Cisco

Exam Questions 642-885

Deploying Cisco Service Provider Advanced Routing (SPADVOUTE)

NEW QUESTION 1
Which four operations are components of MSDP in interdomain multicast setup? (Choose four.)

A. Multiple domains can have a single statically defined RP.
B. RPs interconnect between domains with UDP connections to pass source active messages.
C. RPs interconnect between domains with TCP connections to pass source active messages.
D. RPs send source active messages for internal sources to MSDP peers.
E. Source active messages are Peer-RPF checked before accepting or forwarding.
F. RPs learn about external sources via source active messages and may trigger (S,G) joins on behalf of local receivers.
G. MSDP connections typically parallel PIM-SM connections.

Answer: CDEF

NEW QUESTION 2
Which command configures a Source Specific Multicast on a Cisco IOS XR router?

A. configuremulticast-routing address-family ipv4 interface all enableexitrouter igmp version 3 commit
B. configuremulticast-routing address-family ipv4 interface all enableexitrouter igmp version 2 commit
C. configuremulticast-routing address-family ipv4 interface all enableexitrouter igmp version 1commit
D. configure interface all enable exitrouter igmp version 3 commit

Answer: A

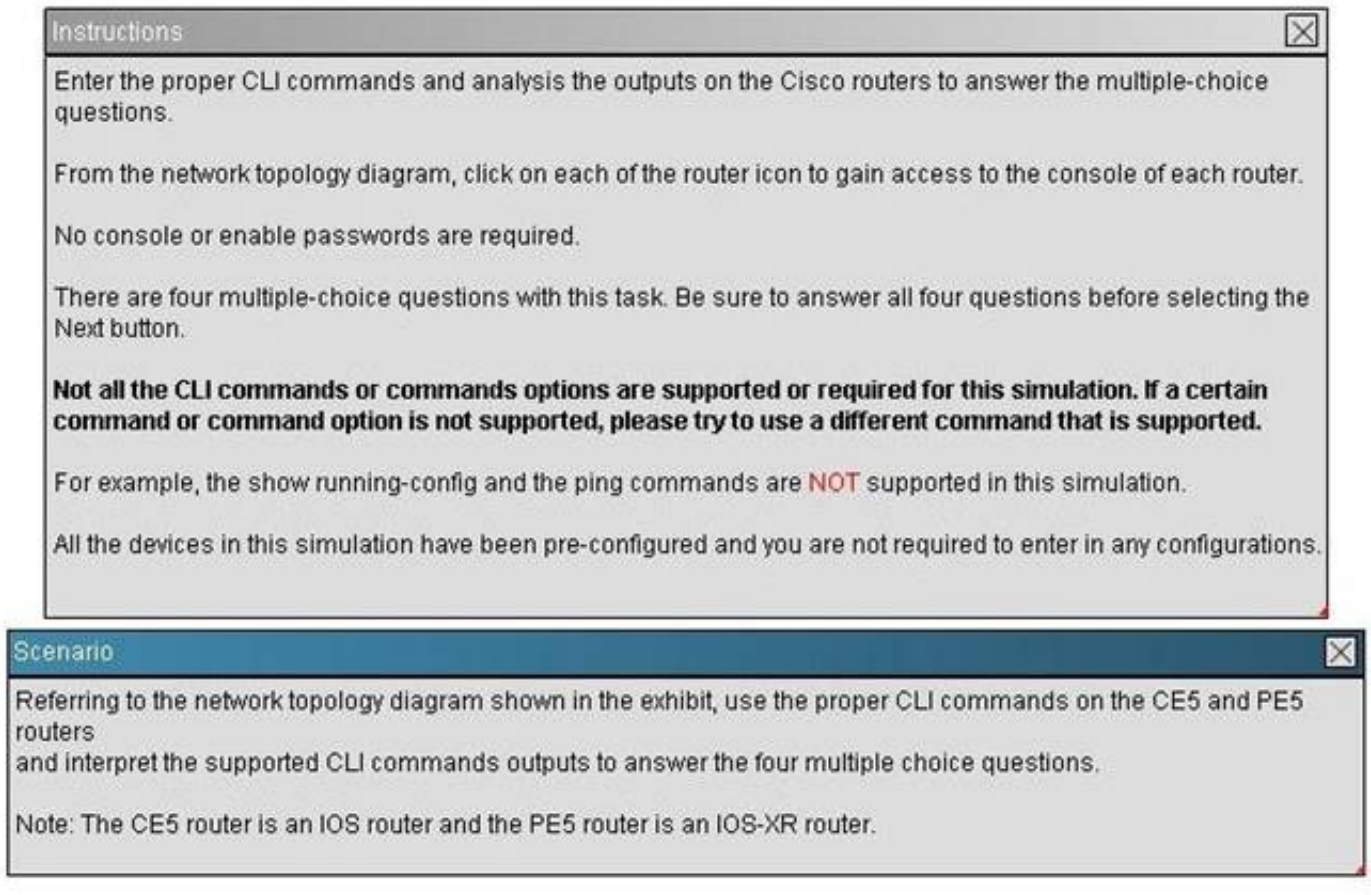
NEW QUESTION 3
When implementing interdomain multicast routing, which mechanism can be used to advertise multicast sources in one domain to the other domains, allowing the RPs to build interdomain multicast distribution trees?

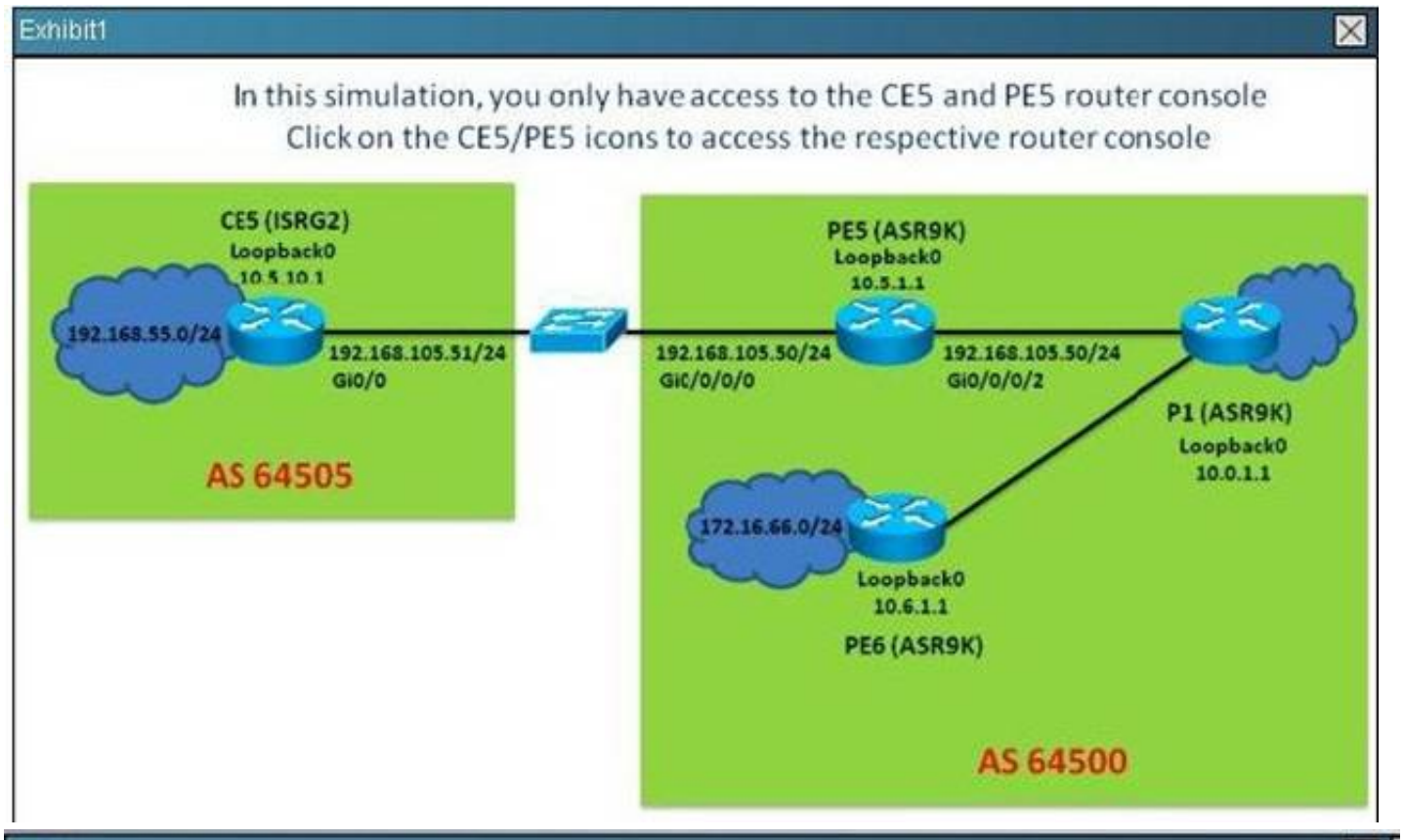
A. Multiprotocol BGP
B. PIM
C. MSDP
D. Auto RP
E. BSR
F. MLD

Answer: C

Explanation: Multicast Source Discovery Protocol
Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode domains.
MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains.
Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP in a PIM-SM domain has MSDP peering relationships with MSDP-enabled routers in other domains.
Each peering relationship occurs over a TCP connection, which is maintained by the underlying routing system.
MSDP speakers exchange messages called Source Active (SA) messages. When an RP learns about a local active source, typically through a PIM register message, the MSDP process encapsulates the register in an SA message and forwards the information to its peers. The message contains the source and group information for the multicast flow, as well as any encapsulated data. If a neighboring RP has local joiners for the multicast group, the RP installs the S, G route, forwards the encapsulated data contained in the SA
message, and sends PIM joins back towards the source. This process describes how a multicast path can be built between domains.

NEW QUESTION 4
Refer to the exhibit.





Which three statements regarding the BGP operations are correct? (Choose three)

A. PE5 will set the local preferences 200 on all the prefixes sent to CE5
B. PE5 will set the local preference to 200 on all the prefixes learned from CE5
C. CE5 has received 5 prefixes from the PE5 EBGP peer
D. CE5 has the BGP scan interval set to 30 seconds
E. CE5 is announcing the 192.168.55.0/24 prefix via EBGP to the PE5 EBGP peer
F. The AS-Path to reach the 209.165.202.128/27 prefix from CE5 is: 64500 64497 64498

Answer: CEF

Explanation: #sh ip bgp | be Network
#sh ip bgp
#show ip bgp neighbors

NEW QUESTION 5
When implementing IP SLA icmp-echo probes on Cisco IOS-XE routers, which two options are available for IPv6? (Choose two.)

A. flow-label
B. hop-limit
C. DSCP
D. traffic-class
E. TOS

Answer: AD

NEW QUESTION 6
Each router (RTA, RTB, and RTC) has one iBGP adjacency with the route reflector router RTD. Router RTC has an iBGP route advertised by RTA, but the same route is missing from RTB. Thenetwork engineer verifies that route filtering does not deny the route advertisement. Which action corrects the problem?

A. RTD(config-router)#neighbor 192.168.1.1 route-reflector-client RTD(config-router)#neighbor 192.168.1.1 description RTA RTD(config-router)#neighbor 192.168.1.2 route-reflector-client RTD(config-router)#neighbor 192.168.1.2 description RTB
B. RTC(config-router)#neighbor 192.168.1.4 route-reflector-client RTC(config-router)#neighbor 192.168.1.4 description RTD
C. RTA(config-router)#neighbor 192.168.1.4 route-reflector-client RTA(config-router)#neighbor 192.168.1.4 description RTDRTB(config-router)#neighbor 192.168.1.4 route-reflector-client RTB(config-router)#neighbor 192.168.1.4 description RTD
D. RTB(config-router)#neighbor 192.168.1.3 route-reflector-client RTB(config-router)#neighbor 192.168.1.3 description RTC
E. RTB(config-router)#neighbor 192.168.1.3 route-reflector-client RTB(config-router)#bgp cluster-id 192.168.1.2RTB(config-router)#no bgp client-to-client reflection

Answer: A

NEW QUESTION 7
Refer to the exhibit.

```
Router A:
 interface GigabitEthernet 0/0/0/0
  ipv4 address 10.6.1.1 255.255.255.252
 interface loopback 0
  ipv4 address 10.0.1.1 255.255.255.255
router msdp
 peer 10.0.1.2

Router B:
interface GigabitEthernet 0/0/0/0
  ipv4 address 10.6.1.2 255.255.255.252
 interface loopback 0
  ipv4 address 10.0.1.2 255.255.255.255
router msdp
 peer 10.0.1.1
```

Router A and Router B are connected via GigabitEthernet interfaces, but they are unable to form an MSDP neighborship. Which two components must be addressed when fixing the MSDP peering issue? (Choose two.)

A. An msdp default peer is configured on both routers.
B. A BGP process on each router is present so that MSDP can peer and carry updates.
C. The router interfaces are PIM-enabled to transport MSDP updates.
D. The connect-source attribute is configured with a host route under the MSDP process.
E. The MSDP peering on both routers specifies an origin ID so that it can peer.
F. The router A loopback interface configures the correct subnet mask.

Answer: DF

NEW QUESTION 8
Refer to the exhibit.

224.10.0.1
224.138.0.1
225.10.0.1
225.138.0.1
226.10.0.1
226.138.0.1
227.10.0.1
227.138.0.1
228.10.0.1
228.138.0.1
229.10.0.1
229.138.0.1
230.10.0.1
230.138.0.1
231.10.0.1
231.138.0.1
232.10.0.1
232.138.0.1
233.10.0.1
233.138.0.1
234.10.0.1
234.138.0.1
235.10.0.1
235.138.0.1
236.10.0.1
236.138.0.1
237.10.0.1
237.138.0.1
238.10.0.1
238.138.0.1
239.10.0.1
239.138.0.1

The following multicast IP addresses map to which multicast MAC address?

A. 01:00:5E:8A:00:01
B. 01:00:5E:0A:00:01
C. 01:00:5E:7A:00:01
D. 01:00:5E:05:00:01

Answer: B

NEW QUESTION 9
Which two commands can be used to implement a valid Cisco IOS XE IPv6 static tunnel configuration? (Choose two.)

A. interface Tunnel100 ipv6 enableipv6 address 2001:DB8::1/128 tunnel destination 209.165.201.2 tunnel mode ipv6ip 6to4
B. interface Tunnel100 ipv6 enableipv6 address 2001:DB8::1/128 tunnel source Ethernet 0/1 tunnel destination 209.165.201.2 tunnel mode gre ip
C. interface Tunnel 100 ipv6 enableip address 209.165.201.2 tunnel source Loopback 0 tunnel mode ipv6ip 6to4
D. interface Tunnel100 ipv6 enableipv6 address 2001:DB8::1/128 tunnel source Ethernet 0/1 tunnel destination 209.165.201.2 tunnel mode isatap
E. interface Tunnel100 ipv6 enableipv6 address 2001:DB8::1/128 tunnel source Ethernet 0/1 tunnel destination 209.165.201.2 tunnel mode auto-tunnel
F. interface Tunnel100 ipv6 enableipv6 address 2001:DB8::1/128 tunnel source Ethernet 0/1 tunnel destination 209.165.201.2tunnel mode ipv6ip

Answer: BF

NEW QUESTION 10
A network engineer for an ISP wants to reduce the number of iBGP adjacencies. A merge is taking place with another ISP network, so the network engineer needs to make both ASNs look like a single network for the Internet. Which BGP technology is most suitable?

