Vendor: Cisco

Exam Code: 300-101

Exam Name: Implementing Cisco IP Routing (ROUTE v2.0)

QUESTION 1
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.

Correct 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 2
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

Correct 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:
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.
Reference:
http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/17812-cef- incomp.html#t4

QUESTION 3
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

Correct 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.
Reference:
http://en.wikipedia.org/wiki/TCP_global_synchronization

QUESTION 4
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

Correct 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.
Reference:
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/spqsd_wp.htm

QUESTION 5
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

Correct 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.
Reference:
http://www.cisco.com/web/strategy/docs/gov/IPV6at_a_glance_c45-625859.pdf

QUESTION 6
Which statement about the use of tunneling to migrate to IPv6 is true?

A. Tunneling is less secure than dual stack or translation.
B. Tunneling is more difficult to configure than dual stack or translation.
C. Tunneling does not enable users of the new protocol to communicate with users of the old protocol without dual-stack hosts.
D. Tunneling destinations are manually determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses.

Correct Answer: C
Explanation:
Using the tunneling option, organizations build an overlay network that tunnels one protocol over the other by encapsulating IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets. The advantage of this approach is that the new protocol can work without disturbing the old protocol, thus providing connectivity between users of the new protocol. Tunneling has two disadvantages, as discussed in RFC 6144:
Users of the new architecture cannot use the services of the underlying infrastructure.
Tunneling does not enable users of the new protocol to communicate with users of the old protocol without dual-stack hosts, which negates interoperability.
Reference:
http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

QUESTION 7
A network administrator executes the command clear ip route. Which two tables does this command clear and rebuild? (Choose two.)

A. IP routing