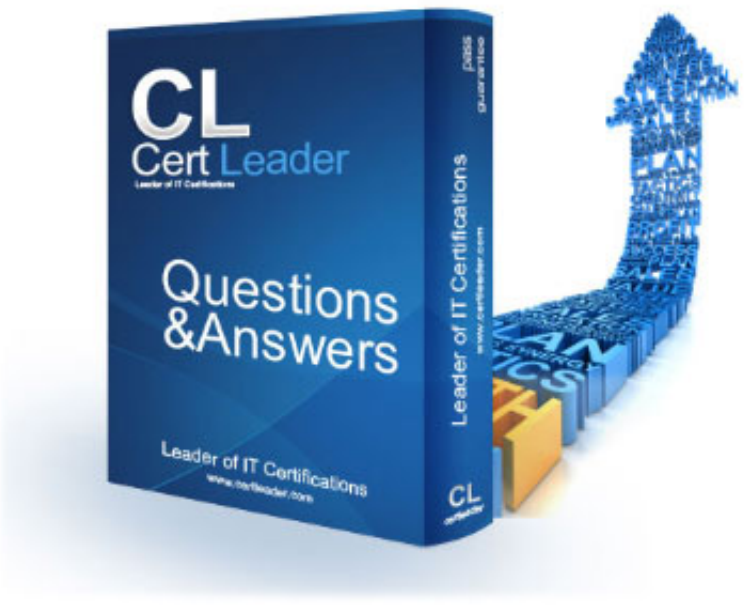
# 642-885 Dumps

# Deploying Cisco Service Provider Advanced Routing (SPADVOUTE)

**https://www.certleader.com/642-885-dumps.html**



**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**
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 5**
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 6**
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 7**
A junior network engineer has just configured a new IBGP peering between two Cisco ASR9K PE routers in the network using the loopback interface of the router, but the IBGP neighborship is not able to be established. Which two verification steps will be helpful in troubleshooting this problem? (Choose two.)

A. Verify that the network command under router BGP is configured correct on each router for announcing the router's loopback interface in BGP
B. Verify that the ibgp-multihop command under the BGP neighbor is configured correctly on each router
C. Verify that the loopback interfaces are reachable over the IGP
D. Verify that the update-source loopback command under the BGP neighbor is configured correctly on each router
E. Verify that the ttl-security command under the BGP neighbor is configured correctly on each router to enable the router to send the BGP packets using a proper TTL value
F. Verify that the UDP port 179 traffic is not being blocked by an ACL or firewall between the two IBGP peers

**Answer:** CD

**NEW QUESTION 8**
After configuring the tunnel interface as shown in the exhibit, no IPv6 traffic is passed over the IPv4 network.

```
interface Tunnel0
ipv6 address 2001:db8:3::1/64
tunnel source GigabitEthernet0/0
tunnel destination 209.165.201.6
tunnel mode ipv6ip
```

Which additional configuration is required to pass the IPv6 traffic over the IPv4 network?

A. Configure an IPv4 address on the tunnel0 interface
B. Configure an IPv6 static route to send the required IPv6 traffic over the tunnel0 interface
C. The tunnel destination should be pointing to an IPv6 address instead of an IPv4 address
D. The tunnel0 interface IPv6 address must use the 2002::/16 prefix

**Answer:** B

**NEW QUESTION 9**
A CRS router that runs Cisco IOS XR has dual routing processors installed. Which solution should be implemented to prevent OSPF adjacency flapping if the primary routing processor fails?

A. NSR
B. OSPF Fast Timers
C. OSPF RE Sync
D. router msdp
E. NSF

**Answer:** A

**NEW QUESTION 10**
Which technology is categorized as multicast ASM and multicast SSM?

A. IP telephony
B. video conferencing

C. IPTV
D. live streaming

**Answer:** D

**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 11**
Which IPv6 mechanism occurs between a provider edge router and the customer premises equipment router to allow an ISP to automate the process of assigning a block of IPv6 addresses to a customer for use within the customer network?

