DUMPSARENA

CCNP Implementing Cisco IP Routing (ROUTE v2.0)

Cisco 300-101

Version Demo

Total Demo Questions: 20

Total Premium Questions: 855

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Principles	13
Topic 2, Layer 2 Technologies	8
Topic 3, Layer 3 Technologies	34
Topic 4, VPN Technologies	8
Topic 5, Infrastructure Security	9
Topic 6, Infrastructure Services	24
Topic 7, Mix Questions	759
Total	855

QUESTION NO: 1

Which two statements are true about using IPv4 and IPv6 simultaneously on a network segment? (Choose two.)

A. Hosts can be configured to receive both IPv4 and IPv6 addresses via DHCP.

B. Host configuration options for IPv4 can be either statically assigned or assigned via DHCP.Host configuration options for IPv6 can be statically assigned only.

C. IPv6 allows a host to create its own IPv6 address that will allow it to communicate to other devices on a network configured via DHCP. IPv4 does not provide a similar capability for hosts.

D. IPv4 and IPv6 addresses can be simultaneously assigned to a host but not to a router interface.

E. IPv6 provides for more host IP addresses but IPv4 provides for more network addresses.

ANSWER: A C

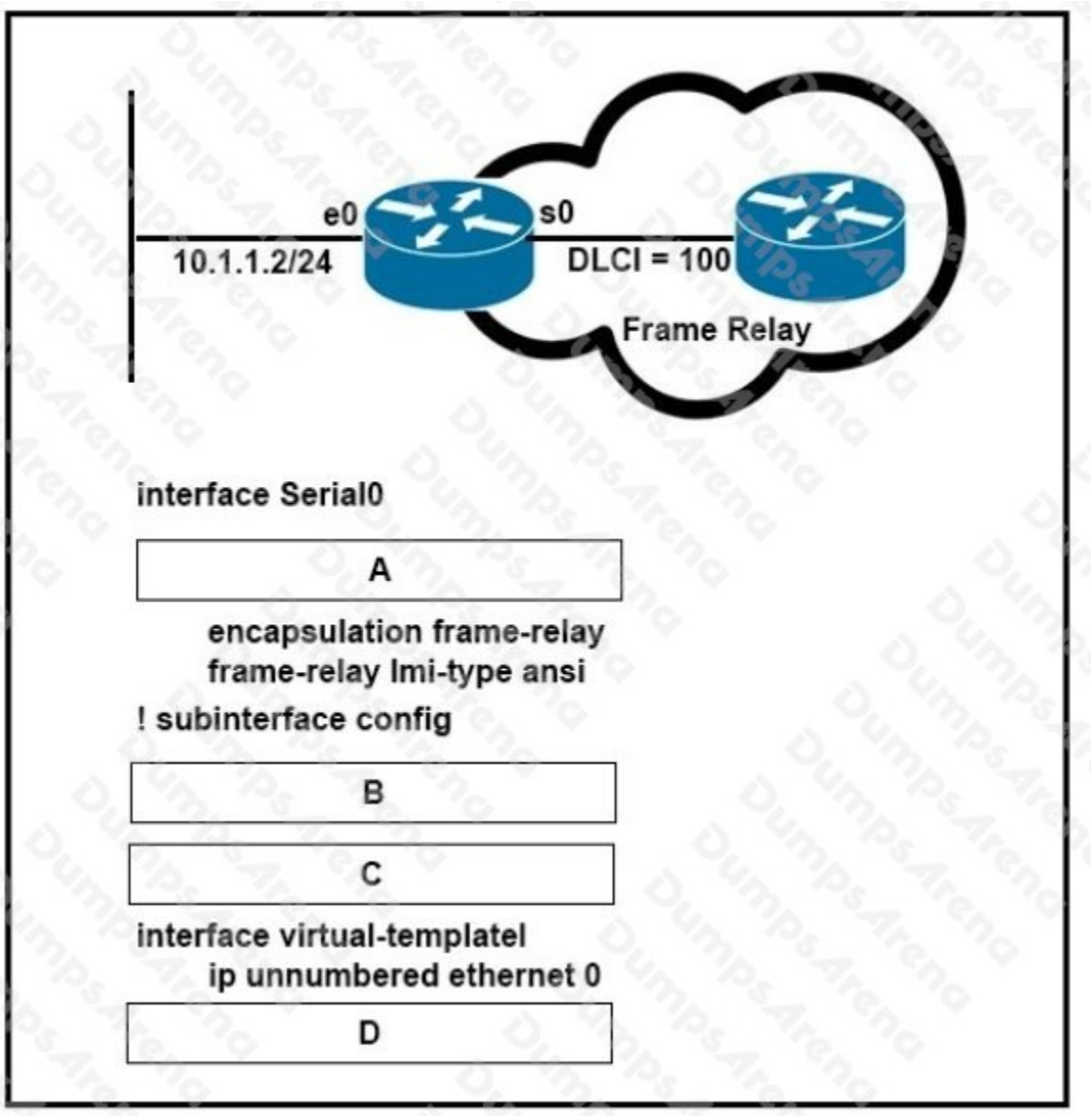
Explanation:

Like DHCP in IPv4, IPv6 hosts can also be configured to acquire connectivity parameters from DHCPv6 servers. IPv4 clients use DHCP broadcasts to locate DHCP servers, and since broadcasts are extinct in IPv6, clients use specialized multicasts to locate DHCPv6 servers. These multicasts use the reserved address FF02::1:2. One notable difference between DHCP and DHCPv6 is that while DHCP can inform clients which node to use as the default gateway, DHCPv6 does not do this.

QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

Refer to the exhibit.



You are configuring the R1 Serial0 interface for a point-to-point connection. drag and drop the required configuration statements from the left onto the correct locations from the diagram on the right. Not all commands are used.

Select and Place:

ANSWER:

QUESTION NO: 3

Which three protocols are supported with EVN? (Choose three.)

A. IS-IS

B. EIGRP

C. RIP

D. OSPFv2

E. BFD

F. BGP

ANSWER: B D F

Explanation:

Restrictions for EVN

An EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.

There are additional platform and line-card restrictions for an EVN trunk. Check Cisco Feature Navigator, www.cisco.com/go/cfn for supported platforms and line cards.

A single IP infrastructure can be virtualized to provide up to 32 virtual networks end-to-end.

If an EVN trunk is configured on an interface, you cannot configure VRF-Lite on the same interface.

OSPFv3 is not supported; OSPFv2 is supported.

The following are not supported by EVN:

--IS-IS

--RIP

--Route replication is not supported with BGP

--Certain SNMP set operations

The following are not supported on an EVN trunk:

--Access control lists (ACLs)

--BGP interface commands are not inherited

--IPv6, except on vnet global

--Network address translation (NAT)

--NetFlow

--Web Cache Communication Protocol (WCCP)

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.html

QUESTION NO: 4

Which two EIGRP packet types are transmitted unreliably? (Choose two.)

A. queries

B. updates

C. replies

D. requests

E. hellos

ANSWER: D E

QUESTION NO: 5

Which two statements are true about 6to4 tunnels? (Choose two.)

A. In a 6to4 tunnel, the first two bytes of the IPv6 address will be 2002 and the next four bytes will be the hexadecimal equivalent of the IPv4 address.

B. In a 6to4 tunnel, the first two bytes of the IPv6 address will be locally derived and the next two bytes will be the hexadecimal equivalent of the IPv4 address.

C. In a 6to4 tunnel, the IPv4 address 192.168.99.1 would be converted to the 2002:c0a8:6301::/48 IPv6 address.

D. In a 6to4 tunnel, the IPv4 address 192.168.99.1 would be converted to the 2002:c0a8:6301::/16 IPv6 address.

E. In a 6to4 tunnel, the IPv4 address 192.168.99.1 would be converted to the 2002:1315:4463:1::/64 IPv6 address.

ANSWER: A C

Explanation:

In a 6to4 tunnel, the first two bytes of the IPv6 address will be 0x2002 and the next four bytes will be the hexadecimal equivalent of the IPv4 address. The IPv4 address 192.168.99.1 would be converted to the 2002:c0a8:6301::/48 IPv6 address.

QUESTION NO: 6

A router receives a routing advertisement for the same prefix and subnet from four different routing protocols. Which advertisement is installed in the routing table?

A. RIP

B. OSPF

C. iBGP

D. EIGRP

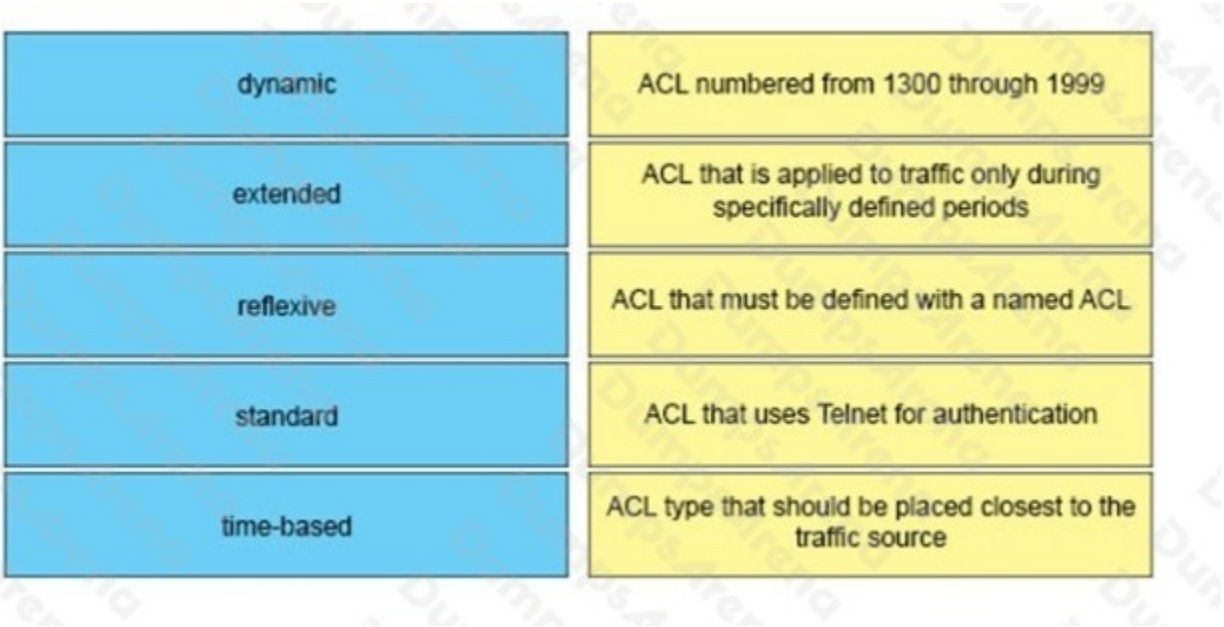
ANSWER: D

QUESTION NO: 7 - (DRAG DROP)

DRAG DROP

Drag and drop the ACL types from the left onto the correct descriptions on the right.