A. route reflector
B. confederation
C. clustering
D. peer group

Answer: B

NEW QUESTION 10
When implementing source-based remote-triggered black hole filtering, which two configurations are required on the edge routers that are not the signaling router? (Choose two.)

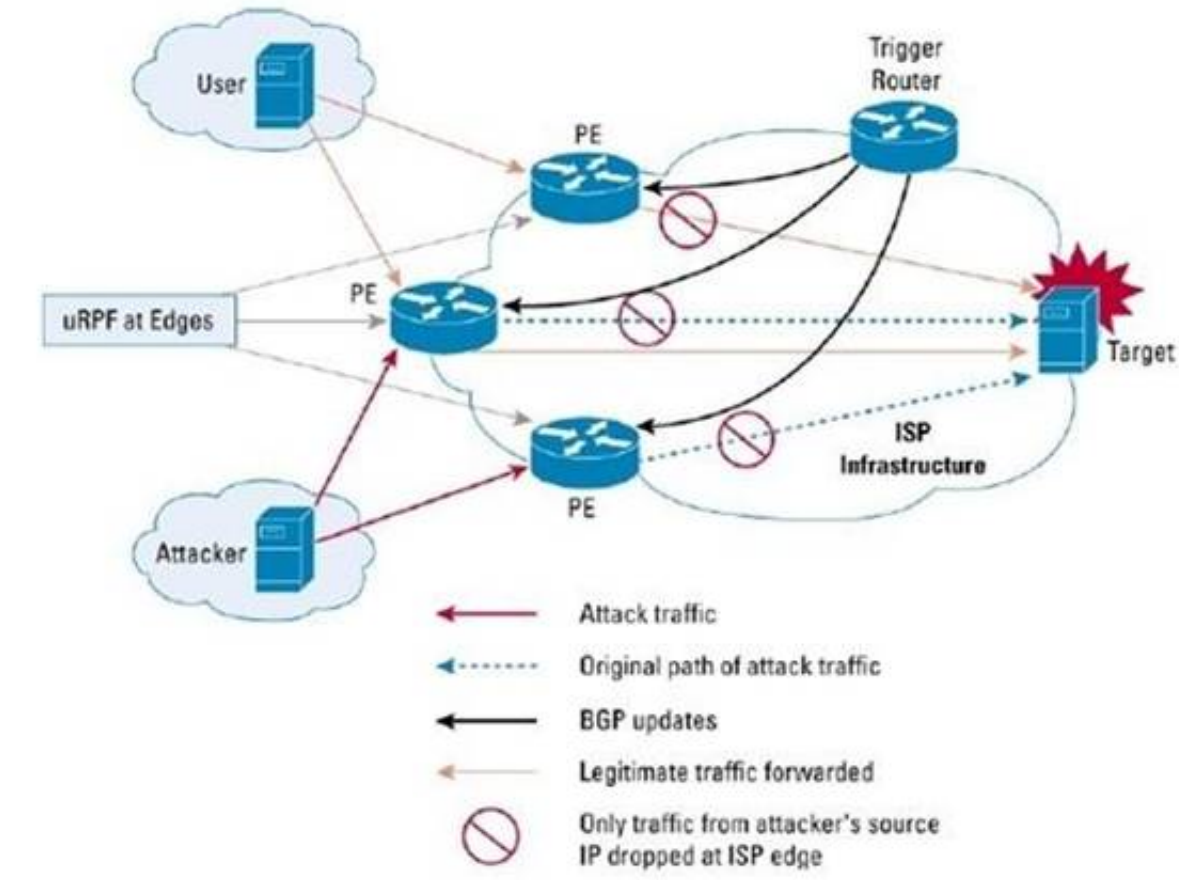
A. A static route to a prefix that is not used in the network with a next hop set to the Null0 interface
B. A static route pointing to the IP address of the attacker
C. uRPF on all external facing interfaces at the edge routers
D. Redistribution into BGP of the static route that points to the IP address of the attacker
E. A route policy to set the redistributed static routes with the no-export BGP community

Answer: AC

Explanation: Source-Based RTBH Filtering
With destination-based black holing, all traffic to a specific destination is dropped after the black hole has been activated, regardless of where it is coming from. Obviously, this could include legitimate traffic destined for the target. Source-based black holes provide the ability to drop traffic at the network edge based on a

specific source address or range of source addresses.
If the source address (or range of addresses) of the attack can be identified (spoofed or not), it would be better to drop all traffic at the edge based on the source address, regardless of the destination address. This would permit legitimate traffic from other sources to reach the target. Implementation of source-based black hole filtering depends on Unicast Reverse Path Forwarding (uRPF), most often loose mode uRPF.
Loose mode uRPF checks the packet and forwards it if there is a route entry for the source IP of the incoming packet in the router forwarding information base (FIB). If the router does not have an FIB entry for the source IP address, or if the entry points to a null interface, the Reverse Path Forwarding (RPF) check fails and the packet is dropped, as shown in Figure
2. Because uRPF validates a source IP address against its FIB entry, dropping traffic from specific source addresses is accomplished by configuring loose mode uRPF on the external interface and ensuring the RPF check fails by inserting a route to the source with a next hop of Null0.
This can be done by using a trigger device to send IBGP updates. These updates set the next hop for the source IP to an unused IP address that has a static entry at the edge, setting it to null as shown in Figure 2.

Figure 2. Source-Based Black Hole Filtering



In this way, traffic that is entering the edge network sourced from a host that has a route pointing to null will result in a uRPF drop.

NEW QUESTION 14
Which two functions are supported for BGP extension MP-BGP for IP multicasting? (Choose two.)

A. A network can support incongruent unicast and multicast topologies.
B. A network can support congruent unicast and multicast topologies.
C. MP-BGP is an enhanced BGP that carries routing information for multiple network layer protocols and IP multicast routes.
D. MP-BGP carries single sets of routes for unicast routing and multicast routing.
E. MP-BGP is useful when a link dedicated to multicast and unicast traffic is desired.

Answer: AC

NEW QUESTION 15
When implementing high-availability stateful switchover BGP routing, in which situation would Cisco NSR be required?

A. On the PE routers connecting to the CE routers which are not NSF aware or are not NSF capable
B. On the PE routers connecting to the CE routers which support graceful restart
C. On the PE routers connecting to the CE routers which are incapable of performing stateful switchover operations because the CE routers are only NSF aware but not NSF capable
D. On the PE routers connecting to the CE routers which are incapable of performingstateful switchover operations because the CE routers are only NSF capable but not NSF aware
E. On the service provider core P routers which are also NSF aware
F. On the service provider core P routers which are also NSF capable

Answer: A

NEW QUESTION 19
Refer to the Cisco IOS-XR show output exhibit.

```
RP/0/RSP0/CPU0:P1#show bgp neighbors 10.1.1.1 configuration
Wed Oct 26 17:45:09.690 UTC
neighbor 10.1.1.1
 remote-as 64500                [ ]
 update-source Loopback0        [ ]
 address-family IPv4 Unicast    [ ]
```

Which statement is correct?

A. The [ ] indicates the configuration has a problem

B. The [ ] indicates the 10.1.1.1 neighbor peering session has not been established
C. The [ ] indicates the configuration was not inherited from a group
D. The [ ] indicates the configuration has not been committed
E. The [ ] indicates the corresponding BGP peer configuration has a mismatch configuration

Answer: C

Explanation: show bgp neighbors
Use the show bgp neighbors command to display information about the BGP configuration for neighbors.
•Use the configuration option to display the effective configuration for the neighbor, including any settings that have been inherited from session groups, neighbor groups, or af-groups used by this neighbor.
•Use the inheritance option to display the session groups, neighbor groups, and af-groups from which this neighbor inherits configuration settings.
The following example displays sample output from the show bgp af-group command using the configuration keyword. This example shows where each configuration item was
inherited from. The default-originate command was configured directly on this address family group (indicated by [ ]). The remove-private-as command was inherited from address family group GROUP_2, which in turn inherited from address family group GROUP_3:

```
RP/0/0/CPU0:router# show bgp af-group GROUP_1 configuration

af-group GROUP_1 address-family ipv4 unicast
  capability orf prefix-list both           [a:GROUP_2]
  default-originate                         []
  maximum-prefix 2500 75 warning-only       []
  policy POLICY_1 in                        [a:GROUP_2 a:GROUP_3]
  remove-private-AS                         [a:GROUP_2 a:GROUP_3]
  send-community-ebgp                       [a:GROUP_2]
  send-extended-community-ebgp              [a:GROUP_2
```

NEW QUESTION 23
The IPv6 2002::/16 prefix is used in which kind of implementations?

A. 6 RD
B. 6 to 4
C. NAT 64
D. IPv6 Multicast

Answer: B

NEW QUESTION 28
An engineer is providing DNS for IPv6 over a currently working IPv4 domain. Which three changes are needed to offer DNS functionality for IPv6? (Choose three.)

A. Define a new record that stores the 128-bit IPv6 address.
B. Expand the existing IP address record to allow for 128 bits.
C. Define the IPv6 equivalent of the in-addr.arpa.com domain of the IPv4 PTR.
D. Modify the in-addr.arpa.com domain of the IPv4 PTR.
E. Change the query messages.
F. Transport IPv6 query messages by using UDP.
G. Transport IPv6 query messages by using TCP.

Answer: ACE

NEW QUESTION 29
Which three statements regarding NAT64 operations are correct? (Choose three.)

A. With stateful NAT64, many IPv6 address can be translated into one IPv4 address, thus IPv4 address conservation is achieved
B. Stateful NAT64 requires the use of static translation slots so IPv6 hosts and initiate connections to IPv4 hosts.
C. With stateless NAT64, the source and destination IPv4 addresses are embedded in the IPv6 addresses
D. NAT64 works in conjunction with DNS64
E. Both the stateful and stateless NAT64 methods will conserve IPv4 address usage

Answer: ACD

Explanation: Stateful NAT64-Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
Stateful NAT64 multiplexes many IPv6 devices into a single IPv4 address. It can be assumed that this technology will be used mainly where IPv6-only networks and clients (ie. Mobile handsets, IPv6 only wireless, etc...) need access to the IPv4 internet and its services.
The big difference with stateful NAT64 is the elimination of the algorithmic binding between the IPv6 address and the IPv4 address. In exchange, state is created in the NAT64 device for every flow. Additionally, NAT64 only supports IPv6-initiated flows. Unlike stateless NAT64, stateful NAT64 does `not' consume a single IPv4 address for each IPv6 device that wants to communicate to the IPv4 Internet. More practically this means that many IPv6- only users consume only single IPv4 address in similar manner as IPv4-to-IPv4 network address and port translation works. This works very well if the connectivity request is initiated from the IPv6 towards the IPv4 Internet. If an IPv4-only device wants to speak to an IPv6-only server for example, manual configuration of the translation slot will be required, making this mechanism less attractive to provide IPv6 services towards the IPv4 Internet. DNS64 is usually also necessary with a stateful NAT64, and works the same with both stateless and stateful NAT64
Stateless NAT64-Stateless translation between IPv4 and IPv6 RFC6145 (IP/ICMP Translation Algorithm) replaces RFC2765 (Stateless IP/ICMP Translation

Algorithm (SIIT)) and provides a stateless mechanism to translate a IPv4 header into an IPv6 header and vice versa. Due to the stateless character this mechanism is very effective and highly fail safe because more as a single-or multiple translators in parallel can be deployed and work all in parallel without a need to synchronize between the translation devices.
The key to the stateless translation is in the fact that the IPv4 address is directly embedded in the IPv6 address. A limitation of stateless NAT64 translation is that it directly translates only the IPv4 options that have direct IPv6 counterparts, and that it does not translate any IPv6 extension headers beyond the fragmentation extension header; however, these limitations are not significant in practice.
With a stateless NAT64, a specific IPv6 address range will represent IPv4 systems within the IPv6 world. This range needs to be manually configured on the translation device. Within the IPv4 world all the IPv6 systems have directly correlated IPv4 addresses that can be algorithmically mapped to a subset of the service provider's IPv4 addresses. By means of this direct mapping algorithm there is no need to keep state for any translation slot between IPv4 and IPv6. This mapping algorithm requires the IPv6 hosts be assigned specific IPv6 addresses, using manual configuration or DHCPv6.
Stateless NAT64 will work very successful as proven in some of the largest networks, however it suffers from some an important side-effect: Stateless NAT64 translation will give an IPv6-only host access to the IPv4 world and vice versa, however it consumes an IPv4 address for each IPv6-only device that desires translation -- exactly the same as a dual- stack deployment. Consequentially, stateless NAT64 is no solution to address the ongoing IPv4 address depletion.Stateless NAT64 is a good tool to provide Internet servers with an accessible IP address for both IPv4 and IPv6 on the global Internet. To aggregate many IPv6 users into a single IPv4 address, stateful NAT64 is required. NAT64 are usually deployed in conjunction with a DNS64. This functions similar to, but different than, DNS- ALG that was part of NAT-PT. DNS64 is not an ALG; instead, packets are sent directly to and received from the DNS64's IP address. DNS64 can also work with DNSSEC (whereas DNS-ALG could not).

NEW QUESTION 33
Which of the following can be used by dual-stack service providers supporting IPv4/IPv6 customers with dual-stack hosts using public IPv6 addresses and private IPv4 addresses?

A. NAT64
B. 6RD
C. 6to4 tunnels
D. Carrier-grade NAT

Answer: D

Explanation: Carrier Grade NAT is a large-scale NAT, capable of providing private-IPv4-to-public-IPv4 translation in the order of millions of translations. Carrier Grade NAT can support several hundred thousand subscribers with the bandwidth throughput of at least 10Gb/s full-duplex. With IPv4 addresses reaching depletion, Carrier Grade NAT is vital in providing private IPv4 connectivity to the public IPv4 internet. In addition, Carrier Grade NAT is not limited to IPv4 NAT; it can also translate between IPv4 and IPv6 addresses.

NEW QUESTION 34
Which two actions result when a network administrator attempts to ping an IPv6 host on the LAN? (Choose two.)

A. ARP is used to determine the MAC address of the destination host.
B. Neighbor Discovery is used to determine the MAC address of the destination host.
C. Neighbor Solicitation messages are sent out by the source host to determine the data link-layer address of the destination host.
D. Neighbor Advertisement messages are sent by the source host to announce its presence on the local link.
E. Router Solicitation messages are sent out on a specific multicast address to request the data link-layer address of the target device.
F. Router Solicitation messages are sent to the local router on the network segment to request data link-layer information about the destination host.

Answer: BC

NEW QUESTION 36
An SP core is running PIM on the network. Multicast groups in this networkare in the 232.0.0.0/8 range. Which commandenables multicast routing operations without using an RP?

