2016 NEW Cisco CCNP Routing and Switching 300-101: Implementing Cisco IP Routing (ROUTE) Exam Questions and Answers RELEASED in Braindump2go.com Online IT Study Website Today!

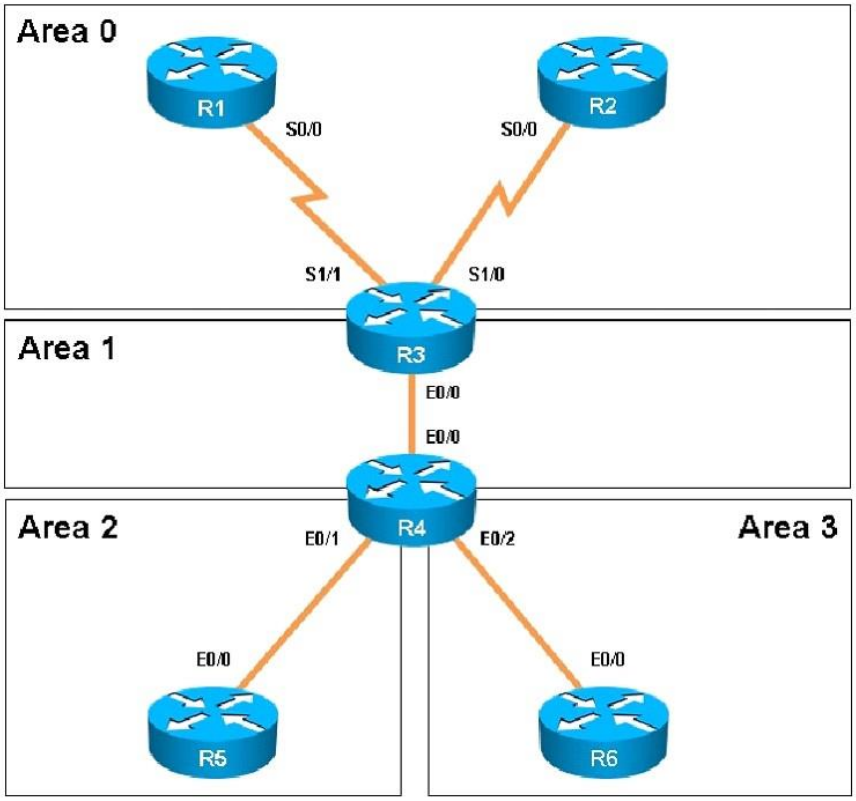
2016 Braindump2go Valid Cisco 300-101 Exam Preparation Materials:

1.| Latest 230Q&As 300-101 PDF Dumps and VCE Dumps:

http://www.braindump2go.com/300-101.html

[Guarantee 100% Exam Pass!]

QUESTION 51
Scenario:
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.



Which of the following statements is true about the serial links that terminate in R3

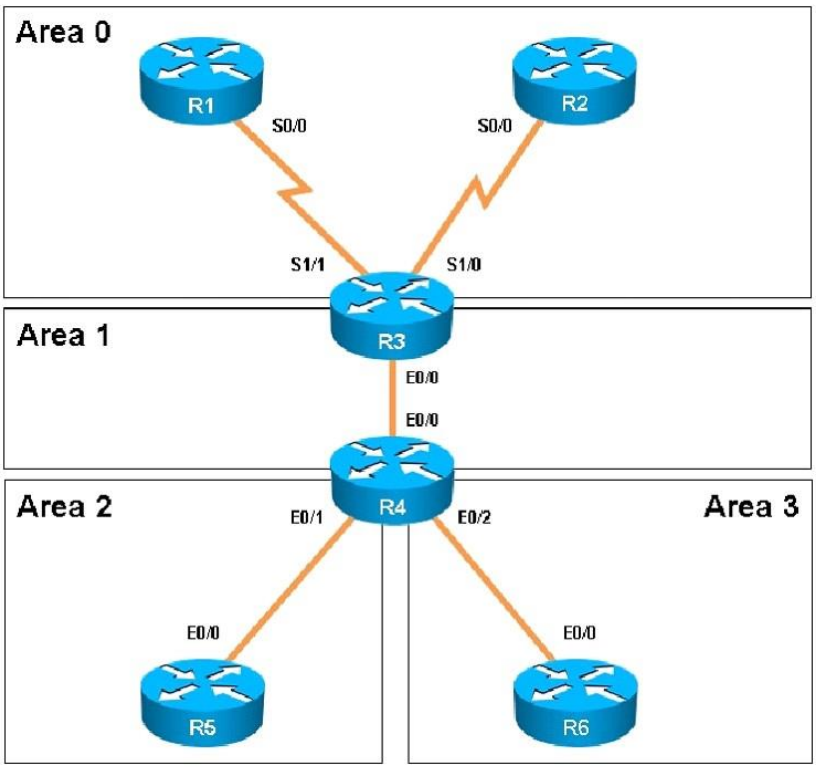
A. The R1-R3 link needs the neighbor command for the adjacency to stay up
B. The R2-R3 link OSPF timer values are 30, 120, 120
C. The R1-R3 link OSPF timer values should be 10,40,40
D. R3 is responsible for flooding LSUs to all the routers on the network.