A. Router Advertisement
B. DHCPv6 Prefix Delegation
C. DHCPv6 Lite
D. Stateful DHCPv6

**Answer:** B

**Explanation:** http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a0080b 8a116.shtml

**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 17**
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 21**
An engineer is enabling multicast routing across an entire core infrastructure. Which two commands enable multicast routing on Cisco IOS XE instances? (Choose two.)

A. ip multicast-routing
B. ip multicast-routing vrf global
C. interface type slot/path_id ip pim sparse-mode
D. interface type slot/path_id ip cgmp
E. interface type slot/path_id ip pim dense-mode
F. ip mroute-cache

**Answer:** AC

**NEW QUESTION 24**
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

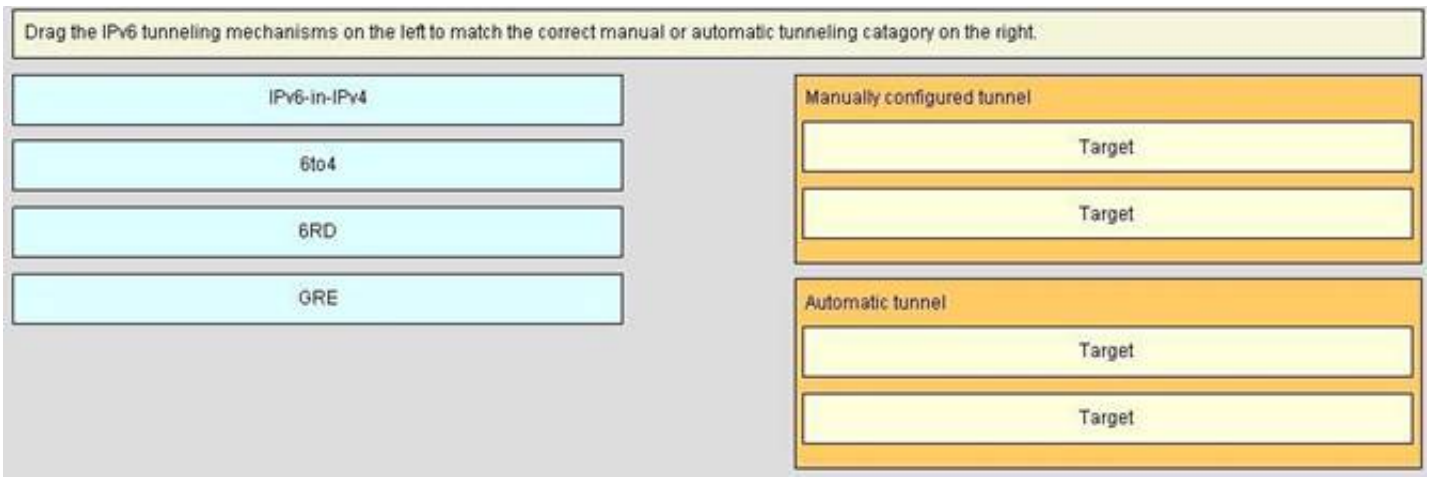
**Answer:** B

**NEW QUESTION 28**
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 33**
DRAG DROP




**Answer:**

**Explanation:** IPv6-in-IPv4 and GRE are manual and 6RDand 6to4

## ipv6-prefix (6rd)

To convert the ipv4 address into ipv6 address to be used in the 6rd domain, use the **ipv6-prefix** command. To remove the ipv6 prefix assigned for the application, use the **no** form of this command.

**ipv6 prefix X:X::X/length** *IPV6 subnet mask*
**no ipv6-prefix X:X::X/length** *IPV6 subnet mask*

| Syntax Description | | |
|---|---|---|
| | **ipv6-prefix** | Specifies the IPv6 prefix used to translate IPv4 address to IPv6 address. |
| | *X:X::X/length* | Specifies the IPv6 address. |