A. ip pim autorp
B. ip pim ssm default
C. ip pim bidir-enable
D. ip pim register-source

Answer: B

NEW QUESTION 40
Refer to the Cisco IOS-XR configuration exhibit.

```
multicast-routing
!
interface Loopback0
 ipv4 address 10.3.1.1 255.255.255.255
!
interface GigabitEthernet0/0/0/0
 ipv4 address 192.168.103.30 255.255.255.0
 no shut
!
interface GigabitEthernet0/0/0/1
 ipv4 address 192.168.156.50 255.255.255.0
 no shut
!
router isis 1
 net 49.0005.0100.0300.1001.00
 address-family ipv4 unicast
  !
 interface Loopback0
  address-family ipv4 unicast
  !
 interface GigabitEthernet0/0/0/0
  address-family ipv4 unicast
 !
 interface GigabitEthernet0/0/0/1
  address-family ipv4 unicast
!
router pim
address-family ipv4
auto-rp mapping-agent Loopback0 scope 16
auto-rp candidate-rp Loopback0 scope 16
!
interface Loopback0
enable
interface GigabitEthernet0/0/0/0
enable
interface GigabitEthernet0/0/0/1
enable
!
```

The Cisco IOS-XR router is unable to establish any PIM neighbor relationships. What is wrong with the configuration?

A. The configuration is missing:interface gi0/0/0/0 ip pim sparse-mode interface gi0/0/0/1 ip pim sparse-mode interface loopback0 ip pim sparse-mode
B. The configuration is missing: multicast-routingaddress-family ipv4 interface gi0/0/0/0 enableinterface gi0/0/0/1 enable
C. The auto-rp scoping configurations should be set to 1 not 16
D. The RP address has not been configured using the rp-address router PIM configuration command
E. PIM defaults to dense mode operations only, so PIM sparse mode must be enabled using the pim sparse-mode router PIM configuration command

Answer: B

NEW QUESTION 42
A service providerrequests more details about the recent Inter-AS MPLS VPN Option B configuration that was recently deployed. Consider this configuration:
router bgp 3717
address-family vpnv4 unicast retain route-target all
commit
!
Which option describes why this particular command is needed?

A. The ASBRcan have many working customer VRFs, so this configuration ensures the coexistence of all the route-target extended communities that belong to the all ASBR- terminated customer VRFs.
B. When implementing the Inter-AS Option B MPLS VPN solution, all the route targets that are transmitted over the Inter-AS links need an ASBR local database to forward thecustomer traffic correctly.
C. The Inter-AS Option B design implements VPNv4 communication over the Inter-AS link, hence the requirement for a route-target association for each customer VPN connected across two or more ASs.
D. In the Inter-AS Option B design, no local VRF is maintained on the ASBR routers,so the default behavior of the operating system is to deny any route-target extended community that is encoded in the incoming iBGP update
E. This configuration permits VPNv4 communication by accepting the iBGP updates even if no route targets are configured locally.

Answer: D

NEW QUESTION 46
Which four statements are correct regarding MSDP configurations and operations? (Choose four.)

A. The MSDP peers are also typically the RPs in respective routing domains.
B. SA messages are flooded to all other MSDP peers without any restrictions
C. On Cisco IOS, IOS-XE, and IOS-XR, the router can be configured to cache the SA messages to reduce the join latency
D. SA messages are used to advertise active sources in a domain
E. MSDP establishes neighbor relationships with other MSDP peers using TCP port 639

F. MSDP peerings on Cisco IOS, IOS-XE, and IOS-XR support MD5 or SHA1 authentication

Answer: ACDE

Explanation: http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_msdp_im_pim_sm.ht ml
When MSDP is enabled, an RP in a PIM-SM domain maintains MSDP peering relationships with MSDPenabled routers in other domains. This peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. MSDP uses TCP (port 639) for its peering connections. As with BGP, using point-to-point TCP peering means that each peer must be explicitly configured. The TCP connections between RPs, moreover, are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source- tree building mechanism provided by PIM-SM. MSDP is also used to announce sources sending to a group. These announcements must originate at the RP of the domain.

NEW QUESTION 49
Refer to the exhibit.

```
router bgp 65123
 bgp cluster-id 17
 address-family ipv4 unicast
 exit
```

Given the partial BGP configuration, which configuration correctly completes the Cisco IOS-XR route reflector configuration where both the 1.1.1.1 and 2.2.2.2 routers are the clients and the 3.3.3.3 router is a non-client IBGP peer?

A. neighbor 1.1.1.1remote-as 65123 route-reflector-client neighbor 2.2.2.2remote-as 65123 route-reflector-client neighbor 3.3.3.3remote-as 65123
B. neighbor 1.1.1.1 address-family ipv4 unicast remote-as 65123route-reflector-client neighbor 2.2.2.2address-family ipv4 unicast remote-as 65123route-reflector-client neighbor 3.3.3.3address-family ipv4 unicast remote-as 65123
C. neighbor 1.1.1.1remote-as 65123address-family ipv4 unicast route-reflector-client neighbor 2.2.2.2remote-as 65123address-family ipv4 unicast route-reflector-client neighbor 3.3.3.3remote-as 65123
D. neighbor 1.1.1.1 remote-as 65123neighbor 1.1.1.1 route-reflector-clientneighbor 2.2.2.2 remote-as 65123neighbor 2.2.2.2 route-reflector-clientneighbor 3.3.3.3 remote-as 65123

Answer: C

NEW QUESTION 50
Refer to the Cisco IOS-XR show output exhibit.

```
RP/0/RSP0/CPU0:PE1#show mrib route
Thu Dec  1 19:14:38.044 UTCIP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
    IF - Inherit From, D - Drop, MA - MDT Address, ME - MDT Encap,
    MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
    CD - Conditional Decap, MPLS - MPLS Decap, MF - MPLS Encap, EX - Extranet
    MoFE - MoFRR Enabled, MoFS - MoFRR State
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, DI - Decapsulation Interface
    EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
    EX - Extranet, A2 - Secondary Accept

<output omitted>

(*,224.1.1.1) RPF nbr: 192.168.11.1 Flags: C
  Up: 14:34:53
  Incoming Interface List
    GigabitEthernet0/0/0/2 Flags: A NS, Up: 14:34:53
  Outgoing Interface List
    Loopback0 Flags: F IC NS II LI, Up: 14:34:53
    GigabitEthernet0/0/0/0 Flags: F NS, Up: 14:34:33
```

Which two statements are correct? (Choose two.)

A. The RPF neighbor 192.168.11.1 is the path towards the RP for the 224.1.1.1 multicast group
B. The RP for the 224.1.1.1 multicast group is reachable over the Gi0/0/0/0 interface
C. This router is the RP for the 224.1.1.1 multicast group
D. Incoming 224.1.1.1 multicast group traffic will be sent out through the Gi0/0/0/0 interface
E. Incoming 224.1.1.1 multicast group traffic will be sent out through the Gi0/0/0/2 interface

Answer: AD

NEW QUESTION 51
Which difference occurs between intradomain and interdomain routing technology?

A. PIM is used in intradomain routing technology and uses reverse path forwarding mechanism to implement optimize multicast data forwarding.
B. MSDP is used in intradomain routing technology to discover the multicast source.
C. Interdomain routing technology uses MSDP and M-BGP for exchanging multicast routing information.
D. RP is not needed in intradomain routing technology, but RP is needed in interdomain routing technology to receive multicast traffic.

Answer: A

NEW QUESTION 53
In which four ways does DHCPv6 differ from DHCPv4? (Choose four.)

A. DHCPv6 uses the same message types as DHCPv4.
B. DHCPv4 functions without external protocols.
C. A host discovers a DHCPv6 server by using a DHCP Discover packet.
D. A hosts discovers a DHCPv6 server by using a DHCP Solicit packet.
E. A DHCPv6 server replies with a DHCP Offer packet.
F. A DHCP server replies with a DHCP Advertise message.
G. An IPv6 host can request multiple addresses at the same time from a DHCPv6 server.
H. An IPv6 host can request only one IP address at a time from a DHCPv6 server.

Answer: BDFG

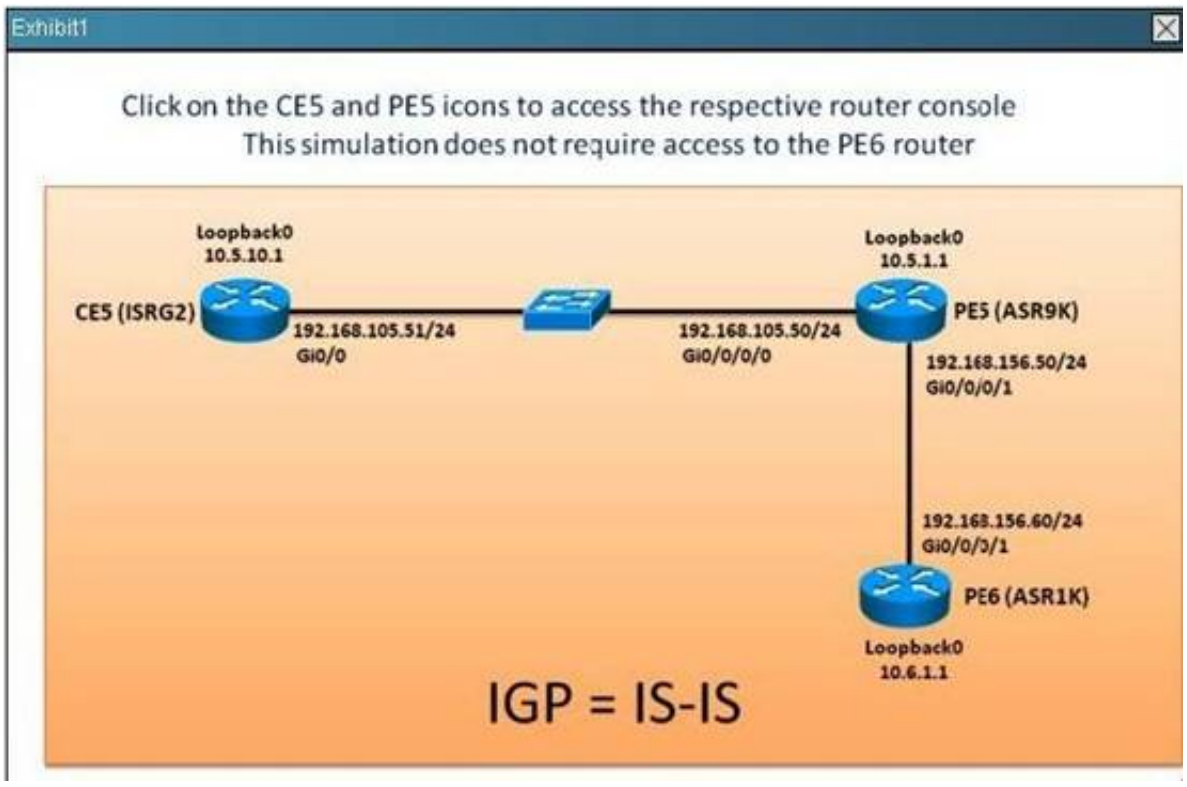
NEW QUESTION 57
Which two statements correctly describe the BGP ttl-security feature? (Choose two.)

A. This feature protects the BGP processes from CPU utilization-based attacks from EBGP neighbors which can be multiple hops away
B. This feature prevents IBGP sessions with non-directly connected IBGP neighbors
C. This feature will cause the EBGP updates from the router to be sent using a TTL of 1
D. This feature needs to be configured on each participating BGP router
E. This feature is used together with the ebgp-multihop command

Answer: AD

Explanation: http://packetlife.net/blog/2009/nov/23/understanding-bgp-ttl-security/

NEW QUESTION 61
Refer to the exhibit.



Which three statements are correct regarding the various multicast groups? (Choose three.)

A. Currently there is no source sending traffic to the 224.1.1.1 multicast group
B. PE5 has a Null OILforthe (*,224.0.1.40) entry
C. PE5 has a Null OILforthe (*,224.1.1.1) entry
D. CE5 has joined the 224.0.1.40 multicast group
E. CE5 has a Null OILforthe (*,224.1.1.1) entry

Answer: CDE

Explanation: #show ip mroute

NEW QUESTION 65
Which multicast implementation is preferred for traffic that is required by a small number of receivers across a large distributed network?

A. DVMRP
B. PIM-DM
C. PIM-SM
D. IGMP

Answer: C

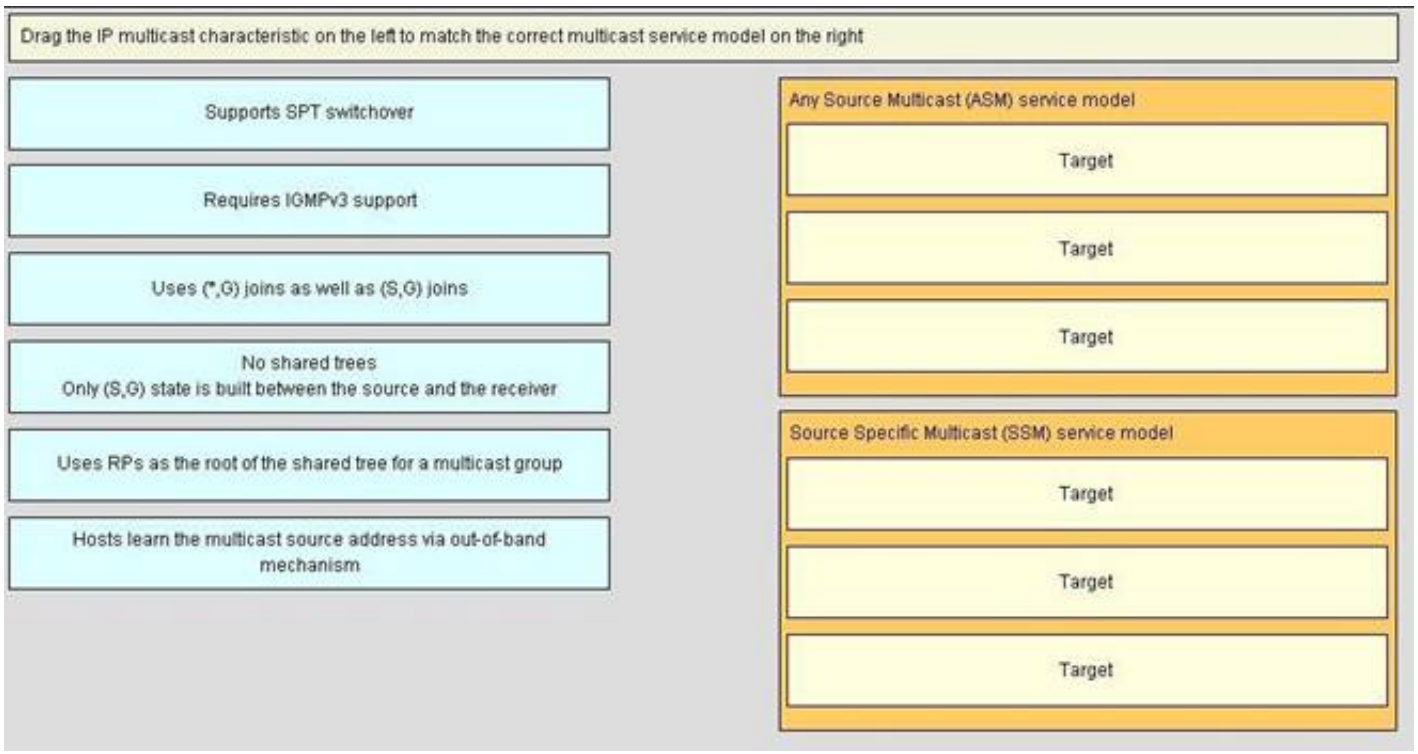
NEW QUESTION 67
Which configuration for implementing 6PE on an IS-IS-enabled Cisco IOS XR router is correct?