Select and Place:



ANSWER:

QUESTION NO: 8

Which feature is not supported when fast-switched PBR is in use?

A. the set ip default next-hop command

B. the set ip next-hop interface command

C. matching IP addresses to a named ACL

D. matching IP addresses to a prefix list

ANSWER: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xe-3se/3850/iri-xe-3se-3850-book/iri-fast-switched-policy-rtg.pdf

QUESTION NO: 9

In which two areas does OSPF send a summary route by default? (Choose two.)

A. NSSA

B. totally stubby

C. normal

D. backbone

E. stub

ANSWER: B E

QUESTION NO: 10

What does stateful NAT64 do that stateless NAT64 does not do?

A. Stateful NAT64 maintains bindings or session state while performing translation

B. Stateful NAT64 maintains bindings of IPv4 to IPv6 link-local addresses

C. Stateful NAT64 translates IPv4 to IPv6

D. Stateful NAT64 translates IPv6 to IPv4

ANSWER: A

Explanation:

Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

QUESTION NO: 11

Which Netflow version supports MPLS?

A. None

B. All of them

C. Version 8 and 9

D. Version 9

ANSWER: D

Explanation:

MPLS-aware NetFlow uses the NetFlow Version 9 export format. If you are exporting MPLS data to a NetFlow collector or a data analyzer, the collector must support NetFlow Version 9 flow export format, and you must configure NetFlow export in Version 9 format on the router.

QUESTION NO: 12

Which Cisco IOS VPN technology leverages Ipsec, mGRE, dynamic routing protocol, NHRP, and Cisco Express Forwarding?

A. FlexVPN

B. DMVPN

C. GETVPN

D. Cisco Easy VPN

ANSWER: B

Explanation:

Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers and Unix-like Operating Systems based on the standard protocols, GRE, NHRP and Ipsec. This DMVPN provides the capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible tunnel end-point peers, including Ipsec (Internet Protocol Security) and ISAKMP (Internet Security Association and Key Management Protocol) peers. DMVPN is initially configured to build out a hub-and-spoke network by statically configuring the hubs (VPN headends) on the spokes, no change in the configuration on the hub is required to accept new spokes. Using this initial hub-and-spoke network, tunnels between spokes can be dynamically built on demand (dynamic-

mesh) without additional configuration on the hubs or spokes. This dynamic-mesh capability alleviates the need for any load on the hub to route data between the spoke networks. DMVPN is combination of the following technologies:

- Multipoint GRE (mGRE)
- Next-Hop Resolution Protocol (NHRP)
- Dynamic Routing Protocol (EIGRP, RIP, OSPF, BGP)
- Dynamic Ipsec encryption
- Cisco Express Forwarding (CEF)

Reference: http://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network

QUESTION NO: 13

Which protocols support DMVPN?

A. EIGRP

B. RIP2

C. OSPF

D. BGP

E. ISIS

ANSWER: A C D

Explanation:

Some documents say RIPv2 also supports DMVPN but, EIGPR, OSPF and BGP are the better choices, so we should choose them.

Several routing protocols can be used in a DMVPN design, including:

Enhanced Interior Gateway Protocol (EIGRP)

Open Shortest Path First (OSPF)

Routing Information Protocol version 2 (RIPv2)

Border Gateway Protocol (BGP) On-Demand Routing (ODR)

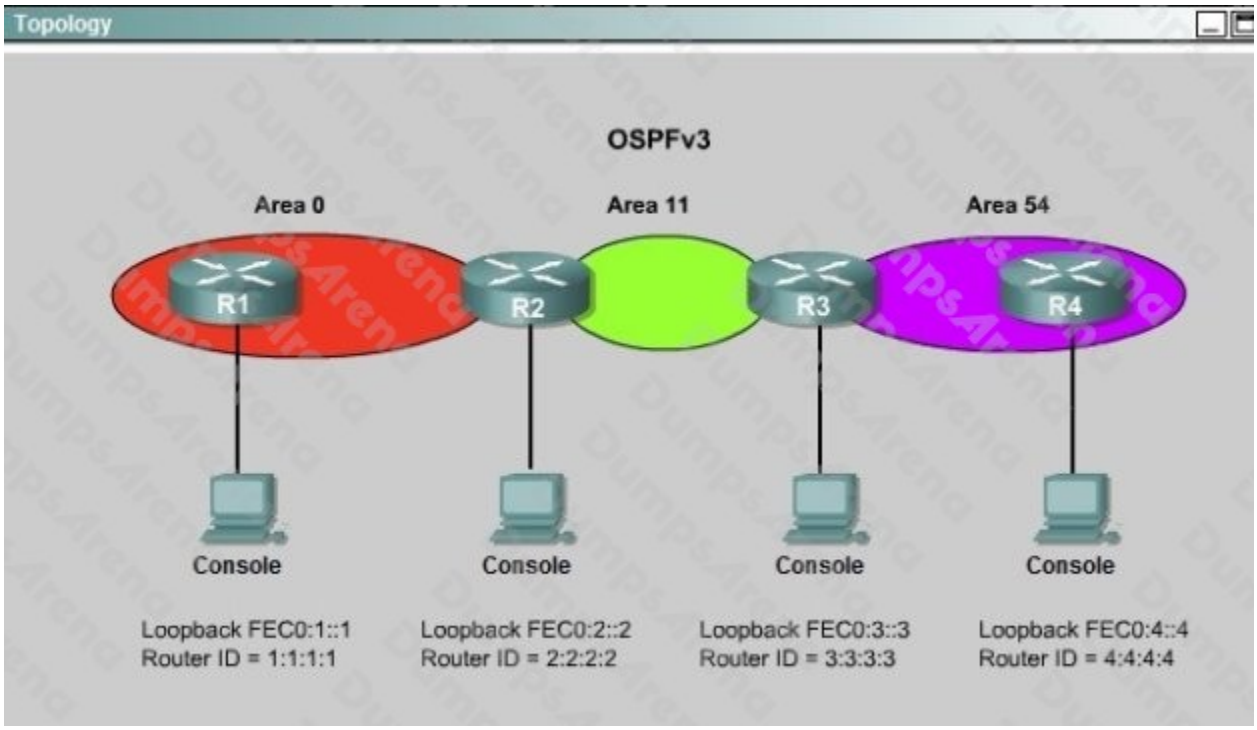
https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf#wp37674 https://www.networkcomputing.com/networking/cisco-dmvpn-choosing-right-routing-protocol/1432661326