**Command Default** None

**Command Modes** TUNNEL-6RD
CGN-NAT64

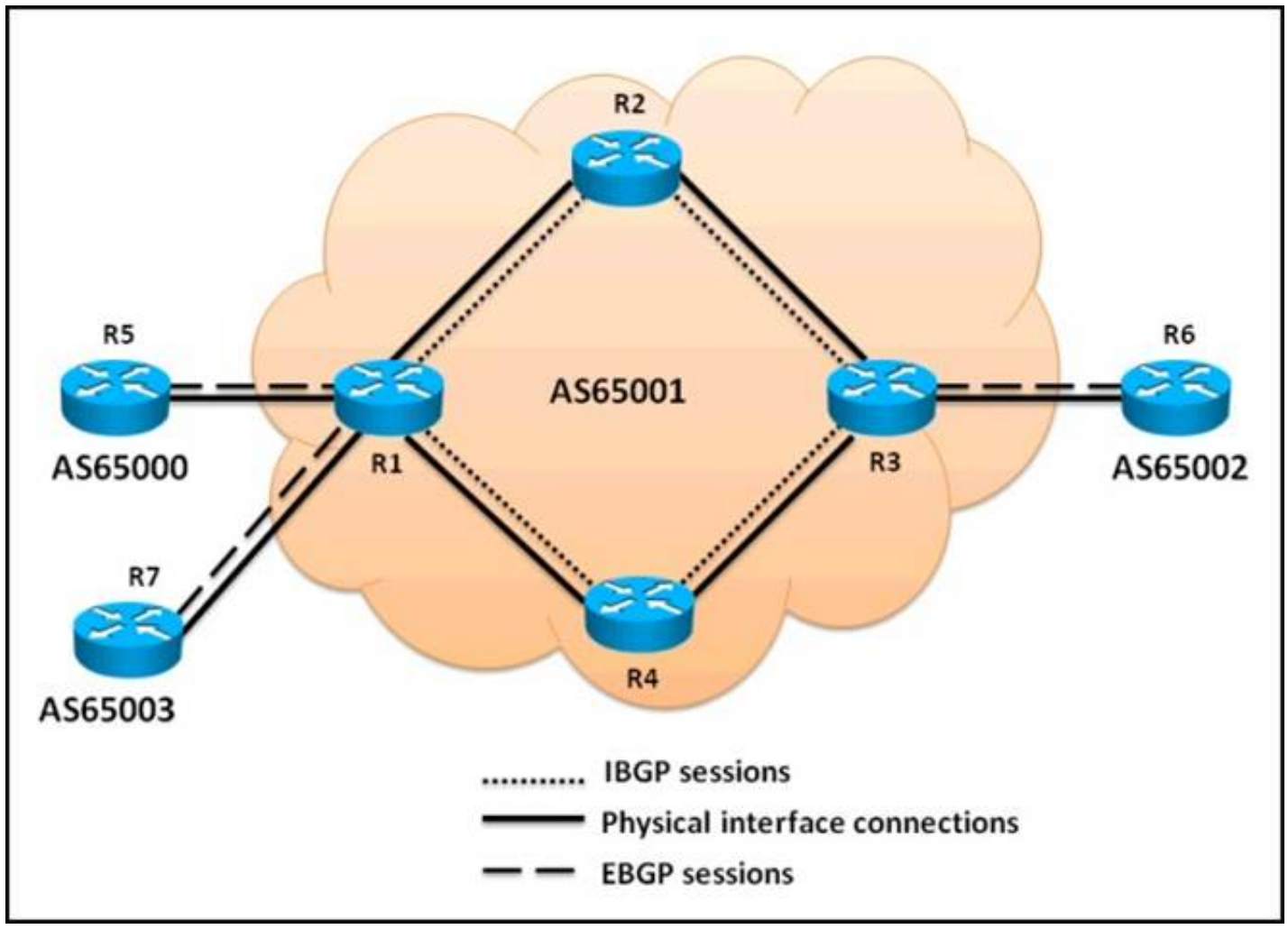
Download this chapter Implementing Tunnels Download the complete book
Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S (PDF - 1 MB) Feedback
Contents Implementing Tunnels
Finding Feature Information Restrictions for Implementing Tunnels
Information About Implementing Tunnels Tunneling Versus Encapsulation
Tunnel ToS
Generic Routing Encapsulation
GRE Tunnel IP Source and Destination VRF Membership GRE IPv4 Tunnel Support for IPv6 Traffic
EoMPLS over GRE
Provider Edge to Provider Edge Generic Routing EncapsulationTunnels Provider to Provider Generic Routing Encapsulation Tunnels
Provider Edge to Provider Generic Routing Encapsulation Tunnels Features Specific to Generic Routing Encapsulation
Features Specific to Ethernet over MPLS
Features Specific to Multiprotocol Label Switching Virtual Private Network Overlay Tunnels for IPv6
IPv6 Manually Configured Tunnels Automatic 6to4 Tunnels
ISATAP Tunnels Path MTU Discovery
QoS Options for Tunnels How to Implement Tunnels Determining the Tunnel Type
Configuring an IPv4 GRE Tunnel GRE Tunnel Keepalive
What to Do Next
Configuring GRE on IPv6 Tunnels What to Do Next
Configuring GRE Tunnel IP Source and Destination VRF Membership What to Do Next
Manually Configuring IPv6 Tunnels What to Do Next
Configuring 6to4 Tunnels What to Do Next
Configuring ISATAP Tunnels
Verifying Tunnel Configuration and Operation Configuration Examples for Implementing Tunnels Example: Configuring a GRE IPv4 Tunnel Example: Configuring