A. interface GigabitEthernet0/0/0/0 ipv6 address 2001:DB8:DD11::1/64 router isis ipv6-tunnet 49.0000.0000.00010.00address-family ipv6 unicast single-topologyredistribute bgp 200interface GigabitEthernet0/0/0/0 address-family ipv6 unicast router bgp 200bgp router-id 209.165.202.129 address-family ipv4 unicast address-family ipv6 unicast redistribute isis ipv6-tun neighbor 209.165.202.130remote-as 200address-family ipv4 unicast address-family ipv6 labeled-unicast
B. interface GigabitEthernet0/0/0/0 ipv6 address 2001:DB8:DD11::1/64 router isis ipv6-tunnet 49.0000.0000.00010.00address-family ipv6 unicast single-

topologyrouter bgp 200bgp router-id 209.165.202.129 address-family ipv4 unicast address-family ipv6 unicast redistribute isis ipv6-tun neighbor 209.165.202.130remote-as 200address-family ipv4 unicast address-family ipv6 labeled-unicast
C. interface GigabitEthernet0/0/0/0 ipv6 address 2001:DB8:DD11::1/64 router isis ipv6-tunnet 49.0000.0000.00010.00address-family ipv6 unicast single-topologyinterface GigabitEthernet0/0/0/0 address-family ipv6 unicast router bgp 200bgp router-id 209.165.202.129 address-family ipv4 unicast address-family ipv6 unicast redistribute staticneighbor 209.165.202.130remote-as 200address-family ipv4 unicast address-family ipv6 labeled-unicast
D. interface GigabitEthernet0/0/0/0 ipv6 address 2001:DB8:DD11::1/64 router isis ipv6-tunnet 49.0000.0000.00010.00address-family ipv6 unicast single-topologyinterface GigabitEthernet0/0/0/0 address-family ipv6 unicast router bgp 200bgp router-id 209.165.202.129 address-family ipv4 unicast address-family ipv6 unicastredistribute connected redistribute isis ipv6-tun neighbor 209.165.202.130remote-as 200address-family ipv4 unicast address-family ipv6 labeled-unicast
E. interface GigabitEthernet0/0/0/0 ipv6 address 2001:DB8:DD11::1/64 router isis ipv6-tunnet 49.0000.0000.00010.00address-family ipv6 unicast single-topologyinterface GigabitEthernet0/0/0/0 address-family ipv6 unicast router bgp 200bgp router-id 209.165.202.129 address-family ipv4 unicast address-family ipv6 unicast redistribute connected redistribute isis ipv6-tun neighbor 209.165.202.130remote-as 200address-family ipv4 unicast

Answer: D

NEW QUESTION 70
DRAG DROP



Answer:

Explanation: Any Source Multicast - Uses RP's as the root of the shared tree for a multicast group, ONly (S,G) state is build between the source and the recevier, Spport SPT Switchover Source Specific Multicast - Uses (*,G) joins as well as (S,G) Joins , Requires IGMPV3 Support,
Hosts learn the multicast source address via out-of-banf mechanism
i) Dense Mode Flood-and-Prune Protocols (DVMRP / MOSPF / PIM-DM)
In dense mode protocols, all routers in the network are aware of all trees, their sources and receivers.
Protocols such as DVMRP and PIM dense mode flood “active source” information across the whole network and build trees by creating “Prune State” in parts of the topology where traffic for a specific tree is unwanted.
They are also called flood-and-prune protocols. In MOSPF, information about receivers is flooded throughout the network to support the building of trees.
Dense mode protocols are undesirable because every tree built in some part of the network will always cause resource utilization (with convergence impact) on all routers in the network (or within the administrative scope, if configured). We will not be discussing these protocols in the rest of this paper.
ii) Sparse Mode Explicit Join Protocols (PIM-SM/PIM-BiDir)
With sparse mode explicit join protocols we do not create a group-specific forwarding state in the network unless a receiver has sent an explicit IGMP/MLD membership report (or “join”) for a group. This variant of ASM is known to scale well and is the multicast paradigm we will mainly be discussing. This is the basis for PIMSparse Mode, which most multicast deployments have used to this point. This is also the basis for PIM-BiDir, which will be increasingly deployed for MANY (sources) TO MANY (receivers) applications.
These protocols are called sparse mode because they efficiently support IP multicast delivery trees with a “sparse” receiver population – creating control plane state only on routers in the path between sources and receivers, and in PIM-SM/BiDir, the Rendezvous Point (RP). They never create state in other parts of the network. State in a router is only built explicitly when it receives a join from a downstream router or receiver, hence the name “explicit join protocols”.
Both PIM-SM and PIM-BiDir employ “SHARED TREES”, which allow traffic from any source to be forwarded to a receiver. The forwarding state on a shared tree is referred to as (*,G) forwarding state, where the * is a wild card for ANY SOURCE. Additionally, PIM- SM supports the creation of forwarding state that relates to traffic from a specific source. These are known as SOURCE TREES, and the associated state is referred to as (S, G) forwarding state SSM is the model used when the receiver (or some proxy) sends (S,G) “joins” to indicate that it wants to receive traffic sent by source S to group G. This is possible with IGMPv3/MLDv2 “INCLUDE” mode membership reports. We therefore refer to this model as the Source-Specific Multicast (SSM) model. SSM mandates the use of an explicit-join protocol between routers. The standard protocol for this is PIM-SSM, which is simply the subset of PIM-SM used to create (S,G) trees. There are no shared trees (*,G) state in SSM. Multicast receivers can thus “join” an ASM group G, or “join” (or more accurately “subscribe” to) an SSM (S, G) channel. To avoid having to repeat the term “ASM group or SSM channel”, we will use the term (multicast) flow in the text, implying that the flow could be an ASM group or an SSM channel

NEW QUESTION 74
What must occur before an (S,G) entry can be populated in the multicast routing table?

A. The (*,G) entry must have timed out
B. The (*,G) entry OIL must be null
C. The router must be directly connected to the multicast source
D. The parent (*,G) entry must be created first

Answer: D

NEW QUESTION 76
Which multicast routing protocol is most optimal for supporting many-to-many multicast applications?

A. PIM-SM
B. PIM-BIDIR
C. MP-BGP
D. DVMRP
E. MSDP

Answer: B

Explanation: PIM-Bidirectional Operations
PIM Bidirectional (BIDIR) has one shared tree from sources to RP and from RP to receivers. This is unlike the PIM-SM, which is unidirectional by nature with multiple source trees - one per (S, G) or a shared tree from receiver to RP and multiple SG trees from RP to sources.
Benefits of PIM BIDIR are as follows:
• As many sources for the same group use one and only state (*, G), only minimal states are required in each router.
• No data triggered events.
• Rendezvous Point (RP) router not required. The RP address only needs to be a routable address and need not exist on a physical device.

NEW QUESTION 81
What is enabled by default on Cisco IOS-XR routers and cannot be disabled?

A. SSH server
B. Multicast routing
C. IPv4 and IPv6 CEF
D. IPv6 routing
E. CDP
F. BFD

Answer: C

Explanation: Before using the BGP policy accounting feature, you must enable BGP on the router (CEF is enabled by default).

NEW QUESTION 85
Which multicast routing protocol supports dense mode, sparse mode and bidirectional mode?

A. DVMRP
B. MOSPF
C. PIM
D. MP-BGP
E. MSDP

Answer: C

NEW QUESTION 89
When configuring PIM operations, what is the effect of setting the SPT threshold to infinity?

A. The multicast source to the RP path will never switch over to the shortest path tree
B. All the PIM routers will have more (S,G) states, thus consuming more router resources
C. The receivers will be able to immediately switch over to the shortest path tree after receiving the first multicast packets on the shared tree via the RP
D. The last-hop routers will never switch over to the shortest path tree and will always remain on the shared tree

Answer: D

NEW QUESTION 91
Which informationdoes the multicast supported router need to forward the multicast traffic over the source or shared tree?

A. source address
B. multicast address
C. destination address
D. mGRE headers
E. MDT Data

Answer: C

NEW QUESTION 94
In secure multicast, which protocol is used to distribute secure keys to a multicast group?

A. ISAKMP
B. RSA
C. IPsec
D. GDOI
E. SKIP

Answer: D

NEW QUESTION 96
A network engineer is working for an ISP and a current eBGP customer requests to enable the BGP TTL security feature. The engineer sees from the current established BGP session that the eBGP peer is directly connected and the ebgp-multihop feature is already in use with a value of one. Which two actions are needed on the Cisco IOS XR router to accomplish the task? (Choose two.)

A. Configure the neighbor with the command ttl-security.
B. Disable the eBGP-multihop feature.
C. Clear the BGP session for the configuration change to take effect.
D. Enable the BGP TTL security and the BGP peer resets automatically for the change to take effect.
E. Configure the neighbor with the command ttl-security 254.

Answer: AC

NEW QUESTION 99
Which four statements are correct regarding MSDP configurations and operations? (Choose four.)

A. The MSDP peers are also typically the RPs in respective routing domains.
B. SA messages are flooded to all other MSDP peers without any restrictions
C. On Cisco IOS, IOS-XE, and IOS-XR, the router can be configured to cache the SA messages to reduce the join latency
D. SA messages are used to advertise active sources in a domain
E. MSDP establishes neighbor relationships with other MSDP peers using TCP port 639
F. MSDP peerings on Cisco IOS, IOS-XE, and IOS-XR support MD5 or SHA1 authentication

Answer: ACDE

NEW QUESTION 100
Refer to the exhibit.

Instructions

Enter the proper CLI commands and analysis the outputs on the Cisco routers to answer the multiple-choice questions.

From the network topology diagram, click on each of the router icon to gain access to the console of each router.

No console or enable passwords are required.

There are four multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.

Not all the CLI commands or commands options are supported or required for this simulation.

For example, the show running-config and the ping commands are NOT supported in this simulation.

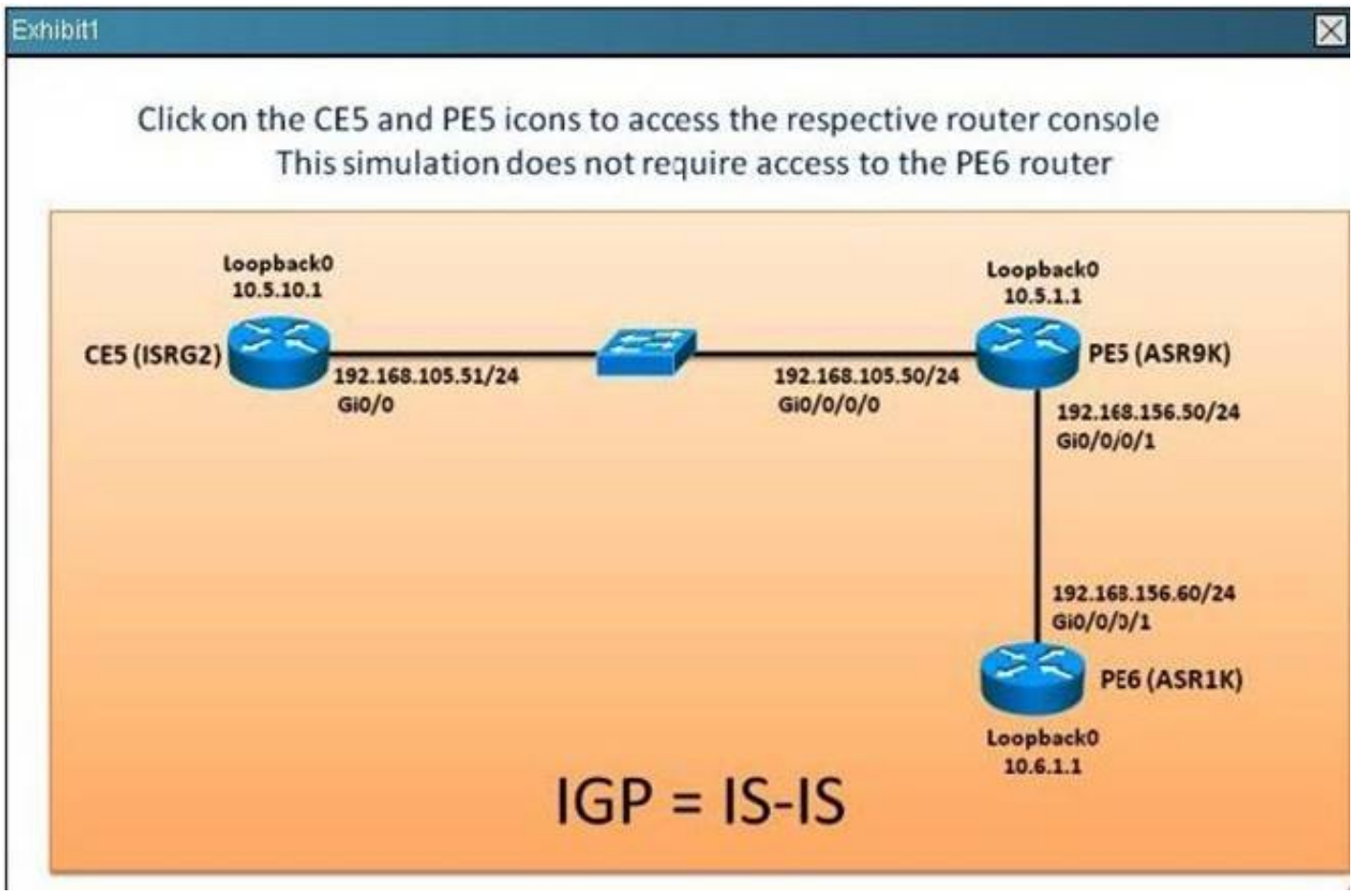
All the devices in this simulation have been pre-configured and you are not required to enter in any configurations.

Scenario

Referring to the network topology diagram shown in the exhibit, use the proper CLI commands on the CE5, PE5 and PE6 routers
and interpret the supported CLI commands outputs to answer the four multiple choice questions.

Note: The CE5 router is an IOS router, the PE5 router is an IOS-XR router, and the PE6 router is an IOS-XE router.