Answer: B
Explanation:
We can see the configured timers using the following command:

```
R3#show ip ospf interface serial 1/0
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 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) 3.3.3.3, Interface address 192.168.13.3
  Backup Designated router (ID) 1.1.1.1, Interface address 192.168.13.1
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:06
  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 2, maximum is 11
  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  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

R3#
```

QUESTION 52
Scenario:
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.



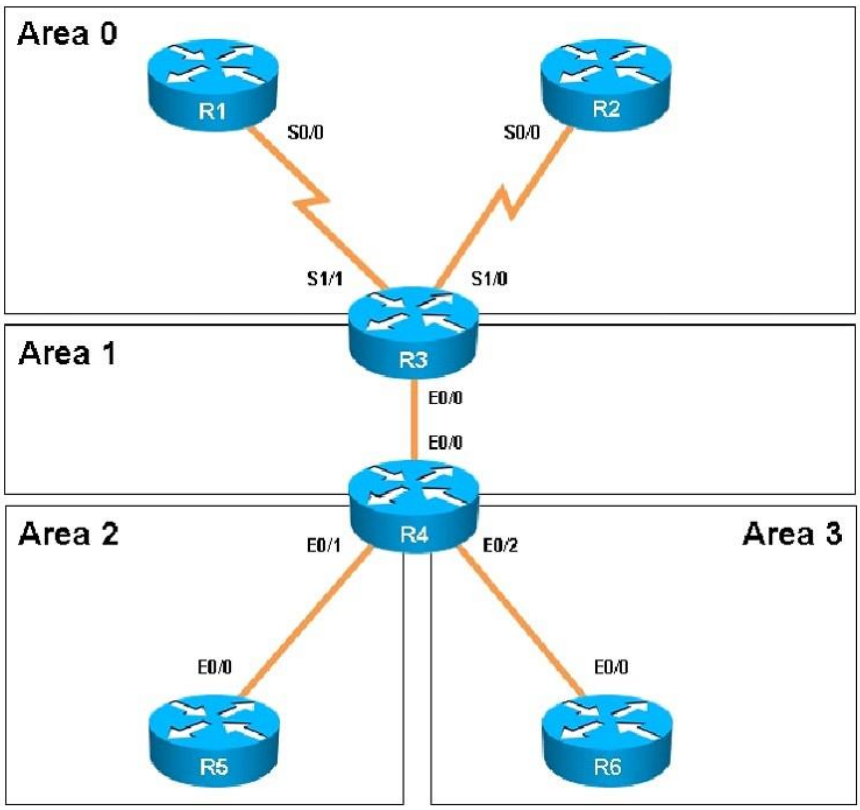
How many times was SPF algorithm executed on R4 for Area 1?

A. 1
B. 5
C. 9
D. 20
E. 54
F. 224

Answer: C
Explanation:
This can be found using the "show ip ospf" command on R4.
Look for the Area 1 stats which shows this:

```
    Flood list length 0
Area 1
    Number of interfaces in this area is 2 (1 loopback)
    This area has transit capability: Virtual Link Endpoint
    Area has no authentication
    SPF algorithm last executed 04:32:05.765 ago
    SPF algorithm executed 9 times
    Area ranges are
    Number of LSA 15. Checksum Sum 0x05538F
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
Area 2
    Number of interfaces in this area is 1
    It is a NSSA area
    Perform type-7/type-5 LSA translation
    Area has no authentication
```

QUESTION 53
Scenario:
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.