GRE on IPv6 Tunnels
Example: Configuring GRE Tunnel IP Source and Destination VRF Membership Example: Configuring EoMPLS over GRE
Example: Manually Configuring IPv6 Tunnels Example: Configuring 6to4 Tunnels Example: Configuring ISATAP Tunnels
Configuring QoS Options on Tunnel Interfaces Examples Policing Example
Additional References
Feature Information for Implementing Tunnels Implementing Tunnels
Last Updated: September 17, 2012
This module describes the various types of tunneling techniques. Configuration details and examples are provided for the tunnel types that use physical or virtual interfaces. Many tunneling techniques are implemented using technology-specific commands, and links are provided to the appropriate technology modules.
Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol.
Tunnels are implemented as virtual interfaces to provide a simple interface for configuration purposes.
The tunnel interface is not tied to specific "passenger" or "transport" protocols, but rather is an architecture to provide the services necessary to implement any standard point-to-point encapsulation scheme. Note
Cisco ASR 1000 Series Aggregation Services Routers support VPN routing and forwarding (VRF)-aware generic routing encapsulation (GRE) tunnel keepalive features. Finding Feature Information
Restrictions for Implementing Tunnels Information About Implementing Tunnels How to Implement Tunnels
Configuration Examples for Implementing Tunnels Additional References
Feature Information for Implementing Tunnels Finding Feature Information
Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for Implementing Tunnels
It is important to allow the tunnel protocol to pass through a firewall and access control list (ACL) check.
Multiple point-to-point tunnels can saturate the physical link with routing information if the bandwidth is not configured correctly on a tunnel interface.
A tunnel looks like a single hop link, and routing protocols may prefer a tunnel over a multihop physical path.
The tunnel, despite looking like a single hop link, may traverse a slower path than a multihop link. A tunnel is as robust and fast, or as unreliable and slow, as the links that it actually traverses. Routing protocols that make their decisions based only on hop counts will often prefer a tunnel over a set of physical links. A tunnel might appear to be a one-hop, point-to-point link and have the lowest-cost path, but the tunnel may actually cost more in terms of latency when compared to an alternative physical topology. For example, in the topology shown in the figure below, packets from Host 1 will appear to travel across networks w, t, and z to get to Host 2 instead of taking the path w, x, y, and z because the tunnel hop count appears shorter. In fact, the packets going through the tunnel will still be traveling across Router A, B, and C, but they must also travel to Router D before coming back to Router C. Figure 1
Tunnel Precautions: Hop Counts
A tunnel may have a recursive routing problem if routing is not configured accurately. The best path to a tunnel destination is via the tunnel itself; therefore recursive routing causes the tunnel interface to flap. To avoid recursive routing problems, keep the control-plane routing separate from the tunnel routing by using the following methods:
Use a different autonomous system number or tag. Use a different routing protocol.
Ensure that static routes are used to override the first hop (watch for routing loops). The following error is displayed when there is recursive routing to a tunnel destination:
%TUN-RECURDOWN Interface Tunnel 0 temporarily disabled due to recursive routing Information About Implementing Tunnels Tunneling Versus Encapsulation
Tunnel ToS