Exhibit1



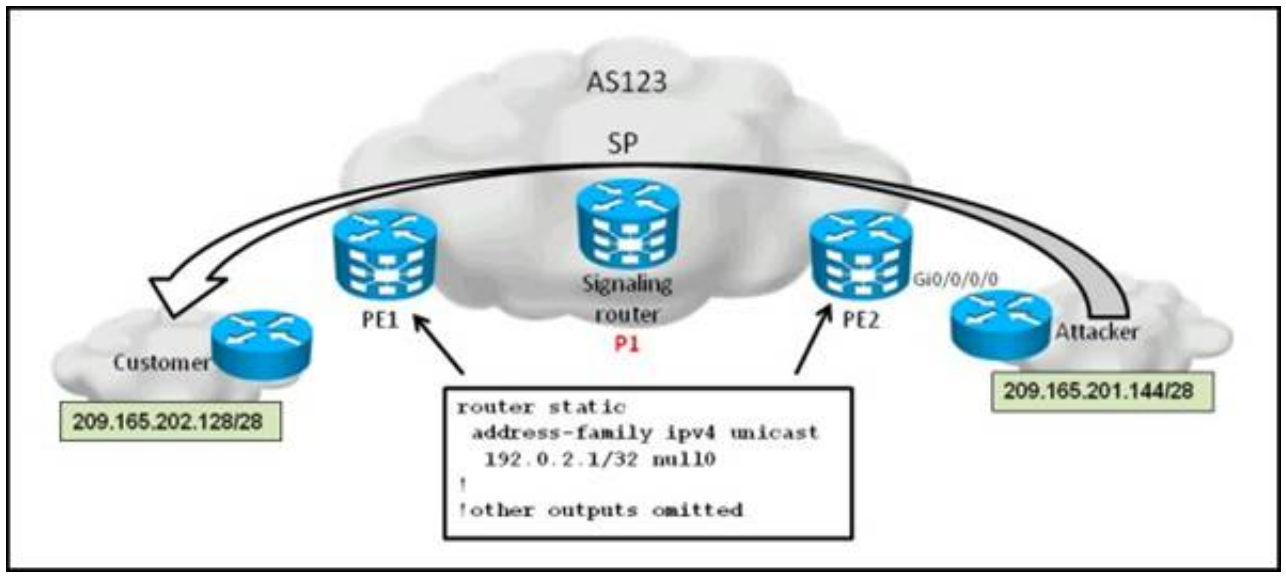
Which two statements are correct regarding the multicast operations on the router that is the RP? (Choose two.)

A. It is using IGMPv3
B. The IGMP query interval is set to 125 seconds
C. It is using the IPv4 unicast routing table to perform the RPF checks
D. Static multicast routes are configured on the RP

Answer: AC

Explanation: #show ip mroute
#show ip pim interface
#show ip igmp group
#show ip pim neighbor

NEW QUESTION 104
Refer to the topology diagram shown in the exhibit and the partial configurations shown below.

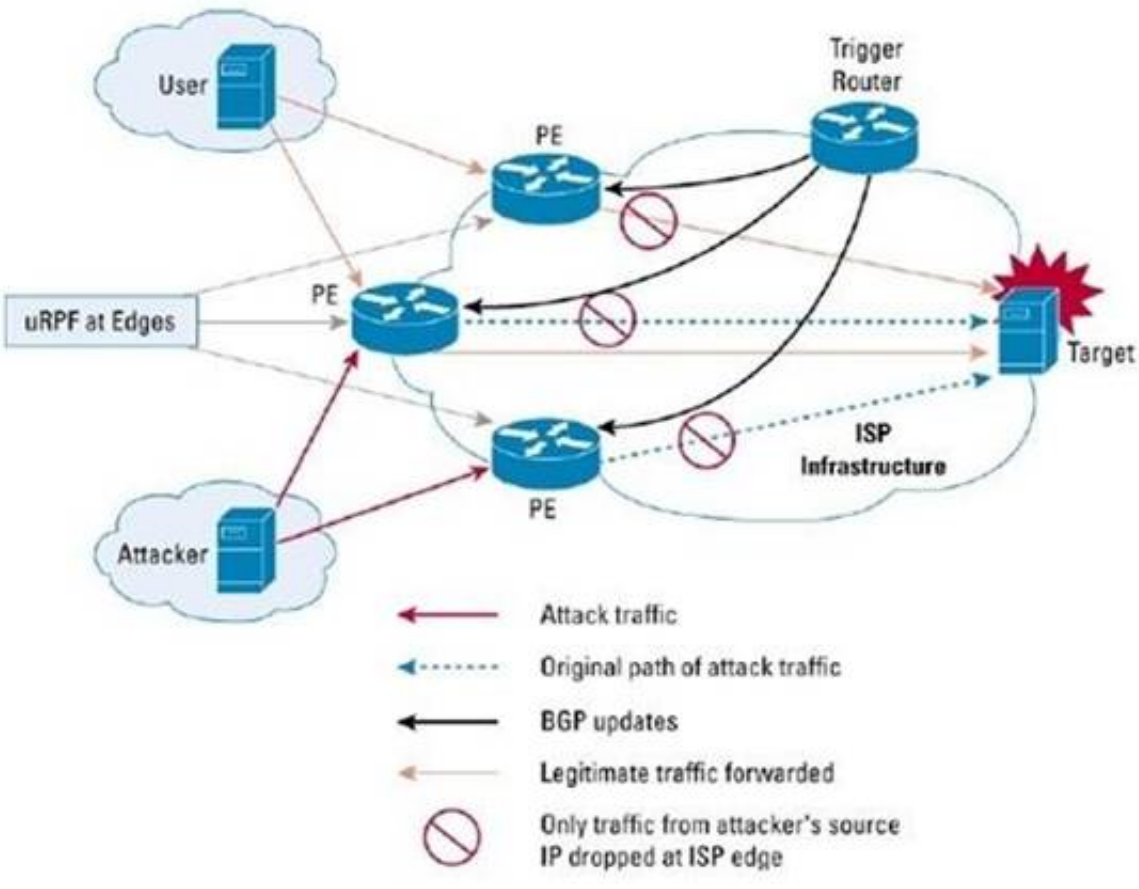


Once the attack from 209.165.201.144/28 to 209.165.202.128/28 has been detected, which additional configurations are required on the P1 IOS-XR router to implement source-based remote-triggered black hole filtering?
!
router bgp 123
address-family ipv4 unicast redistribute static route-policy test
!

A. router staticaddress-family ipv4 unicast 209.165.202.128/28 null0 tag 666192.0.2.1/32 null0 tag 667!route-policy test if tag is 666 thenset next-hop 192.0.2.1 endifif tag is 667 thenset community (no-export) endifend-policy!
B. router staticaddress-family ipv4 unicast 209.165.201.144/28 null0 tag 666192.0.2.1/32 null0 tag 667!route-policy test if tag is 666 thenset next-hop 192.0.2.1 endifif tag is 667 thenset community (no-export) endifend-policy!
C. router staticaddress-family ipv4 unicast 209.165.201.144/28 null0 tag 666192.0.2.1/32 null0!route-policy test if tag is 666 thenset next-hop 192.0.2.1set community (no-export) endifend-policy
D. router staticaddress-family ipv4 unicast 209.165.202.128/28 null0 tag 666192.0.2.1/32 null0!route-policy test if tag is 666 thenset next-hop 192.0.2.1set community (no-export) endifend-policy!

Answer: C

Explanation: Source-Based RTBH Filtering
With destination-based black holing, all traffic to a specific destination is dropped after the black hole has been activated, regardless of where it is coming from. Obviously, this could include legitimate traffic destined for the target. Source-based black holes provide the ability to drop traffic at the network edge based on a specific source address or range of source addresses.
If the source address (or range of addresses) of the attack can be identified (spoofed or not), it would be better to drop all traffic at the edge based on the source address, regardless of the destination address. This would permit legitimate traffic from other sources to reach the target. Implementation of source-based black hole filtering depends on Unicast Reverse Path Forwarding (uRPF), most often loose mode uRPF. Loose mode uRPF checks the packet and forwards it if there is a route entry for the source IP of the incoming packet in the router forwarding information base (FIB). If the router does not have an FIB entry for the source IP address, or if the entry points to a null interface, the Reverse Path Forwarding (RPF) check fails and the packet is dropped, as shown in Figure 2. Because uRPF validates a source IP address against its FIB entry, dropping traffic from specific source addresses is accomplished by configuring loose mode uRPF on the external interface and ensuring the RPF check fails by inserting a route to the source with a next hop of Null0. This can be done by using a trigger device to send IBGP updates. These updates set the next hop for the source IP to an unused IP address that has a static entry at the edge, setting it to null as shown in Figure 2.
Figure 2. Source-Based Black Hole Filtering



In this way, traffic that is entering the edge network sourced from a host that has a route pointing to null will result in a uRPF drop.

NEW QUESTION 109
In Cisco IOS-XR, the maximum-prefix command, to control the number of prefixes that can be installed from a BGP neighbor, is configured under which configuration mode?

A. RP/0/RSP0/CPU0:P2(config-bgp)#
B. RP/0/RSP0/CPU0:P2(config-bgp-af)#
C. RP/0/RSP0/CPU0:P2(config-bgp-nbr)#
D. RP/0/RSP0/CPU0:P2(config-bgp-nbr-af)#

Answer: D

Explanation: http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a00801 0a28a.shtml

NEW QUESTION 110
In Cisco IOS-XR, the ttl-security command is configured under which configuration mode?

A. RP/0/RSP0/CPU0:P2(config)#
B. RP/0/RSP0/CPU0:P2(config-bgp)#
C. RP/0/RSP0/CPU0:P2(config-bgp-nbr)#
D. RP/0/RSP0/CPU0:P2(config-bgp-af)#
E. RP/0/RSP0/CPU0:P2(config-bgp-nbr-af)#

Answer: C

Explanation: http://packetlife.net/blog/2009/nov/23/understanding-bgp-ttl-security/

NEW QUESTION 112
The bsr-border router PIM interface configuration command is used for what purpose?

A. To enable the router as the candidate RP
B. To enable the router as the candidate BSR
C. To enable the router as the BSR mapping agent
D. To set up an administrative boundary to prevent BSR messages from being sent out through an interface
E. To define a boundary to restrict the RP discovery and announcement messages from being sent outside the PIM-SM domain

Answer: D

NEW QUESTION 115
When enabling interdomain multicast routing, which two statements are correct? (Choose two.)

A. Multiprotocol BGP is used instead of PIM SM to build the intradomain and interdomain multicast distribution trees
B. Use MSDP to enable the RPs from different domains to exchange information about active multicast sources
C. MSDP SA packets are sent between the multiprotocol BGP peers
D. Noncongruent unicast and multicast topologies can be supported using multiprotocol BGP

Answer: BD

Explanation: http://prakashkalsaria.wordpress.com/2010/08/11/mbgp-msdp/
MSDP In the PIM-SM model, multicast sources and receivers must register with their local RP. Actually, the router closest to the sources or receivers registers with the RP, but the key point to note is that the RP knows about all the sources and receivers for any particular
group. RPs in other domains have no way of knowing about sources located in other domains. MSDP is an elegant way to solve this problem.
MSDP is a mechanism that allows RPs to share information about active sources. RPs know about the receivers in their local domain. When RPs in remote domains hear about the active sources, they can pass on that information to their local receivers and multicast data can then be forwarded between the domains.
A useful feature of MSDP is that it allows each domain to maintain an independent RP that does not rely on other domains, but it does enable RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.
The RP in each domain establishes an MSDP peering session using a TCP connection with the RPs in other domains or with border routers leading to the other domains. When the RP learns about a new multicast source within its own domain (through the normal PIM register mechanism), the RP encapsulates the first data packet in a Source-Active (SA) message and sends the SA to all MSDP peers. The SA is forwarded by each receiving peer using a modified RPF check, until the SA reaches every MSDP router in the interconnected networks—theoretically the entire multicast internet. If the receiving MSDP peer is an RP, and the RP has a (*, G) entry for the group in the SA (there is an interested receiver), the RP creates (S, G) state for the source and joins to the shortest path tree for the source. The encapsulated data is decapsulated and forwarded down the shared tree of that RP. When the packet is received by the last hop router of the receiver, the last hop router also may join the shortest path tree to the source. The MSDP speaker periodically sends SAs that include all sources within the own domain of the RP
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.2/routing/configuration/guide/rc32bgp.html
Multiprotocol BGP
Multiprotocol BGP is an enhanced BGP that carries routing information for multiple network layer protocols and IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing.
The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) feature to build data distribution trees.
Multiprotocol BGP is useful when you want a link dedicated to multicast traffic, perhaps to limit which resources are used for which traffic. Multiprotocol BGP allows you to have a unicast routing topology different from a multicast routing topology providing more control over your network and resources.
In BGP, the only way to perform interdomain multicast routing was to use the BGP infrastructure that was in place for unicast routing. Perhaps you want all multicast traffic exchanged at one network access point (NAP).
If those routers were not multicast capable, or there were differing policies for which you wanted multicast traffic to flow, multicast routing could not be supported without multiprotocol BGP.
Note It is possible to configure BGP peers that exchange both unicast and multicast network layer reachability information (NLRI), but you cannot connect multiprotocol BGP clouds with a BGP cloud. That is, you cannot redistribute multiprotocol BGP routes into BGP.

Figure 1 illustrates simple unicast and multicast topologies that are incongruent, and therefore are not possible without multiprotocol BGP.

Autonomous systems 100, 200, and 300 are each connected to two NAPs that are FDDI rings. One is used for unicast peering (and therefore the exchange of unicast traffic). The Multicast Friendly Interconnect (MFI) ring is used for multicast peering (and therefore the exchange of multicast traffic). Each router is unicast and multicast capable.

Figure 1 Incongruent Unicast and Multicast Routes

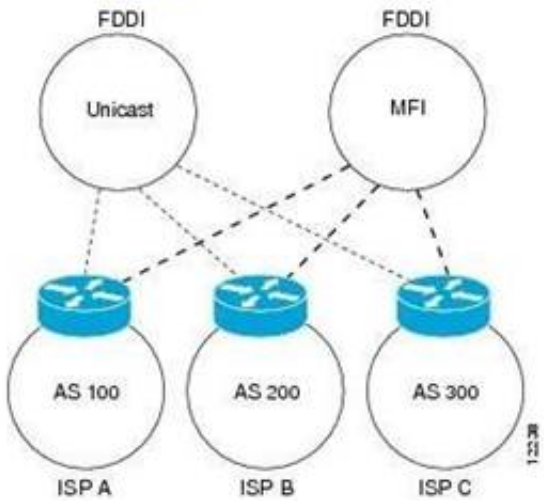


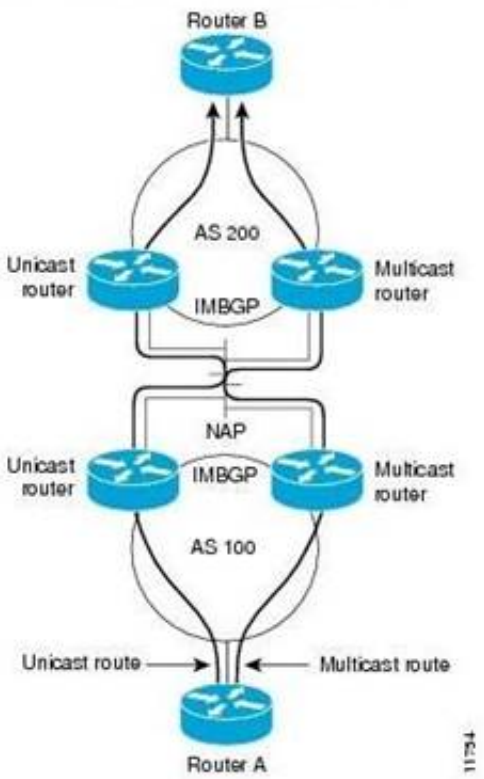
Figure 2 is a topology of unicast-only routers and multicast-only routers. The two routers on the left are unicast-only routers (that is, they do not support or are not configured to perform multicast routing). The two routers on the right are multicast-only routers. Routers A and B support both unicast and multicast routing. The unicast-only and multicast-only routers are connected to a single NAP.

