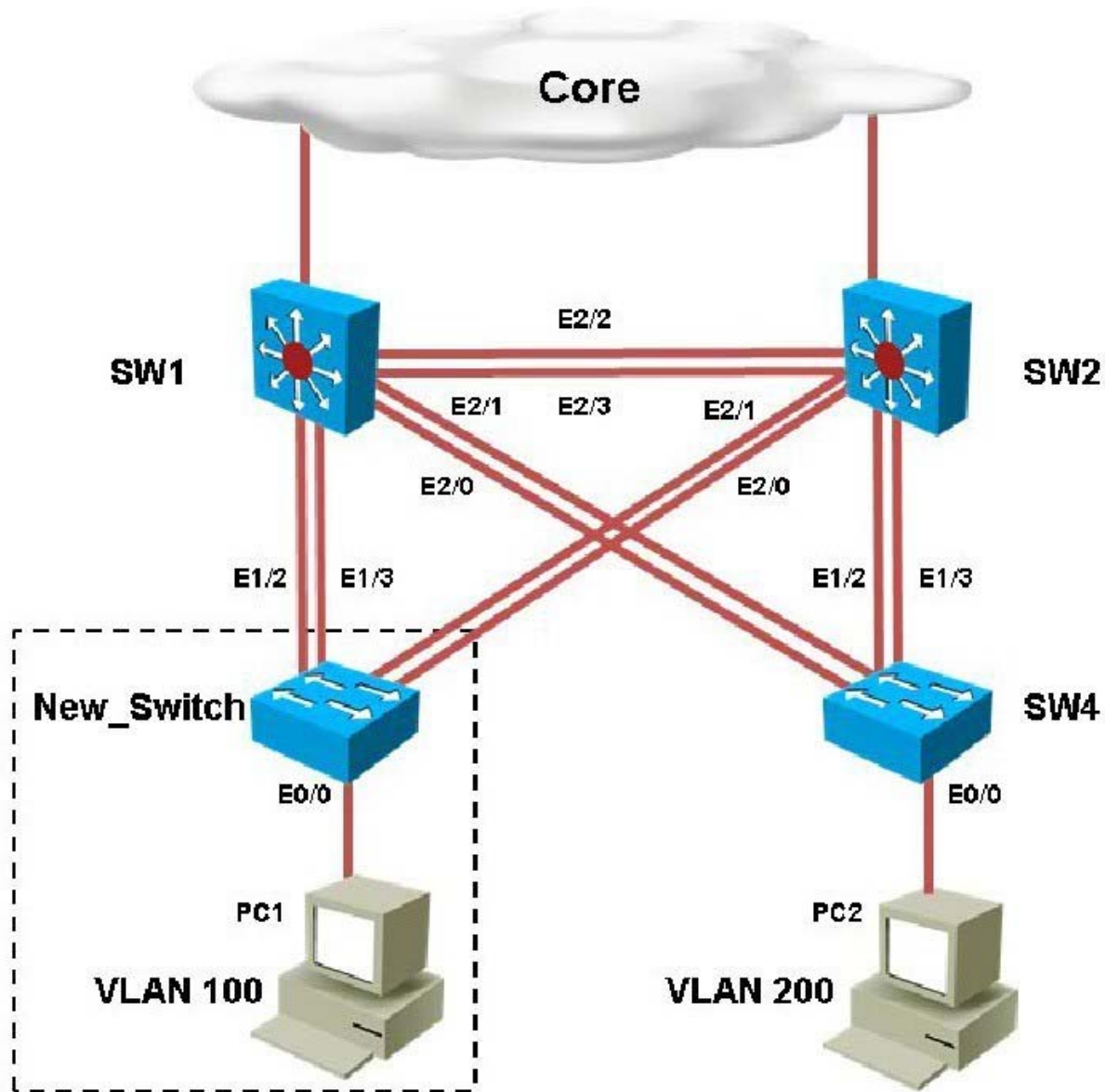
Explanation:

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:

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



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

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

Correct Answer: A

Explanation

Explanation/Reference:

Explanation:

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

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

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