Generic Routing Encapsulation EoMPLS over GRE
Overlay Tunnels for IPv6
IPv6 Manually Configured Tunnels Automatic 6to4 Tunnels
ISATAP Tunnels Path MTU Discovery
QoS Options for Tunnels
Tunneling Versus Encapsulation
To understand how tunnels work, you must be able to distinguish between concepts of encapsulation and tunneling. Encapsulation is the process of adding headers to data at each layer of a particular protocol stack.
The Open Systems Interconnection (OSI) reference model describes the functions of a network. To send a data packet from one host (for example, a PC) to another on a network, encapsulation is used to add a header in front of the data packet at each layer of the protocol stack in descending order. The header must contain a data field that indicates the type of data encapsulated at the layer immediately above the current layer. As the packet ascends the protocol stack on the receiving side of the network, each encapsulation header is removed in reverse order.
Tunneling encapsulates data packets from one protocol within a different protocol and transports the packets on a foreign network. Unlike encapsulation, tunneling allows a lower-layer protocol and a same-layer protocol to be carried through the tunnel. A tunnel interface is a virtual (or logical) interface. Tunneling consists of three main components: Passenger protocol--The protocol that you are encapsulating. For example, IPv4 and IPv6 protocols. Carrier protocol--The protocol that encapsulates. For example, generic routing encapsulation (GRE) and Multiprotocol Label Switching (MPLS).
Transport protocol--The protocol that carries the encapsulated protocol. The main transport protocol is IP.
The figure below illustrates IP tunneling terminology and concepts: Figure 2
IP Tunneling Terminology and Concepts Tunnel ToS
Tunnel type of service (ToS) allows you to tunnel network traffic and group all packets in the same ToS byte value. The ToS byte values and Time-to-Live (TTL) hop-count value can be set in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. Tunnel ToS feature is supported for Cisco Express Forwarding (formerly known as CEF), fast switching, and process switching.
The ToS and TTL byte values are defined in RFC 791. RFC 2474, and RFC 2780 obsolete the use of the ToS byte as defined in RFC 791. RFC 791 specifies that bits 6 and 7 of the ToS byte (the first two least significant bits) are reserved for future use and should be set to
1. For Cisco IOS XE Release 2.1, the Tunnel ToS feature does not conform to this standard and allows you touse the whole ToS byte value, including bits 6 and 7, and to decide to which RFC standard the ToS byte of your packets should conform.
Generic Routing Encapsulation
GRE is defined in RFC 2784. GRE is a carrier protocol that can be used with many different underlying transport protocols and can carry many passenger protocols. RFC
2784 also covers the use of GRE with IPv4 as the transport protocol and the passenger protocol. Cisco software supports GRE as the carrier protocol with many combinations of passenger and transport protocols.
GRE tunnels are described in the following sections: GRE Tunnel IP Source and Destination VRF Membership GRE IPv4 Tunnel Support for IPv6 Traffic
GRE Tunnel IP Source and Destination VRF Membership
The GRE Tunnel IP Source and Destination VRF Membership feature allows you to configure the source and destination of a tunnel to belong to any VPN routing and forwarding (VRFs) tables. A VRF table stores routing data for each VPN. The VRF table defines the VPN membership of a customer site that is attached to the network access server (NAS). Each VRF table comprises an IP routing table, a derived Cisco Express Forwarding table, and guidelines and routing protocol