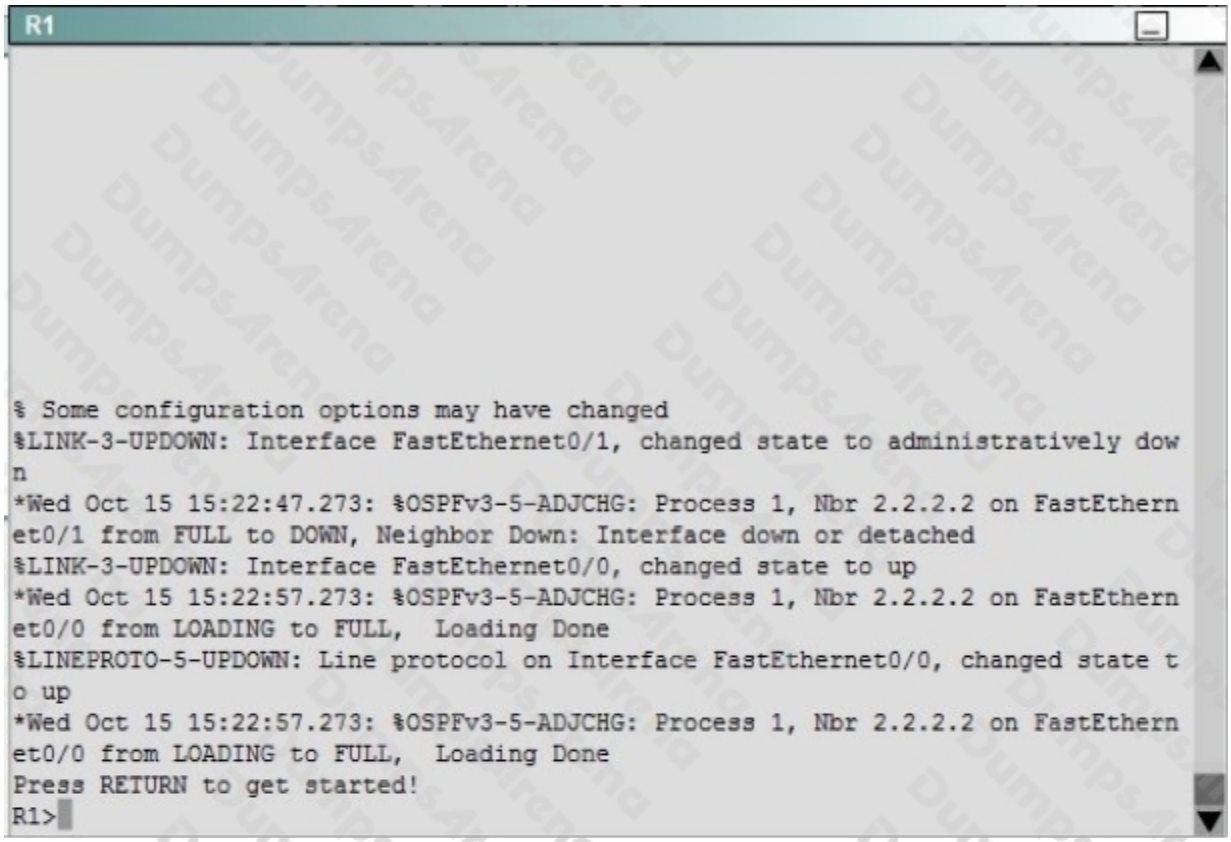
QUESTION NO: 14 - (SIMULATION)