In Figure 2, only unicast traffic can travel from Router A to the unicast routers to Router B and back. Multicast traffic could not flow on that path, so another routing table is required. Multicast traffic uses the path from Router A to the multicast routers to Router B and back.

Figure 2 illustrates a multiprotocol BGP environment with a separate unicast route and multicast route from Router A to Router B. Multiprotocol BGP allows these routes to be incongruent. Both of the autonomous systems must be configured for internal multiprotocol BGP (IMBGP) in the figure.

A multicast routing protocol, such as PIM, uses the multicast BGP database to perform Reverse Path Forwarding (RPF) lookups for multicast-capable sources. Thus, packets can be sent and accepted on the multicast topology but not on the unicast topology.

Figure 2 Multicast BGP Environment



NEW QUESTION 120
Which keyword is used in the syntax to refer to Cisco IOS XR address-family groups, session groups, or neighbor groups?

A. inherit
B. apply
C. use
D. commit

Answer: C

NEW QUESTION 123
Which two specific characteristics categorize traceroute in an IPv6 routing environment? (Choose two.)

A. Traceroute can show the path to reach any destination IPv6 address.
B. Traceroute returns an error for a link-local IPv6 address.
C. Traceroute is based on ICMPv6 Type 1 (Destination Unreachable) reply packets to determine the network path.
D. Traceroute is based on ICMPv6 Type 3 (Time Exceeded) reply packets to determine the network path.
E. Traceroute is based on ICMPv6 Type 2 (Packet Too Big) reply packets to determine the network path.
F. Traceroute for IPv6 implements a backwards compatibility option to provide a detailed report in environments running dual-stack.

Answer: AD

NEW QUESTION 128

The 224.192.16.1 multicast IP address maps to which multicast MAC address?

A. 01-00-5E-C0-10-01
B. 01-00-5E-40-10-01
C. 01-00-5E-00-10-01
D. 01-00-5E-C0-16-01

Answer: B

Explanation: Least significant 23 bits of IP address and pre-pend 01-00-5E
224 ignore
192 less 128 becomes 64 = 40
16 = 10
1 = 01
01-00-5E-40-10-01

NEW QUESTION 130
Which configuration would an engineer use to exchange IPv6 multicast routes via BGP with a neighbor that does not support thecorresponding Multicast SAFI onCisco IOS XE?

A. router bgp 100bgp router-id 209.165.201.10 no bgp default ipv4-unicastneighbor 2001:DB8::10 remote-as 201neighbor 2001:DB8::10 update-source GigabitEthernet 0/10 address-family ipv6 multicastneighbor 2001:DB8::10 activate network 2001:DB8:CDCD:1::/64exit-address-family
B. router bgp 100bgp router-id 209.165.201.10 no bgp default ipv4-unicastneighbor 2001:DB8::10 remote-as 201neighbor 2001:DB8::10 update-source GigabitEthernet 0/10 address-family ipv6neighbor 2001:DB8::10 translate-update ipv6 multicast unicast neighbor 2001:DB8::10 activateno synchronization exit address-familyaddress-family ipv6 multicast neighbor 2001:DB8::10 activate network 2001:DB8:CDCD:1::/64exit-address-family
C. router bgp 100bgp router-id 209.165.201.10 no bgp default ipv4-unicastneighbor 2001:DB8::10 remote-as 201neighbor 2001:DB8::10 update-source GigabitEthernet 0/10 address-family ipv6neighbor 2001:DB8::10 activate address-family ipv6 multicast neighbor 2001:DB8::10 activate network 2001:DB8:CDCD:1::/64exit-address-family
D. router bgp 100bgp router-id 209.165.201.10 no bgp default ipv4-unicastneighbor 2001:DB8::10 remote-as 201neighbor 2001:DB8::10 update-source GigabitEthernet 0/10 address-family ipv6neighbor 2001:DB8::10 translate-update ipv6 multicast unicast no synchronizationexit address-familyaddress-family ipv6 multicast neighbor 2001:DB8::10 activate network 2001:DB8:CDCD:1::/64exit-address-family
E. router bgp 100bgp router-id 209.165.201.10 no bgp default ipv4-unicastneighbor 2001:DB8::10 remote-as 201neighbor 2001:DB8::10 update-source GigabitEthernet 0/10 address-family ipv6neighbor 2001:DB8::10 send-labelneighbor 2001:DB8::10 override-capability-neg neighbor 2001:DB8::10 activateno synchronization exit address-familyaddress-family ipv6 multicast network 2001:DB8:CDCD:1::/64exit-address-family

Answer: B

NEW QUESTION 132
Which type of DNS record is used for IPv6 forward lookups?

A. A records
B. AAAA records
C. PTR records
D. MX records

Answer: B

NEW QUESTION 136
Which field in the IPv6 header can be used to set the DSCP value?

A. Flow Label
B. Type of Service
C. Traffic Class
D. Precedence
E. EXP

Answer: C

Explanation: Traffic Class
The Traffic Class field is an 8 bit field that is used to signify the importance of the data contained within this specific packet. With IPv4, this information was signified with the TOS field and supported both IP precedence and Differentiated Services Code Point (DSCP). The Traffic Class field used with IPv6 supports DSCP solely; this specification uses the first 6 bits to indicate the Per Hop Behavior (PHB) of the contained data; these PHB's are defined in RFC 2474 and its additions.

NEW QUESTION 141
Which multicast routing protocol is used to forward multicast data along the optimal path from source to receivers?

A. PIM DM
B. PIM Bi-Dir
C. PIM SM
D. SSM
E. IGMP
F. MSDP

Answer: C

NEW QUESTION 145
Which two features are used to provide high availability multicast? (Choose two.)

A. BFD
B. NSF/SSO
C. PIM NSR
D. PIM triggered join
E. IGMP triggered report
F. MSDP

Answer: BD

Explanation: Triggered joins are sent when the primary or the secondary RPF information changes. No RPF change prunes are sent for MoFRR streams.
mofrr
To perform a fast convergence (multicast-only fast reroute, or MoFRR) of specified routes/flows when a failure is detected on one of multiple equal-cost paths between the router and the source, use the mofrr command under PIM configuration mode.
mofrr rib acl_name no rib acl_name

NEW QUESTION 148
Which protocol can be used to secure multicast in a group multicast solution where group key management is needed for secure key exchange?

A. DOI
B. ISAKMP
C. GDOI
D. IPsec

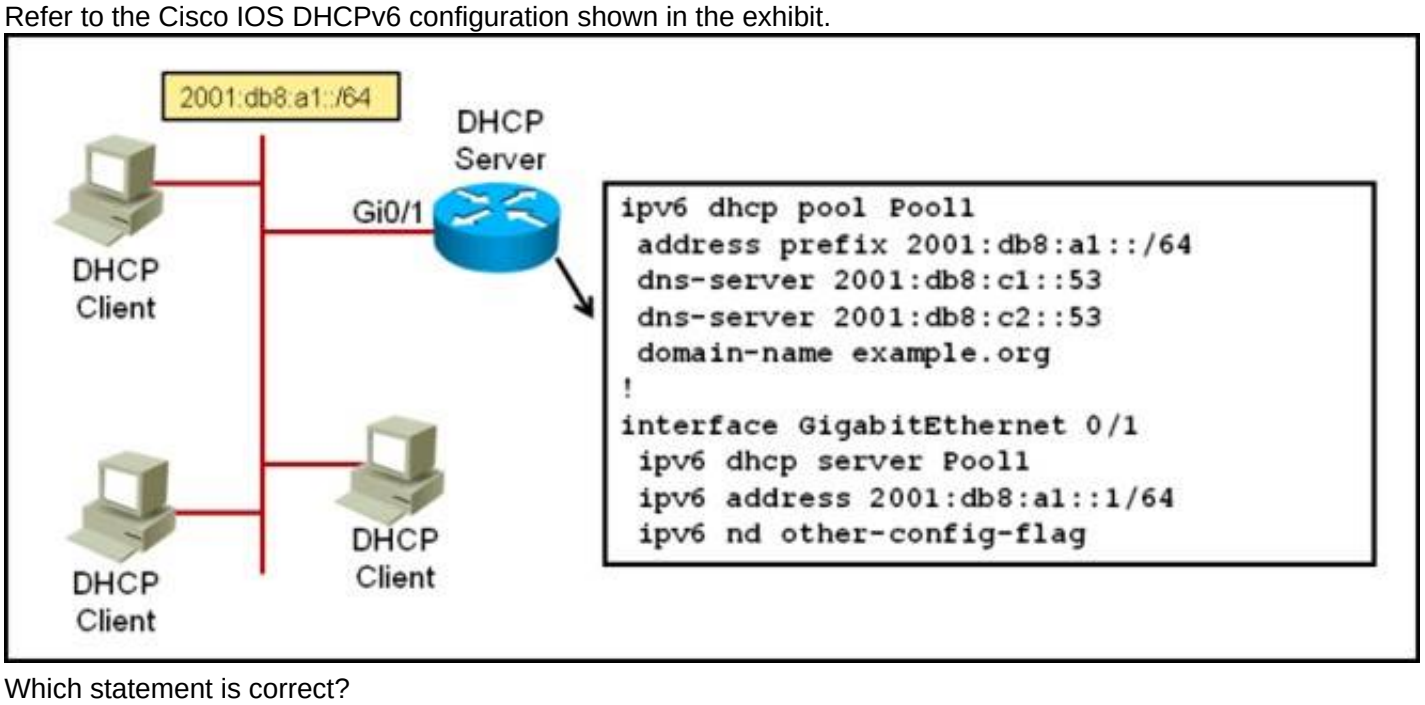
Answer: C

NEW QUESTION 153
Which Cisco IOS XR command setssuccessfully configure a value of 20 for the advertisement-interval?

A. RP/0/RSP0/CPU0:routerconfig)# router bgp 65512 RP/0/RSP0/CPU0:router(config-bgp)# session-group test RP/0/RSP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 20 RP/0/RSP0/CPU0:router(config-bgp-sngrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor-group test RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# advertisement-interval 25 RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor 192.168.1.1RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 65513 RP/0/RSP0/CPU0:router(config-bgp-nbr)# use session-group test RP/0/RSP0/CPU0:router(config-bgp-nbr)# use neighbor-group test
B. RP/0/RSP0/CPU0:routerconfig)# router bgp 65512 RP/0/RSP0/CPU0:router(config-bgp)# session-group test RP/0/RSP0/CPU0:router(config-bgp-sngrp)# ebgp-multihop 2 RP/0/RSP0/CPU0:router(config-bgp-sngrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor-group test RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# advertisement-interval 20 RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor 192.168.1.1RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 65513 RP/0/RSP0/CPU0:router(config-bgp-nbr)# use session-group test RP/0/RSP0/CPU0:router(config-bgp-nbr)# use neighbor-group test
C. RP/0/RSP0/CPU0:routerconfig)# router bgp 65512 RP/0/RSP0/CPU0:router(config-bgp)# session-group test RP/0/RSP0/CPU0:router(config-bgp-sngrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor-group test RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor 192.168.1.1RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 65513 RP/0/RSP0/CPU0:router(config-bgp-nbr)# use session-group test RP/0/RSP0/CPU0:router(config-bgp-nbr)# use neighbor-group test
D. RP/0/RSP0/CPU0:routerconfig)# router bgp 65512 RP/0/RSP0/CPU0:router(config-bgp)# session-group test RP/0/RSP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 25 RP/0/RSP0/CPU0:router(config-bgp-sngrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor-group test RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# advertisement-interval 20 RP/0/RSP0/CPU0:router(config-bgp-nbrgrp)# exit RP/0/RSP0/CPU0:router(config-bgp)# exit RP/0/RSP0/CPU0:router(config-bgp)# neighbor 192.168.1.1RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 65513 RP/0/RSP0/CPU0:router(config-bgp-nbr)# use session-group test RP/0/RSP0/CPU0:router(config-bgp-nbr)# use neighbor-group test

Answer: A

NEW QUESTION 154
Refer to the Cisco IOS DHCPv6 configuration shown in the exhibit.



Which statement is correct?

A. The configuration is missing a command under interface Gi0/1 to indicate to the attached hosts to use stateful DHCPv6 to obtain their IPv6 addresses
B. The IPv6 router advertisements indicate to the attached hosts on the Gi0/1 interface to get other information besides their IPv6 address via stateless auto configuration

C. The IPv6 DHCPv6 server pool configuration is misconfigured
D. The DNS server address can also be imported from another upstream DHCPv6 server

Answer: A

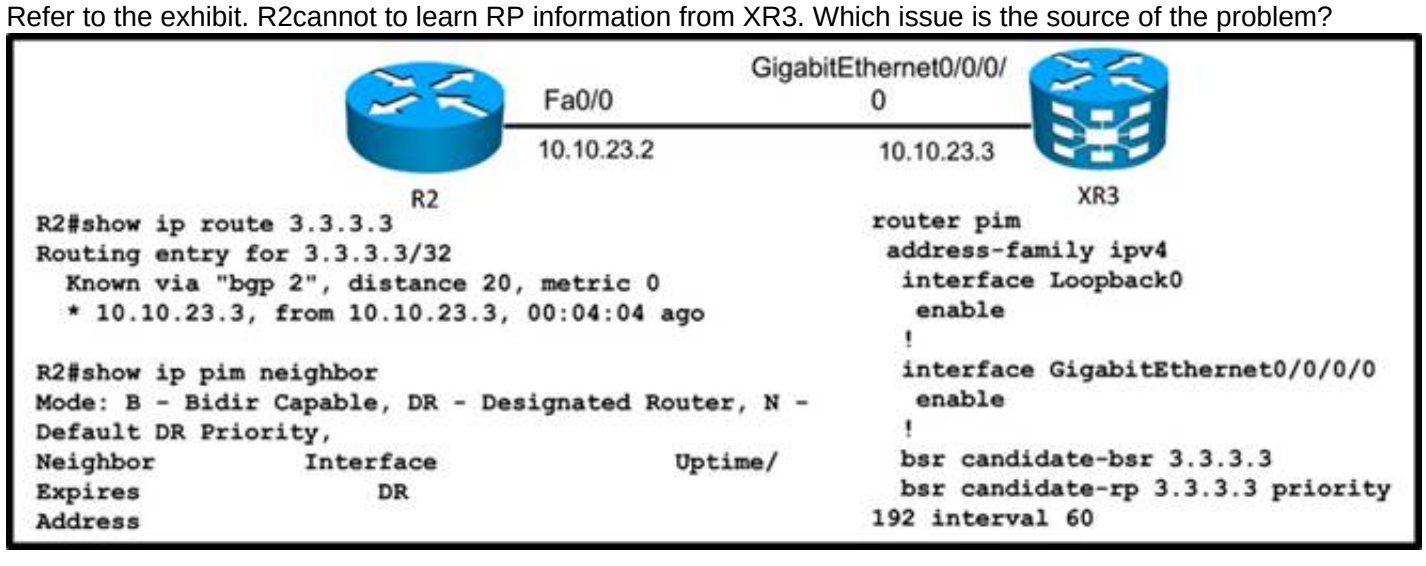
Explanation: Server Configuration
In Global Configuration Mode ipv6 unciast-routing
ipv6 dhcp pool <pool name>
address prefix <specify address prefix> lifetime <infinite> <infinite> dns-server <specify the dns server address>
domain-name <specify the domain name> exit
In Interface Configuration Mode
ipv6 address <specify IPv6 Address>
ipv6 dhcp server <server name>rapid-commit Client Configuration
In Global Configuration Mode enable
configure terminal ipv6 unicast-routing
In Interface Configuration Mode ipv6 address dhcp rapid commit ipv6 enable
exit

NEW QUESTION 156
Which two methods represent IPv6 tunneling implementations? (Choose two.)