parameters that control the information that is included in the routing table.
Prior to Cisco IOS XE Release 2.2, GRE IP tunnels required the IP tunnel destination to be in the global routing table. The implementation of this feature allows you to configure a tunnel source and destination to belong to any VRF. As with existing GRE tunnels, the tunnel becomes disabled if no route to the tunnel destination is defined.
GRE IPv4 Tunnel Support for IPv6 Traffic
IPv6 traffic can be carried over IPv4 GRE tunnels by using the standard GRE tunneling technique to provide the services necessary to implement a standard point-to-point encapsulation scheme. GRE tunnels are links between two points, with a separate tunnel for each point. GRE tunnels are not tied to a specific passenger or transport protocol, but in case of IPv6 traffic, IPv6 is the passenger protocol, GRE is the carrier protocol, and IPv4 is the transport protocol.
The primary use of GRE tunnels is to provide a stable connection and secure communication between two edge devices or between an edge device and an end system. The edge device and the end system must have a dual-stack implementation.
GRE has a protocol field that identifies the passenger protocol. GRE tunnels allow intermediate system to intermediate system (IS-IS) or IPv6 to be specified as the passenger protocol, therebyallowing both IS-IS and IPv6 traffic to run over the same tunnel. If GRE does not have a protocol field, it becomes impossible to distinguish whether the tunnel is carrying IS-IS or IPv6 packets.
EoMPLS over GRE
Ethernet over MPLS (EoMPLS) is a tunneling mechanism that allows you to tunnel Layer 2 traffic through a Layer 3 MPLS network. EoMPLS is also known as Layer 2 tunneling.
EoMPLS effectively facilitates Layer 2 extension over long distances. EoMPLS over GRE helps you to create the GRE tunnel as hardware-based switched, and encapsulates EoMPLS frames within the GRE tunnel. The GRE connection is established between the two core routers, and then the MPLS label switched path (LSP) is tunneled over.
GRE encapsulation is used to define a packet that has header information added to it prior to being forwarded.
De-encapsulation is the process of removing the additional header information when the packet reaches the destination tunnel endpoint.
When a packet is forwarded through a GRE tunnel, two new headers are added to the front of the packet and hence the context of the new payload changes. After encapsulation, what was originally the data payload and separate IP header are now known as the GRE payload. A GRE header is added to the packet to provide information on the protocol type and the recalculated checksum. A new IP header is also added to the front of the GRE header. This IP header contains the destination IP address of the tunnel. The GRE header is added to packets such as IP, Layer 2 VPN, and Layer 3 VPN before the header enters into the tunnel. All routers along the path that receives the encapsulated packet use the new IP header to determine how the packet can reach the tunnel endpoint.
In IP forwarding, on reaching the tunnel destination endpoint, the new IP header and the GRE header are removed from the packet and the original IP header is used to forward the packet to the final destination.
The EoMPLS over GRE feature removes the new IP header and GRE header from the packet at the tunnel destination, and the MPLS label is used to forward the packet to the appropriate Layer 2 attachment circuit or Layer 3 VRF.
The scenarios in the following sections describe the L2VPN and L3VPN over GRE deployment on provider edge (PE) or provider (P) routers:
Provider Edge to Provider Edge Generic Routing EncapsulationTunnels Provider to Provider Generic Routing Encapsulation Tunnels
Provider Edge to Provider Generic Routing Encapsulation Tunnels Features Specific to Generic Routing Encapsulation
Features Specific to Ethernet over MPLS
Features Specific to Multiprotocol Label Switching Virtual Private Network Provider Edge to Provider Edge Generic Routing EncapsulationTunnels
In the Provider Edge to Provider Edge (PE) GRE tunnels scenario, a customer does not transition any part of the core to MPLS but prefers to offer EoMPLS and basic MPLS VPN services. Therefore, GRE tunneling of MPLS traffic is done between PEs.