Areas of Router 5 and 6 are not normal areas, inspect their routing tables and determine which statement is true?

A. R5's Loopback and R6's Loopback are both present in R5's Routing table
B. R5's Loopback and R6's Loopback are both present in R6's Routing table
C. Only R5's loopback is present in R5's Routing table
D. Only R6's loopback is present in R5's Routing table
E. Only R5's loopback is present in R6's Routing table

Answer: A
Explanation:
Here are the routing tables of R5 and R6:

R5

```
      1.0.0.0/32 is subnetted, 1 subnets
O IA     1.1.1.1 [110/2544] via 192.168.45.4, 00:46:34, Ethernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O IA     2.2.2.2 [110/2544] via 192.168.45.4, 04:57:48, Ethernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O IA     3.3.3.3 [110/601] via 192.168.45.4, 04:57:48, Ethernet0/0
      4.0.0.0/32 is subnetted, 1 subnets
O IA     4.4.4.4 [110/301] via 192.168.45.4, 04:57:48, Ethernet0/0
      5.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        5.5.1.0/24 is directly connected, Loopback1
L        5.5.1.1/32 is directly connected, Loopback1
C        5.5.2.0/24 is directly connected, Loopback2
L        5.5.2.1/32 is directly connected, Loopback2
C        5.5.3.0/24 is directly connected, Loopback3
L        5.5.3.1/32 is directly connected, Loopback3
C        5.5.4.0/24 is directly connected, Loopback4
L        5.5.4.1/32 is directly connected, Loopback4
C        5.5.5.5/32 is directly connected, Loopback0
      6.0.0.0/32 is subnetted, 2 subnets
O IA     6.6.6.6 [110/1600] via 192.168.45.4, 04:56:43, Ethernet0/0
O IA     6.6.66.6 [110/601] via 192.168.45.4, 04:56:43, Ethernet0/0
O IA  192.168.13.0/24 [110/2543] via 192.168.45.4, 00:46:44, Ethernet0/0
O IA  192.168.23.0/24 [110/2543] via 192.168.45.4, 04:57:48, Ethernet0/0
O IA  192.168.34.0/24 [110/600] via 192.168.45.4, 04:57:48, Ethernet0/0

      192.168.45.0/24 is variably subnetted, 2 subnets, 2 masks
```

R6

```
R6#show ip route
R6#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 192.168.46.4 to network 0.0.0.0

O*IA  0.0.0.0/0 [110/301] via 192.168.46.4, 05:09:56, Ethernet0/0
      6.0.0.0/32 is subnetted, 2 subnets
C        6.6.6.6 is directly connected, Loopback0
C        6.6.66.6 is directly connected, Loopback1
      192.168.46.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.46.0/24 is directly connected, Ethernet0/0
L        192.168.46.6/32 is directly connected, Ethernet0/0

R6#
```