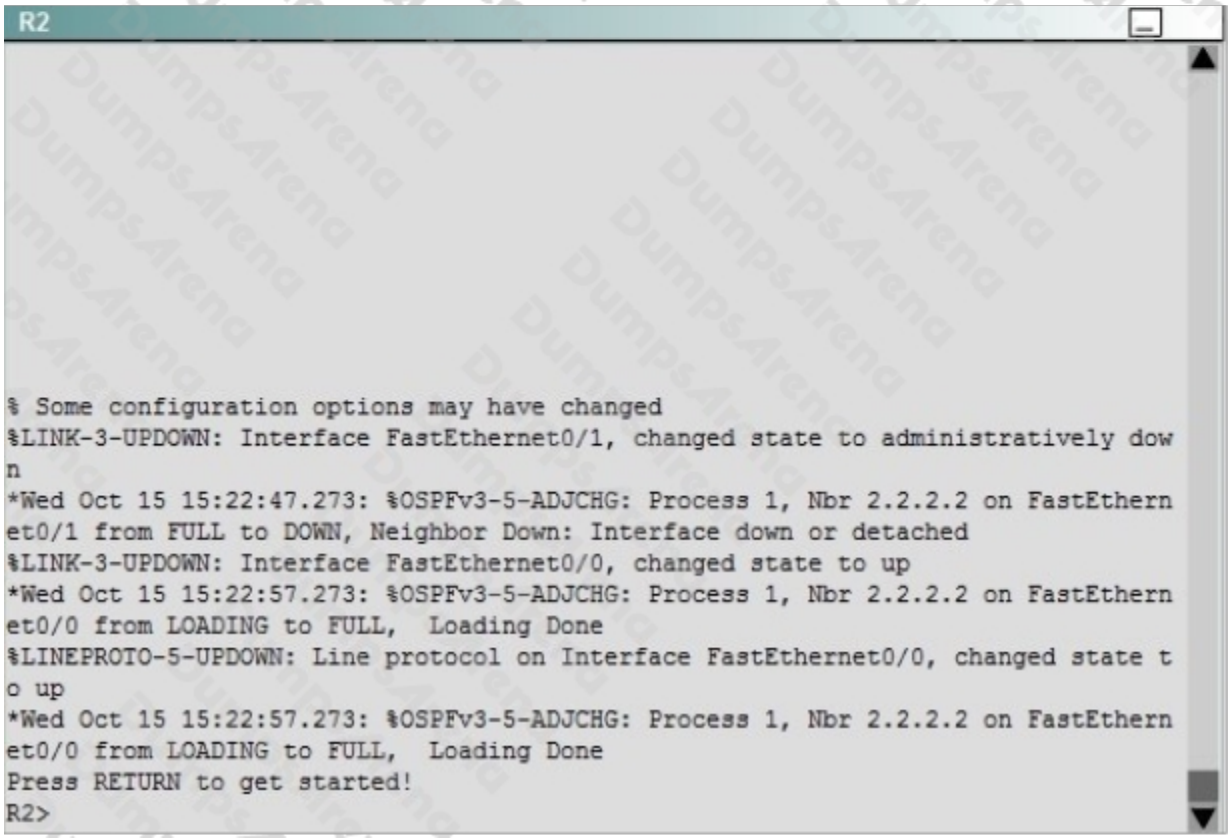
SIMULATION

ROUTE.com is a small IT corporation that has an existing enterprise network that is running IPv6 0SPFv3. Currently OSPF is configured on all routers. However, R4's loopback address (FEC0:4:4) cannot be seen in R1's IPv6 routing table. You are tasked with identifying the cause of this fault and implementing the needed corrective actions that use OSPF features and do not change the current area assignments. You will know that you have corrected the fault when R4's loopback address (FEC0:4:4) can be seen in R1's IPv6 routing table.

Special Note: To gain the maximum number of points you must remove all incorrect or unneeded configuration statements related to this issue.



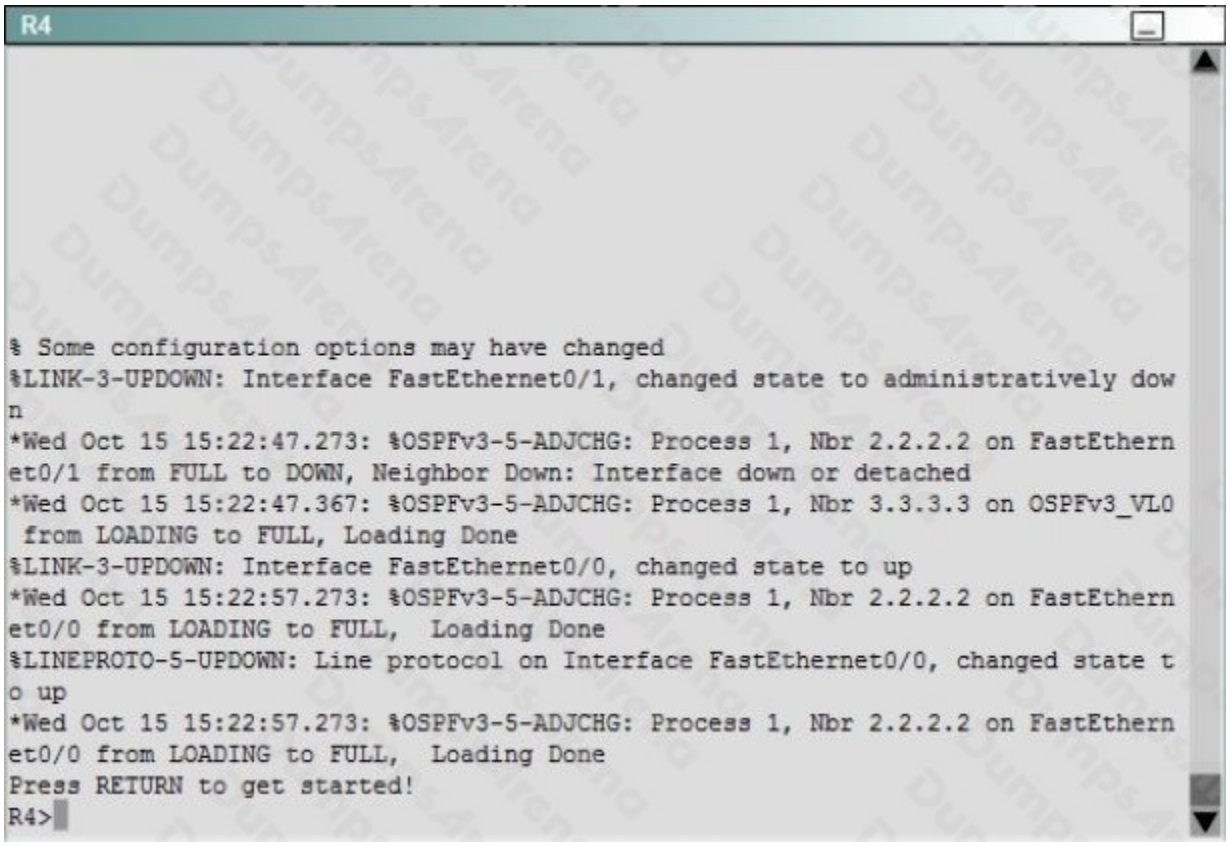

R1
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL, Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL, Loading Done
Press RETURN to get started!
R1>