A. IPv6 over GRE tunneling
B. manually configured tunnels
C. automatic tunnels
D. 6to4 tunneling
E. IPv6 over an IPv4 tunnel over MPLS

Answer: BC

NEW QUESTION 159
Refer to the exhibit. R2cannot to learn RP information from XR3. Which issue is the source of the problem?



A. XR3 is not the DR.
B. Multicast routing is not enabled on the XR3 Giga0/0/0/0 interface.
C. R2 is learning the RP address via non-IGP routing protocol.
D. Multicast routing is not enabled on the XR3 Loopback0 interface.
E. BGP IPv4 MDT address family is not enabled on XR3.

Answer: D

NEW QUESTION 164
In which three cases is a dual-stack IPv6/IPv4 router required? (Choose three.)

A. tunnel endpoint routers in the case of IPv6 over GRE
B. transit routers in case of an IPv6 over GRE implementation
C. 6to4 implementation border routers
D. 6to4 implementation border and neighboring routers
E. PE routers in case of an IPv6 over IPv4 tunnel over MPLS implementation
F. PE and P routers in case of an IPv6 over IPv4 tunnel over MPLS implementation

Answer: ACE

NEW QUESTION 169
A network engineer of an ISP using Cisco IOS XR routers wants to limit the number of prefixes that BGP peers can accept. To accomplish this task, the command maximum- prefix 1000 is used. Which two results of this configuration are expected? (Choose two.)

A. A warning message displays by default when 750 prefixes are received.
B. A warning message displays by default when 850 prefixes are received.
C. A BGP peer resets when it receives 1001 prefixes.
D. A BGP peer resets when it receives 1000 prefixes.
E. A BGP peer ceases when it receives 1001 prefixes.
F. A BGP peer ceases when it receives 1000 prefixes.

G. The BGP peer tries to reestablish the session after one minute.

Answer: AE

NEW QUESTION 174
Refer to the exhibit.

```
interface loopback 0
 ipv4 address 10.0.0.1/24
 no shutdown
!
interface loopback 1
 ipv4 address 10.2.0.1/24
 no shutdown
!
ipv4 access-list acl1
 10 permit 224.11.11.11 0.0.0.0 any
!
ipv4 access-list acl2
 10 permit 224.99.99.99 0.0.0.0 any
!
multicast-routing
 interface all enable
!
router pim
 auto-rp mapping-agent loopback 0 scope 15 interval 60
 auto-rp candidate-rp loopback 0 scope 15 group-list acl1 interval 60 bidir
 auto-rp candidate-rp loopback 1 scope 15 group-list acl2 interval 60
!
end
```

Which three statements are correct regarding the Cisco IOS-XR configuration? (Choose three.)

A. This router, acting as the RP mapping agent, will send RP announcement messages to the 224.0.1.40 group
B. This router, acting as the RP mapping agent, will send RP discovery messages to the224.0.1.39 group
C. This router is the RP mapping agent only for the 224.11.11.11 and 224.99.99.99 multicast groups
D. This router is a candidate PIM-SM RP for the 224.99.99.99 multicast group
E. This router is a candidate PIM-BIDIR RP for the 224.11.11.11 multicast group
F. IGMPv3 is enabled on all interfaces
G. Other routers will recognize this router as the RP for all multicast groups with this router loopback 0 IP address

Answer: DEF

NEW QUESTION 179
Which two options are thecommon methods for implementing Site of Origin on Cisco IOS XE routers for loop avoidance in multihome BGP customers? (Choose two.)

A. Configure the route-map in command on the CE BGP neighbor.
B. Configure Site of Origin directly on the CE BGP neighbor command.
C. Configure site-map on VRF interface and redistribution of iBGP.
D. Configure site-map on VRF interface and network command.
E. Configure the route-map out command on the P router.

Answer: AB

NEW QUESTION 180
On Cisco IOS-XR, which BGP configuration group allows you to define address-family independent commands and address-family dependent commands for each address family?

A. neighbor-group
B. session-group
C. af-group
D. peer-group

Answer: A

Explanation: •Commands relating to a peer group found in Cisco IOS Release 12.2 have been removed from Cisco IOS XR software. Instead, the af-group, session-group, and neighbor-group configuration commands are added to support the neighbor in Cisco IOS XR software:
–The af-group command is used to group address family-specific neighbor commands within an IPv4 or IPv6 address family. Neighbors that have the same address family configuration are able to use the address family group name for their address family- specific configuration. A neighbor inherits the configuration from an address family group by way of the use command. If a neighbor is configured to use an address family group, the neighbor will (by default) inherit the entire configuration from the address family group. However, a neighbor will not inherit all ofthe configuration from the address family group if items are explicitly configured for the neighbor.
–The session-group command allows you to create a session group from which neighbors can inherit address family-independent configuration. A neighbor inherits the configuration from a session group by way of the use command. If a neighbor is configured to use a session group, the neighbor (by default) inherits the session group's entire configuration. A neighbor does not inherit all the configuration from a session group if a configuration is done directly on that neighbor.
–The neighbor-group command helps you apply the same configuration to one or more neighbors. Neighbor groups can include session groups and address family groups. This additional flexibility can create a complete configuration for a neighbor. Once a neighbor group is configured, each neighbor can inherit the configuration through the use command. If a neighbor is configured to use a neighbor group, the neighbor (by default) inherits the neighbor group's entire BGP configuration.
–However, a neighbor will not inherit all of the configuration from the neighbor group if items are explicitly configured for the neighbor. In addition, some part of the

neighbor group's configuration could be hidden if a session group or address family group was also being used

NEW QUESTION 183
Which statement is correct regarding MP-BGP?

A. MP-BGP can indicate whether an advertised prefix (NLRI) is to be used for unicast routing, multicast RPF checks or for both using different SAFIs.
B. MP-BGP uses a single BGP table to maintain all the unicast prefixes for unicast forwarding and all the unicast prefixes for RPF checks.
C. MP-BGP can be used to propagate multicast state information, which eliminates the need to use PIM for building the multicast distribution trees.
D. MP-BGP enables BGP to carry IP multicast routes used by MSDP to build the multicast distribution trees.

Answer: A

Explanation: Protocol Independent Multicast
Protocol Independent Multicast (PIM) is a routing protocol designed to send and receive multicast routing updates. Proper operation of multicast depends on knowing the unicast paths towards a source or an RP. PIM relies on unicast routing protocols to derive this reverse-path forwarding (RPF) information. As the name PIM implies, it functions independently of the unicast protocols being used. PIM relies on the Routing Information Base (RIB) for RPF information. If the multicast subsequent address family identifier (SAFI) is configured for Border Gateway Protocol (BGP), or if multicast intact is configured, a separate multicast unicast RIB is created and populated with the BGP multicast SAFI routes, the intact information, and any IGP information in the unicast RIB. Otherwise, PIM gets information directly from the unicast SAFI RIB. Both multicast unicast and unicast databases are outside of the scope of PIM.
The Cisco IOS XR implementation of PIM is based on RFC 4601 Protocol Independent Multicast - Sparse
Mode (PIM-SM): Protocol Specification. For more information, see RFC 4601 and the Protocol Independent Multicast (PIM): Motivation and Architecture Internet Engineering Task Force (IETF) Internet draft

NEW QUESTION 188
Refer to the Cisco IOS-XR BGP configuration exhibit.

```
!
route-policy passall
permit
end-policy
!
router bgp 65123
af-group abc address-family ipv4 unicast
route-policy passall in
route-policy passall out
!
neighbor-group efg
password C!sc0!3o
ttl-security
update-source Loopback0
maximum-prefix 10
address-family ipv4 unicast
use af-group abc
!
neighbor 209.165.201.130
remote-as 65234
use neighbor-group efg
!
```

Identify two configuration errors. (Choose two.)

A. The neighbor-group efg is missing the ebgp-multihop 2 configuration
B. The ttl-security configuration command is missing the option to set the number of hops
C. The passall route policy is wrong
D. The route-policy passall in and route-policy passall out commands should be configured under the neighbor-group efg instead of the af-group abc
E. The maximum-prefix 10 configuration should be configured under the af-group abc instead of the neighbor-group efg

Answer: CE

Explanation: http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a00801 0a28a.shtml

NEW QUESTION 191
What is one of the configuration errors within an AS that can stop a Cisco IOS-XR router from announcing certain prefixes to its EBGP peers?

A. Some prefixes were mistagged with the no-export BGP community
B. Some prefixes were set with an MED of 0
C. The outbound BGP route policy only has set actions defined without any pass actions defined
D. The inbound BGP route policy only has set actions defined without any pass actions defined

Answer: A

NEW QUESTION 196
Which command set should be used for a 6to4 tunnel in a Cisco IOS XE router, considering the border interface with IPv4 address of 209.165.201.2?

A. interface Tunnel2002 ipv6 enableipv6 address 2002:D1A5:C902::1/128 tunnel source Ethernet0/0tunnel mode ipv6ip 6to4
B. interface Tunnel2002 ipv6 enableipv6 address 2002:D1A5:D902::1/128 tunnel source Ethernet0/0tunnel mode ipv6ip 6to4
C. interface Tunnel2002 ipv6 enableipv6 address 2002:D1A5:D902::1/128 tunnel source Ethernet0/0tunnel mode ipv6ip
D. interface Tunnel2002 ipv6 enableipv6 address 2002:D1A5:C902::1/128 tunnel source Ethernet0/0tunnel mode ipv6ip auto-tunnel
E. interface Tunnel2002ipv6 enableipv6 address 2002:D1A5:D902::1/128 tunnel source Ethernet0/0tunnel mode ipv6ip auto-tunnel

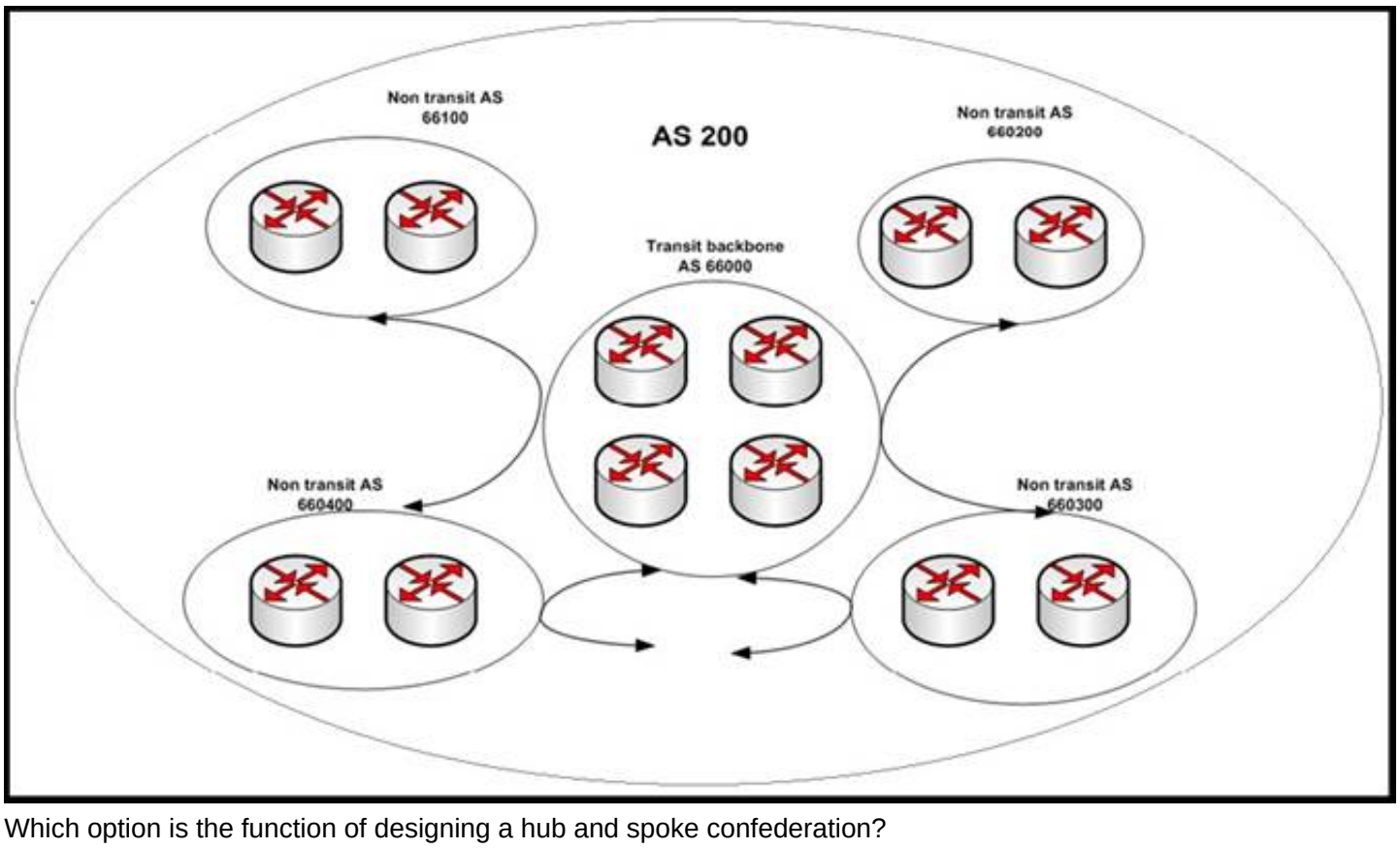
Answer: B

NEW QUESTION 197
Which two options areadvantages of an IPv6 dual-stack implementation in an enterprise environment? (Choose two.)