QUESTION 54

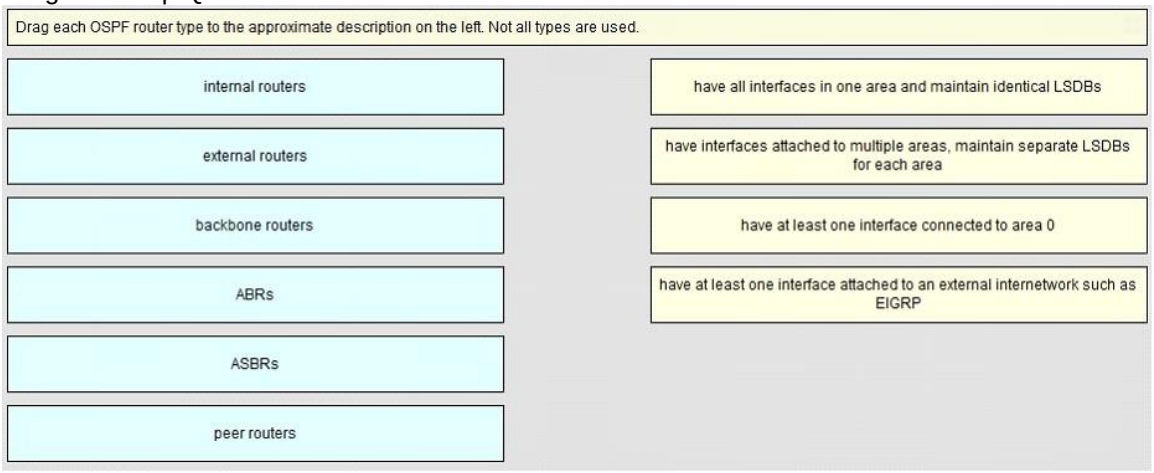
Drag and Drop Question

Drag each OSPF state to the correct definition.

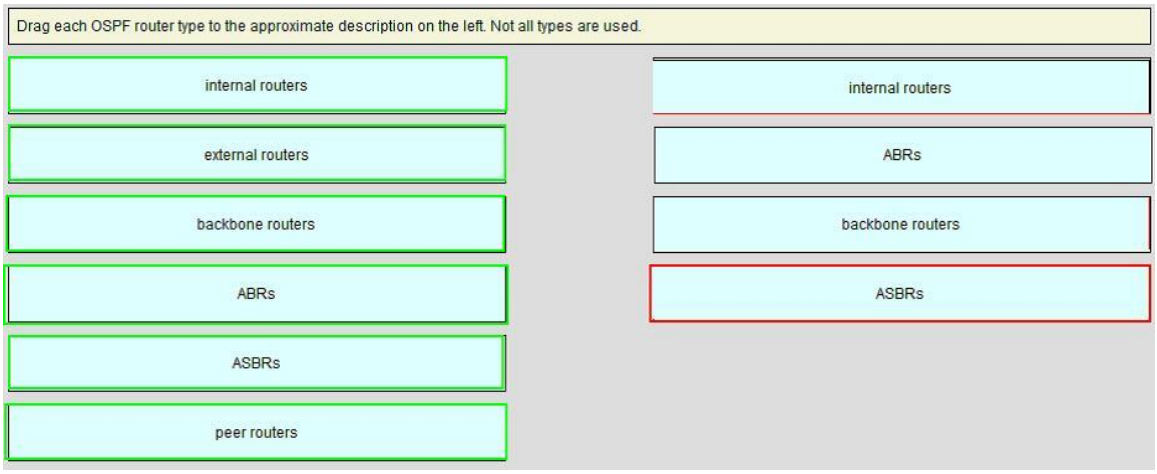
init	No information has been received, but Hello packets can still be sent to the neighbor.
loading	A Hello packet is received, but the ID of the receiving router was not included in the Hello packet.
exstart	Each router see its own Router ID in the neighbor field of the Hello packet; there is a DR / BDR election.
full	The routers and their DR and BDR establish a master-slave relationship.
2-Way	Routers exchange DBD packets that describe the contents of the entire link-state database.
down	Based on the information provided by the DBDs, routers send link-state request packets.
exchange	All the router and network LSAs are exchanged and the router databases are synchronized.

Answer:

QUESTION 55
Drag and Drop Question



Answer:



QUESTION 56
Refer to the exhibit. Based on this FIB table, which statement is correct?

```
R2#show ip cef

      Prefix              Next Hop          Interface
0.0.0.0/0             192.168.201.1     FastEthernet0/0
0.0.0.0/32            receive
192.168.201.0/27      attached          FastEthernet0/0
192.168.201.0/32      receive
192.168.201.1/32      192.168.201.1     FastEthernet0/0
192.168.201.2/32      receive
192.168.201.31/32     receive
224.0.0.0/4           drop
224.0.0.0/24          receive
255.255.255.255/32    receive
```

A. There is no default gateway.
B. The IP address of the router on FastEthernet is 209.168.201.1.
C. The gateway of last resort is 192.168.201.1.
D. The router will listen for all multicast traffic.

Answer: C
Explanation:
The 0.0.0.0/0 route is the default route and is listed as the first CEF entry. Here we see the next hop for this default route lists 192.168.201.1 as the default router (gateway of last resort).