R2
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL, Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL, Loading Done
Press RETURN to get started!
R2>

```
et0/0 from LOADING to FULL,  Loading Done
Press RETURN to get started!
R2>
```

R3

```
% Some configuration options may have changed
*Wed Oct 15 15:22:47.367: %OSPFv3-5-ADJCHG: Process 1, Nbr 4.4.4.4 on OSPFv3_VL0
 from LOADING to FULL, Loading Done
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
Press RETURN to get started!
R3>
```



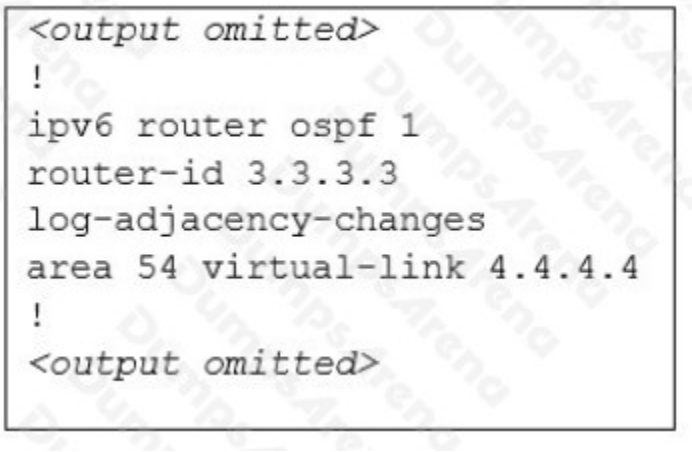
ANSWER: See explanation below

Explanation:

To troubleshoot the problem, first issue the show running-config on all of 4 routers. Pay more attention to the outputs of routers R2 and R3 The output of the “show running-config” command of R2:

```
<output omitted>
!
ipv6 router ospf 1
router-id 2.2.2.2
log-adjacency-
changes
!
<output omitted>
```

The output of the “show running-config” command of R3:



We knew that all areas in an Open Shortest Path First (OSPF) autonomous system must be physically connected to the backbone area (Area 0). In some cases, where this is not possible, we can use a virtual link to connect to the backbone through a non-backbone area. The area through which you configure the virtual link is known as a transit area. In this case, the area 11 will become the transit area. Therefore, routers R2 and R3 must be configured with the area virtual-link command. + Configure virtual link on R2 (from the first output above, we learned that the OSPF process ID of R2 is 1):

R2>enable

R2#configure terminal

R2(config)#ipv6 router ospf 1

R2(config-rtr)#area 11 virtual-link 3.3.3.3 Save the configuration:

R2(config-rtr)#end

R2#copy running-config startup-config

(Notice that we have to use neighbor router-id 3.3.3.3, not R2's router-id 2.2.2.2) + Configure virtual link on R3 (from the second output above, we learned that the OSPF process ID of R3 is 1 and we have to disable the wrong configuration of "area 54 virtual-link 4.4.4.4"): R3>enable

R3#configure terminal

R3(config)#ipv6 router ospf 1

R3(config-rtr)#no area 54 virtual-link 4.4.4.4 R3(config-rtr)#area 11 virtual-link 2.2.2.2 Save the configuration:

R3(config-rtr)#end

R3#copy running-config startup-config

You should check the configuration of R4, too. Make sure to remove the incorrect configuration statements to get the full points. R4(config)#ipv6 router ospf 1

R4(config-router)#no area 54 virtual-link 3.3.3.3

R4(config-router)#end

After finishing the configuration doesn't forget to ping between R1 and R4 to make sure they work.

Note. If you want to check the routing information, use the show ipv6 route command, not "show ip route".

QUESTION NO: 15

When a packet is denied by an IPv6 traffic filter, which additional action does the device perform?

A. It scans the rest of the ACL for a permit entry matching the destination.

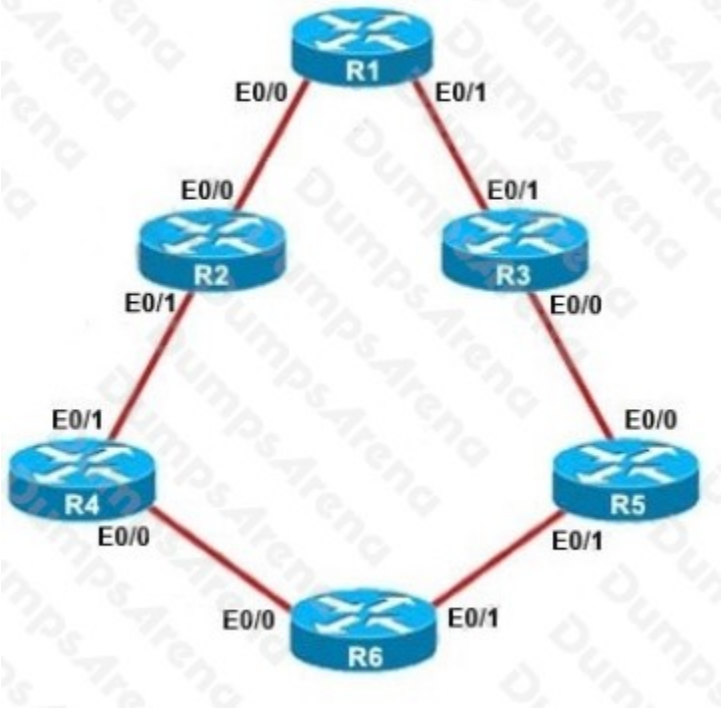
B. It generates an ICMP unreachable message for the frame.