Provider to Provider Generic Routing Encapsulation Tunnels
In the Provider to Provider (P) GRE tunnels scenario, Multiprotocol Label Switching (MPLS) is enabled between Provider Edge (PE ) and P routers but the network core can either have non-MPLS aware routers or IP encryption boxes. In this scenario, GRE tunneling of the MPLS labeled packets is done between P routers.
Provider Edge to Provider Generic Routing Encapsulation Tunnels in a Provider Edge to Provider GRE tunnels scenario, a network has MPLS-aware P to P nodes. GRE tunneling is done between a PE to P non-MPLS network segment. Features Specific to Generic Routing Encapsulation You should understand the following configurations and information for a deployment scenario:
Tunnel endpoints can be loopbacks or physical interfaces.
Configurable tunnel keepalive timer parameters per endpoint and a syslog message must be generated when the keepalive timer expires.
Bidirectional forwarding detection (BFD) is supported for tunnel failures and for the Interior Gateway Protocol (IGP) that use tunnels.
IGP load sharing across a GRE tunnel is supported. IGP redundancy across a GRE tunnel is supported. Fragmentation across a GRE tunnel is supported. Ability to pass jumbo frames is supported.
All IGP control plane traffic is supported.
IP ToS preservation across tunnels is supported.
A tunnel should be independent of the endpoint physical interface type; for example, ATM, Gigabit, Packet over SONET (POS), and TenGigabit.
Up to 100 GRE tunnels are supported. Features Specific to Ethernet over MPLS
Any Transport over MPLS (AToM) sequencing. IGP load sharing and redundancy.
Port mode Ethernet over MPLS (EoMPLS). Pseudowire redundancy.
Support for up to to 200 EoMPLS virtual circuits (VCs).
Tunnel selection and the ability to map a specific pseudowire to a GRE tunnel. VLAN mode EoMPLS.
Features Specific to Multiprotocol Label Switching Virtual Private Network Support for the PE role with IPv4 VRF.
Support for all PE to customer edge (CE) protocols.
Load sharing through multiple tunnels and also equal cost IGP paths with a single tunnel. Support for redundancy through unequal cost IGP paths with a single tunnel.
Support for the IP precedence value being copied onto the expression (EXP) bits field of the Multiprotocol Label Switching (MPLS) label and then onto the precedence bits on the outer IPv4 ToS field of the generic routing encapsulation (GRE) packet.
See the section, "Example: Configuring EoMPLS over GRE" for a sample configuration sequence of EoMPLS over GRE. For more details on EoMPLS over GRE, see the Deploying and Configuring MPLS Virtual Private Networks
In IP Tunnel Environments document. Overlay Tunnels for IPv6
The figure below illustrates how overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the Internet). By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border routers or between a border router and a host; however, both tunnel endpoints must support, IPv4 and IPv6 protocol stacks. IPv6 supports the following types of overlay tunneling mechanisms:
6to4 GRE
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) IPv4-compatible
Manual Figure 3
Overlay Tunnels Note
If the basic IPv4 packet header does not have optional fields, overlay tunnels can reduce the maximum transmission unit (MTU) of an interface by 20 octets. A network that uses overlay tunnels is difficult to troubleshoot. Therefore, overlay tunnels that connect isolated IPv6 networks should not be considered as the final IPv6 network architecture. The use of overlay tunnels is considered as a transition technique for a network that supports either both IPv4 and IPv6 protocol stacks or just the IPv6 protocol stack.
Consult the table below to determine which type of tunnel you want to configure to carry IPv6 packets over an IPv4 network.
Table 1
Suggested Usage of Tunnel Types to Carry IPv6 Packets over an IPv4 Network Tunneling Type
Suggested Usage Usage Notes 6to4
Point-to-multipoint tunnels that can be used to connect isolated IPv6 sites. Sites use addresses that begin with the 2002::/16 prefix.
GRE/IPv4