QUESTION 57
Refer to the exhibit. A network administrator checks this adjacency table on a router.
What is a possible cause for the incomplete marking?

```
Router#show adjacency

 Protocol   Interface              Address
IP          Serial0     192.168.209.130(2) (incomplete)
IP          Serial0     192.168.209.131(7)
IP          Ethernet0   192.168.201.1(7)
```

A. incomplete ARP information
B. incorrect ACL
C. dynamic routing protocol failure
D. serial link congestion

Answer: A
Explanation:
To display information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table, use the show adjacency command.
Reasons for Incomplete Adjacencies
There are two known reasons for an incomplete adjacency:
The router cannot use ARP successfully for the next-hop interface.
After a clear ip arp or a clear adjacency command, the router marks the adjacency as incomplete. Then it fails to clear the entry.
In an MPLS environment, IP CEF should be enabeled for Label Switching. Interface level command ip route-cache cef
No ARP Entry
When CEF cannot locate a valid adjacency for a destination prefix, it punts the packets to the CPU for ARP resolution and, in turn, for completion of the adjacency.
http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/17812-cef-incomp.html#t4

QUESTION 58
A network engineer notices that transmission rates of senders of TCP traffic sharply increase and decrease simultaneously during periods of congestion. Which condition causes this?

A. global synchronization
B. tail drop
C. random early detection
D. queue management algorithm

Answer: A
Explanation:
TCP global synchronization in computer networks can happen to TCP/IP flows during periods of congestion because each sender will reduce their transmission rate at the same time when packet loss occurs.
Routers on the Internet normally have packet queues, to allow them to hold packets when the network is busy, rather than discarding them.
Because routers have limited resources, the size of these queues is also limited. The simplest technique to limit queue size is known as tail drop. The queue is allowed to fill to its maximum size, and then any new packets are simply discarded, until there is space in the queue again. This causes problems when used on TCP/IP routers handling multiple TCP streams, especially when bursty traffic is present. While the network is stable, the queue is constantly full, and there are no problems except that the full queue results in high latency. However, the introduction of a sudden burst of traffic may cause large numbers of established, steady streams to lose packets simultaneously.
http://en.wikipedia.org/wiki/TCP_global_synchronization

QUESTION 59
Which three problems result from application mixing of UDP and TCP streams within a network with no QoS? (Choose three.)

A. starvation
B. jitter
C. latency
D. windowing
E. lower throughput

Answer: ACE
Explanation:
It is a general best practice not to mix TCP-based traffic with UDP-based traffic (especially streaming video) within a single service provider class due to the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters will throttle-back flows when drops have been detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely oblivious to drops and thus never lower transmission rates due to dropping. When TCP flows are combined with UDP flows in a single service provider class and the class experiences congestion, then TCP flows will continually lower their rates, potentially giving up their bandwidth to drop-oblivious UDP flows. This effect is called TCP-starvation/UDP-dominance. This can increase latency and lower the overall throughput.
TCP-starvation/UDP-dominance likely occurs if (TCP-based) mission-critical data is assigned to the same service provider class as (UDP-based) streaming video and the class experiences sustained congestion. Even if WRED is enabled on the service provider class, the same behavior would be observed, as WRED (for the most part) only affects TCP-based flows.
Granted, it is not always possible to separate TCP-based flows from UDP-based flows, but it is beneficial to be aware of this behavior when making such application-mixing decisions.
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/spqsd_wp.htm

QUESTION 60
Which method allows IPv4 and IPv6 to work together without requiring both to be used for a single connection during the migration process?

A. dual-stack method
B. 6to4 tunneling
C. GRE tunneling
D. NAT-PT

Answer: A
Explanation:
Dual stack means that devices are able to run IPv4 and IPv6 in parallel. It allows hosts to simultaneously reach IPv4 and IPv6 content, so it offers a very flexible coexistence strategy. For sessions that support IPv6, IPv6 is used on a dual stack endpoint. If both endpoints support Ipv4 only, then IPv4 is used.
Benefits:
Native dual stack does not require any tunneling mechanisms on internal networks ?Both IPv4 and IPv6 run independent of each other

Dual stack supports gradual migration of endpoints, networks, and applications.
http://www.cisco.com/web/strategy/docs/gov/IPV6at_a_glance_c45-625859.pdf