C. It generates a TCP Fin bit and sends it to the source.

D. A creates a null route for the destination and adds it to the route table.

ANSWER: B

QUESTION NO: 16



The configuration of R1 to R6 are posted below for your reference, useless lines are omitted:

R1
```
interface Loopback0
ip address 150.1.1.1 255.255.255.255
!
interface Ethernet0/0
description Link to R2
ip address 192.168.12.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
!
interface Ethernet0/1
description Link to R3
ip address 192.168.13.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
delay 5773
!
router eigrp 1
network 192.168.12.0
network 192.168.13.0
net 150.1.1.1 0.0.0.0
variance 11
```

R2
```
interface Ethernet0/0
description Link to R1
ip address 192.168.12.2 255.255.255.0
!
interface Ethernet0/1
description Link to R4
ip address 192.168.24.2 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.12.0
network 192.168.24.0
!
key chain CISCO
key 1
key-string firstkey
key chain FIRSTKEY
key 1
key-string CISCO
key chain R3
key 1
key-string R3
key 2
key-string R1
```

R3
```
interface Ethernet0/0
description Link to R5
ip address 192.168.35.3 255.255.255.0
!
interface Ethernet0/1
description Link to R1
ip address 192.168.13.3 255.255.255.0
!
router eigrp 1
network 192.168.13.0
network 192.168.35.0
```

R4
```
interface Loopback0
ip address 150.1.4.4 255.255.255.255
!
interface Ethernet0/0
description Link to R6
ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/1
description Link to R2
ip address 192.168.24.4 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.46.0
network 192.168.24.0
network 150.1.4.4 0.0.0.0
!
key chain CISCO
key 1
key-string firstkey
```

R5
```
interface Ethernet0/0
description Link to R3
ip address 192.168.35.5 255.255.255.0
!
interface Ethernet0/1
description Link to R6
ip address 192.168.56.5 255.255.255.0
!
router eigrp 1
network 192.168.35.0
network 192.168.56.0
```

R6
```
interface Loopback0
ip address 150.1.6.6 255.255.255.255
!
interface Loopback1
ip address 172.16.6.6 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.46.6 255.255.255.0
!
interface Ethernet0/1
ip address 192.168.56.6 255.255.255.0
!
router eigrp 1
distribute-list 1 out
network 150.1.6.6 0.0.0.0
network 172.16.6.6 0.0.0.0
network 192.168.46.0
network 192.168.56.0
!
access-list 1 permit 192.168.46.0
access-list 1 permit 192.168.56.0
access-list 1 permit 150.1.6.6
access-list 1 deny 172.16.6.6
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
```

What type of route filtering is occurring on R6?

A. Distribute-list using an ACL

B. Distribute-list using a prefix-list

C. Distribute-list using a route-map

D. An ACL using a distance of 255

ANSWER: A

Explanation:

Use the “show running-config” on R6 we will see a distribute-list applying under EIGRP:

```
R6#show running-config
<ouput omitted>
router eigrp 1
 distribute-list 1 out
 network 150.1.6.6 0.0.0.0
 network 172.16.6.6 0.0.0.0
 network 192.168.46.0
 network 192.168.56.0
!
access-list 1 permit 192.168.46.0
access-list 1 permit 192.168.56.0
access-list 1 permit 150.1.6.6
access-list 1 deny 172.16.6.6
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
<ouput omitted>
```

With this distribute-list, only networks 192.168.46.0; 192.168.56.0 and 150.1.6.6 are advertised out by R6.

QUESTION NO: 17

What happens when an IPv6 enabled router running 6to4 must send a packet to a remote destination and the next hop is the address of 2002::/16?

A. The IPv6 packet has its header removed and replaced with an IPv4 header

B. The IPv6 packet is encapsulated in an IPv4 packet using an IPv4 protocol type of 41

C. The IPv6 packet is dropped because that destination is unable to route IPv6 packets

D. The packet is tagged with an IPv6 header and the IPv6 prefix is included

ANSWER: B

Explanation:

6to4 and Teredo are dynamic tunneling techniques used by desktop operating systems to help their users gain access to the IPv6 Internet. These techniques tunnel the IPv6 packets within IPv4 packets.

The 6to4 method places the IPv6 packets within IPv4 protocol 41 packets.

The Teredo method places the IPv6 packets within IPv4 packets with a UDP 3544 header.

QUESTION NO: 18

Which two statements are true of the OSPF link-state routing protocol? (Choose two.)

A. Using the Bellman-Ford algorithm, each OSPF router independently calculates its best paths to all destinations in the network.
OSPF send hello packets every 10 seconds, not the updates, OSPF sends triggered updates when a network change occurs. For OSPF, D Rother use the multicast address 224.0.0.6 to send packets to DR and BDR, only DR and BDR can get the information from this multicast address.