A. simplifies the route redistribution policies complexity
B. requires IPv6-to-IPv4 translation on the uplinks to the service providers
C. provides built-in support for Kerberos authentication
D. does not have to worry about NAT traversal
E. supports multicast properly

Answer: DE

NEW QUESTION 200
Refer to the exhibit.



Which option is the function of designing a hub and spoke confederation?

A. allows transit backbone area 66000 to be a blackhole for non-transit ASs
B. reduces the iBGP mesh, iBGP mesh will be in sub non-transit ASs
C. increases eBGP sessions between the confederation sub ASs
D. allows transit backbone area and non-transit ASs to run the same IGP

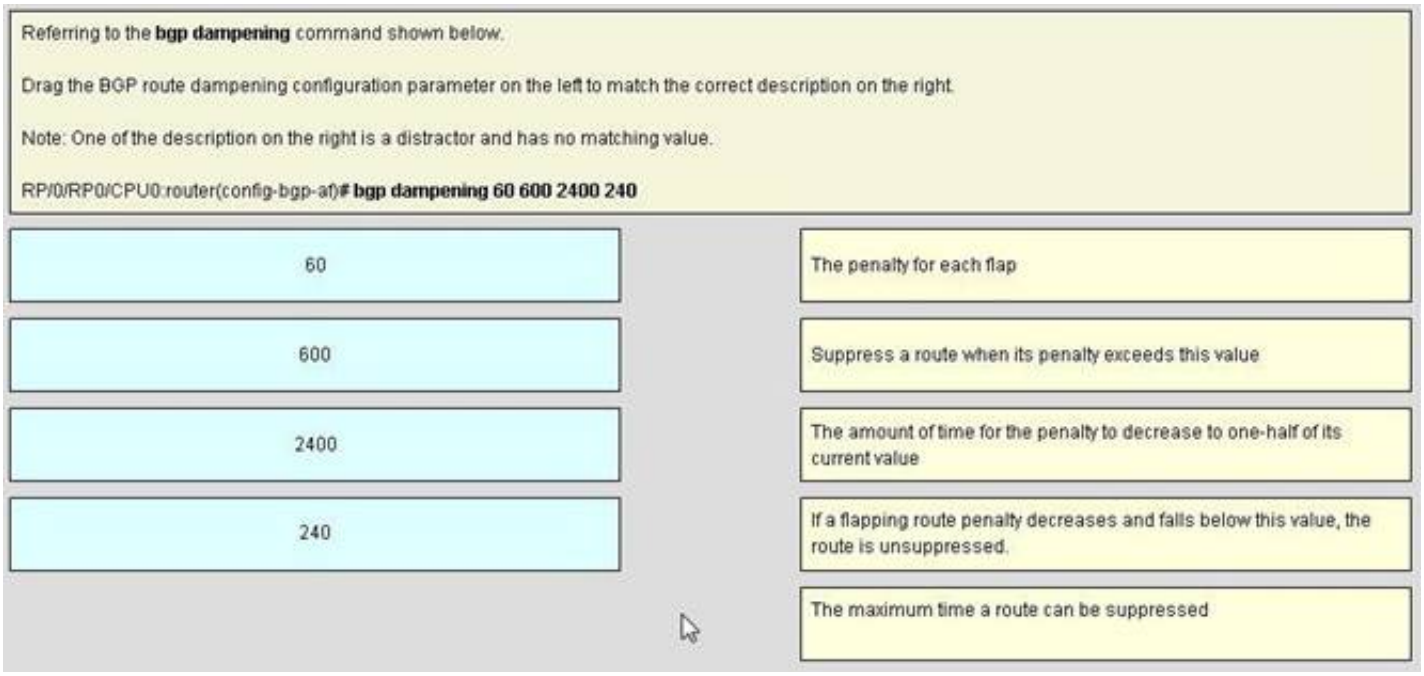
Answer: B

NEW QUESTION 203
When verifying multicast configurations and operations on Cisco IOS-XR routers, which two statements regarding show commands are correct? (Choose two.)

A. Use the show route ipv4 multicast command to display the incoming and outgoing interface lists for each of the joined multicast groups
B. Use the show pim rpf command to display the RPF information for the RP or for the multicast source
C. Use the show mrib route command to display the (*, G) and (S, G) states information on the router
D. Use the show mrib route command to display the configured static multicast routes

Answer: BC

NEW QUESTION 205
DRAG DROP



Answer:

Explanation: The amount of time for the penalty to decrease to one-half of its current value - 60 Suppress a route when its penalty exceeds this value - 2400
If a flapping route penalty decreases and falls below this value , the route is unsuppressed - 600
The maximum time a route can be suppressed – 240

bgp dampening

To enable Border Gateway Protocol (BGP) route dampening or change various BGP route dampening factors, use the **bgp dampening** command in address family configuration mode. To disable route dampening and reset default values, use the **no** form of this command.

bgp dampening [*half-life* [*reuse suppress max-suppress-time*] | **route-policy** *route-policy-name*]

no bgp dampening

Syntax Description

half-life	(Optional) Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). Penalty reduction happens every 5 seconds. Range of the half-life period is from 1 to 45 minutes.
reuse	(Optional) Value for route reuse if the flapping route penalty decreases and falls below the reuse value. When this happens, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. Range is 1 to 20000.
suppress	(Optional) Maximum penalty value. Suppress a route when its penalty exceeds the value specified. When this happens, the route is suppressed. Range is 1 to 20000.
max-suppress-time	(Optional) Maximum time (in minutes) a route can be suppressed. Range is 1 to 20000. If the *half-life* value is allowed to default, the maximum suppress time defaults to 60 minutes.
route-policy *route-policy-name*	(Optional) Specifies the route policy to use to set dampening parameters.

SO bgp dampening 60 600 2400 240 is:
60 half life
600 reuse
2400 suppress
240 max-suppress-time

NEW QUESTION 209
What are three BGP configuration characteristics of a multihomed customer that is connected to multiple service providers? (Choose three.)

A. The multihomed customer can use local preference to influence the return traffic from the service providers
B. The multihomed customer announces its assigned IP address space to its service providers through BGP
C. The multihomed customer has to decide whether to perform load sharing or use a primary/backup implementation
D. The multihomed customer must use private AS number
E. The multihomed customer configures outbound route filters to prevent itself from becoming a transit AS

Answer: BCE

NEW QUESTION 211
Refer to the exhibit for the outputs from an ASR9K router.

```
RP/0/RSP0/CPU0:PE1#show route ipv6
Wed Oct 26 20:57:46.433 UTC

Codes: C - connected, S - static, R - RIP, 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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local, G  - DAGR
       A - access/subscriber, (!) - FRR Backup path

Gateway of last resort is not set

L    2001:db8:10:1:1::1/128 is directly connected,
     09:20:18, Loopback0
i L2 2001:db8:10:1:10::1/128
     [105/20] via fe80::eab7:48ff:fe2c:a180, 07:59:22, GigabitEthernet0/0/0/0
C    2001:db8:192:168:101::/80 is directly connected,
     1d05h, GigabitEthernet0/0/0/0
L    2001:db8:192:168:101::10/128 is directly connected,
     1d05h, GigabitEthernet0/0/0/0

RP/0/RSP0/CPU0:PE1#ping 2001:db8:10:1:10::1/128
Wed Oct 26 20:58:01.969 UTC
%Bad hostname or protocol not running
```

Why did the ping fail?

A. The ping command is missing the ipv6 option: ping ipv6 2001:db8:10:1:10::1/128
B. There is a problem with the IS-IS configurations
C. The fe80::eab7:48ff:fe2c:a180 next-hop is not reachable
D. The prefix length should be removed from the IPv6 address in the ping command: ping ipv6 2001:db8:10:1:10::1
E. IPv6 is not enabled on the Gi0/0/0/0 interface
F. The IPv6 neighbor discovery protocol is not enabled on the Gi0/0/0/0 interface

Answer: D

NEW QUESTION 212
Which of the following is a feature added in IGMPv3?

A. Support for source filtering
B. Support for Host Membership Report and a Leave Group message
C. Uses a new variation of the Host Membership Query called the Group-Specific Host Membership Query
D. Uses an election process to determine the querying router on the LAN
E. Uses an election process to determine the designated router on the LAN
F. IPv6 support

Answer: A

NEW QUESTION 214
Which optionshowsthe equivalent multicast MAC address mapping of multicast address 239.210.101.190?

A. 01:00:5e:52:65:be
B. 01:00:5d:52:65:be
C. 01:00:5f:52:65:be
D. 01:00:5c:52:65:be

Answer: A

NEW QUESTION 215
Which two options are characteristics ofconfiguration templates used by Cisco IOS XRto optimize BGP peering implementations? (Choose two.)

A. Session groups are used to inherit address family-specific configurations.
B. Cisco IOS XR provides by default a session group operating with all the supported address families.
C. Session groups are used to inherit address family-independent configurations.
D. Session groups can be included within a neighbor group.
E. Session groups can include neighbor groups.

Answer: CD

NEW QUESTION 219
What is determined by running the same hash algorithm on all PIMv2 routers?

A. The SPT from the RP to the multicast source
B. The SPT from the last hop router to the multicast source
C. Auto RP election

D. Which BSR to use for a particular multicast group
E. Which RP to use from a set of candidate RPs in the RP set

Answer: E

NEW QUESTION 222
Assume that the R1 router is enabled for PIM-SM and receives a multicast packet sourced from 172.16.1.100, and the R1 router has multicast receivers on the Gi0/1, Gi0/2, Gi0/3 and Gi0/4 interfaces.

R1 routing table:

172.16.1.0/24 via Gi0/1
172.16.2.0/24 via Gi0/2
172.16.3.0/24 via Gi0/3
0.0.0.0/0 via Gi0/4

The multicast packet from the 172.16.1.100 source must arrive on which interface on the R1 router for it to be forwarded out the other interfaces?

A. Gi0/1
B. Gi0/2
C. Gi0/3
D. Gi0/4
E. Gi0/1 or Gi0/2 or Gi0/3 or Gi0/4
F. Gi0/2 or Gi0/3
G. Gi0/1 or Gi0/4

Answer: A

NEW QUESTION 223
Which two statements correctly describe the RPF check when a multicast packet arrives at a router? (Choose two.)

A. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source
B. The router looks up the destination address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the destination
C. If the packet has arrived on the interface leading back to the destination, the RPF check passes and the packet is forwarde
D. If the RPF check fails, the packet is dropped
E. If the packet has arrived on the interface leading back to the source, the RPF check passes and the packet is forwarde
F. If the RPF check fails, the packet is dropped

Answer: AD

Explanation: Reverse Path Forwarding (RPF)
RPF is a fundamental concept in multicast routing that enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will only forward a multicast packet if it is received on the upstream interface.
This RPF check helps to guarantee that the distribution tree will be loop free. RPF Check
When a multicast packet arrives at a router, the router will perform an RPF check on the packet. If the RPF check is successful, the packet will be forwarded. Otherwise it will be dropped.
For traffic flowing down a source tree, the RPF check procedure works as follows:
Step 1. Router looks up the source address in the unicast routing table to determine if it has arrived on the interface that is on the reverse path back to the source.
Step 2. If packet has arrived on the interface leading back to the source, the RPF check is successful and the packet will be forwarded.
Step 3. If the RPF check in 2 fails, the packet is dropped.

NEW QUESTION 227
On Cisco IOS-XR, which BGP process can be distributed into multiple instances?

A. BGP process manager
B. BGP RIB process
C. BGP speaker process
D. BGP scanner process
E. BGP dampening process

Answer: C

Explanation: Cisco IOS XR allows you to control the configuration of the number of distributed speakers and enables you to selectively assign neighbors to specific speakers. On the CRS-1 platform, multiple speaker processes up to 15 may be configured. However, configuring all the different speakers on the primary route processor simply adds to the load on the single RP.
Distributed speaker functionality is useful if Distributed Route Processor (DRP) hardware is available to take advantage of process placement. Later sections in this chapter depict distributed
BGP and placement of BGP process speakers on DRPs on a CRS-1 router.
In addition to the speaker process, BPM starts the bRIB process once BGP is configured. bRIB process is responsible for performing the best-path calculation based on partial best paths received from the speaker processes. The best route is installed into the bRIB and is advertised back to all speakers. The bRIB process is also responsible for installing routes

NEW QUESTION 230
Refer to the Cisco IOS configuration exhibit.

```
interface Gi0/0
 ip multicast boundary 1
!
access-list 1 deny 224.0.1.39
access-list 1 deny 224.0.1.40
```

Which statement is correct?

A. This configuration is typically configured on the boundary routers within a PIM SM domain to filter out malicious candidate-RP-announce and candidate-RP-discovery packets
B. This configuration is typically configured on the RPs within a PIM-SM domain to restrict the candidate-RP-announce packets
C. This configuration is typically configured on the mapping agents within a PIM-SM domain to restrict the candidate-RP-discovery packets
D. This configuration is typically configured on the MSDP peering routers within a PIM-SM domain to filter out malicious MSDP SA packets

Answer: A

NEW QUESTION 231
When implementing Anycast RP, the RPs are also required to establish which kind of peering with each other?

A. BGP
B. Multiprotocol BGP
C. MSDP
D. Bidirectional PIM
E. PIM SSM

Answer: C

Explanation: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/anycast.ht ml
Using Anycast RP is an implementation strategy that provides load sharing and redundancy in Protocol Independent Multicast sparse mode (PIM-SM) networks. Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and the ability to act as hot backup routers for each other. Multicast Source Discovery Protocol (MSDP) is the key protocol that makes Anycast RP possible.

NEW QUESTION 236
When configuring BFD, the multiplier configuration option is used to determine which value?

A. The retry interval
B. The number of BFD packets that can be lost before the BFD peer is declared "down"
C. The minimum interval between packets accepted from the BFD peers
D. The number of BFD echo packets that will be originated by the router
E. The number of routing protocols that will use BFD for fast peer failure detection

Answer: B

NEW QUESTION 241
Refer to the configuration exhibit, taken from a Cisco IOS-XR router.

```
!
router static
address-family ipv4 unicast
192.0.2.1/32 Null0
!
route-policy RTBH
if tag is 666 then
set next-hop 192.0.2.1
endif
end-policy
!
router bgp 65123
address-family ipv4 unicast
redistribute static route-policy RTBH
!
!When attacks are detected from 209.165.201.144/28
!
router static
address-family ipv4 unicast
209.165.201.144/28 null0 tag 666
!
```

Which configuration change is required to properly enable this router as the signaling router for implementing source-based RTBH filtering?

A. Set community (no-export) in the route policy
B. Pass in the route policy
C. Set local-preference 1000 in the route policy
D. The 192.0.2.1/32 static route should be tagged as 666 (tag 666)

Answer: A

NEW QUESTION 243
Whichtwo attributes does BGP select before MED? (Choose two.)

A. local preference
B. weight

C. lowest router ID
D. lowest neighbor IP
E. oldest route

Answer: AB

NEW QUESTION 244
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

642-885 Practice Exam Features:

* 642-885 Questions and Answers Updated Frequently

* 642-885 Practice Questions Verified by Expert Senior Certified Staff

* 642-885 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 642-885 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year