B. Using the DUAL algorithm, each OSPF router independently calculates its best paths to all destinations in the network.

C. OSPF sends summaries of individual link-state entries every 30 minutes to ensure LSDB synchronization.

D. OSPF sends triggered updates when a network change occurs.

E. OSPF sends updates every 10 seconds.

F. When a link changes state, the router that detected the change creates a link-state advertisement (LSA) and propagates it to all OSPF devices using the 224.0.0.6 multicast address.

ANSWER: C D

Explanation:

The point of this question is the basis of OSPF.

Incorrect answer

A. OSPF send hello packets every 10 seconds, not the updates, OSPF sends triggered updates when a network change occurs. For OSPF, D Rother use the multicast address 224.0.0.6 to send packets to DR and BDR, only DR and BDR can get the information from this multicast address.

QUESTION NO: 19

Which three route filtering statements are true? (Choose three)

A. After the router rip and passive-interface s0/0 commands have been issued, the s0/0 interface will not send any RIP updates, but will receive routing updates on that interface.

B. After the router eigrp 10 and passive-interface s0/0 commands have been issued, the s0/0 interface will not send any EIGRP updates, but will receive routing updates on that interface

C. After the router ospf 10 and passive-interface s0/0 commands have been issued , the s0/0 interface will not send any OSPF updates, but will receive routing updates on that interface

D. When you use the passive-interface command with RIPv2, multicasts are sent out the specified interface

E. When you use the passive-interface command with EIGRP, hello messages are not sent out the specified interface

F. When you use the passive-interface command with OSPF, hello messages are not sent out the specified interface

ANSWER: A E F

Explanation:

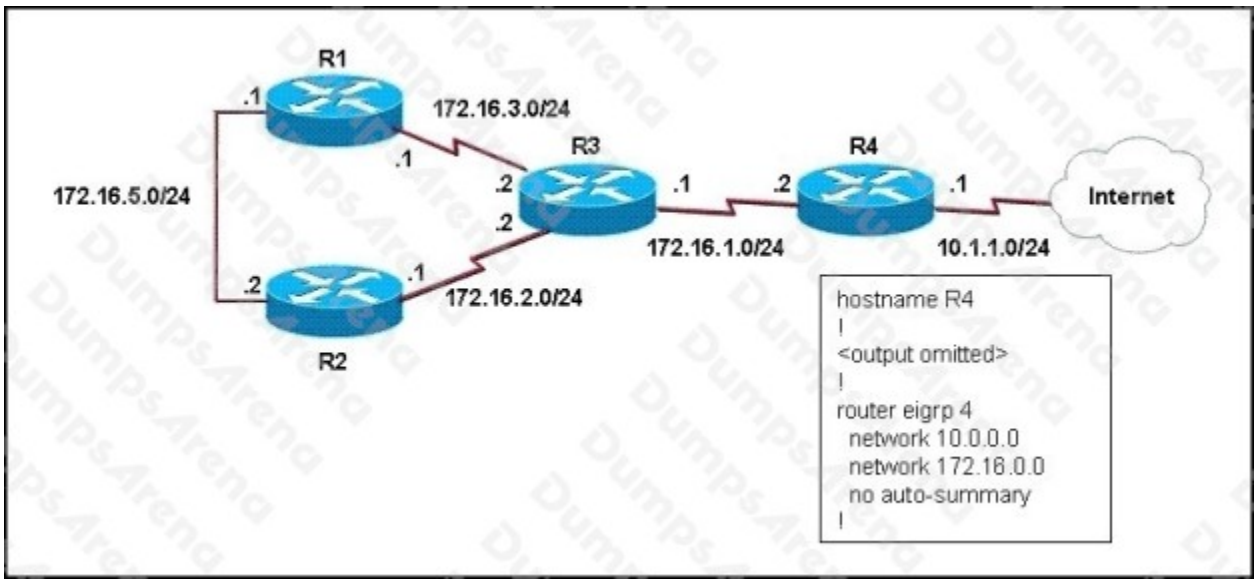
Passive-interface command is used in all routing protocols to disable sending updates out from a specific interface. However the command behavior varies from one protocol to another"

-- In RIP, this command will not allow sending multicast updates via a specific interface but will allow listening to incoming updates from other RIP speaking neighbors. This means that the router will still be able to receive updates on that passive interface and use them in its routing table.

-- In EIGRP and OSPF the passive-interface command stops sending outgoing hello packets, hence the router can not form any neighbor relationship via the passive interface. This behavior stops both outgoing and incoming routing updates.

QUESTION NO: 20

Refer to the exhibit.



EIGRP has been configured on all routers in the network. What additional configuration statement should be included on router R4 to advertise a default route to its neighbors?

A. R4(config)# ip default-network 10.0.0.0

B. R4(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1

C. R4(config)# ip route 10.0.0.0 255.0.0.0 10.1.1.1

D. R4(config-router)# default-information originate

ANSWER: A

Explanation:

The “ip default-network ” command will direct other routers to send its unknown traffic to this network. Other router (R1,R2,R3) will indicate this network as the “Gateway of last resort”.

There is another way to route unknown traffic to 10.1.1.0/24 network: create a static route using “ip route 0.0.0.0 0.0.0.0 10.1.1.2” command then inject this route using the “network 0.0.0.0” command, or using “redistribute static” command.

Note: In EIGRP, default routes cannot be directly injected (as they can in OSPF with the default-information originate command. Also, EIGRP does not have the “default-information originate” command).