Simple point-to-point tunnels that can be used within a site or between sites.
Tunnels can carry IPv6, Connectionless Network ServiceCLNS, and many other types of packets.
ISATAP
Point-to-multipoint tunnels that can be used to connect systems within a site. Sites can use any IPv6 unicast addresses.
Manual
Simple point-to-point tunnels that can be used within a site or between sites. Tunnels can carry IPv6 packets only.
Individual tunnel types are discussed in detail in the following concepts, and we recommend that you review and understand the information on the specific tunnel type that you want to implement. Consult the table below for a summary of the tunnel configuration parameters that you may find useful.
Table 2
Overlay Tunnel Configuration Parameters by Tunneling Type Overlay Tunneling Type
Overlay Tunnel Configuration Parameter Tunnel Mode
Tunnel Source Tunnel Destination
Interface Prefix/Address 6to4
ipv6ip 6to4
An IPv4 address or a reference to an interface on which IPv4 is configured.
Not required. These are all point-to-multipoint tunneling types. The IPv4 destination address is calculated, on a per-packet basis, from the IPv6 destination.
An IPv6 address. The prefix must embed the tunnel source IPv4 address.
GRE/IPv4
gre ip
An IPv4 address. An IPv6 address. ISATAP
ipv6ip isatap
Not required. These are all point-to-multipoint tunneling types. The IPv4 destination address is calculated on a per-packet basis from the IPv6 destination.
An IPv6 prefix in modified eui-64 format. The IPv6 address is generated from the prefix and the tunnel source IPv4 address.
Manual ipv6ip
An IPv4 address. An IPv6 address.
IPv6 Manually Configured Tunnels
A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. The primary use of a manually configured tunnel is to stabilize connections that require secure communication between two edge routers, or between an end system and an edge router. The manual configuration tunnel also stabilizes connection between remote IPv6 networks.
An IPv6 address is manually configured on a tunnel interface. Manually configured IPv4 addresses are assigned to the tunnel source and destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks. Manually configured tunnels can be configured between border routers or between a border router and a host. Cisco Express Forwarding switching can be used for manually configured IPv6 tunnels. Switching can be disabled if process switching is required.
Automatic 6to4 Tunnels
An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. The key difference between automatic 6to4 tunnels and manuallyconfigured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint. In automatic 6to4 tunnels, routers are not configured in pairs because they treat the IPv4 infrastructure as a virtual nonbroadcast multiaccess (NBMA) links. The IPv4 address embedded in the IPv6 address is used to find the other end of the automatic tunnel.
An automatic 6to4 tunnel may be configured on a border router in an isolated IPv6 network, which creates a tunnel on a per-packet basis on a border router in another IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:border-router-IPv4-address ::/48.The embedded IPv4 addresses are 16 bits and can be used to number networks within the site. The border router at each end of a 6to4 tunnel must support both IPv4 and IPv6 protocol stacks. 6to4 tunnels are configured between border routers or between a border router and a host.
The simplest deployment scenario for 6to4 tunnels is to interconnect multiple IPv6 sites, each of which has at least one connection to a shared IPv4 network. This IPv4 network could either be the Internet or a corporate backbone. The key requirement is that each site have a globally unique IPv4 address; the Cisco software uses this address to construct a globally unique 6to4/48 IPv6 prefix. A tunnel with appropriate entries in a Domain Name System (DNS) that maps hostnames and IP addresses for both IPv4 and IPv6 domains, allows the applications to choose the required address IPv6 traffic can be carried over IPv4 GRE tunnels by using the standard GRE tunneling technique to provide the services necessary to implement a standard point-to-point encapsulation scheme. GRE tunnels are links between two points, with a separate tunnel for each point. GRE tunnels are not tied to a specific passenger or transport protocol, but in case of IPv6 traffic, IPv6 is the passenger protocol, GRE is the carrier protocol, and IPv4 is the transport protocol.
The primary use of GRE tunnels is to provide a stable connection and secure communication between two edge devices or between an edge device and an end system. The edge device and the end system must have a dual-stack implementation. GRE has a protocol field that identifies the passenger protocol. GRE tunnels allow intermediate system to intermediate system (IS-IS) or IPv6 to be specified as the passenger protocol, thereby allowing both IS-IS and IPv6 traffic to run over the same tunnel. If GRE does not have a protocol field, it becomes impossible to distinguish whether the tunnel is carrying IS-IS or IPv6 packets.

**NEW QUESTION 36**
Referring to the topology diagram show in the exhibit,




which three statements are correct regarding the BGP routing updates? (Choose three.)

A. The EBGP routing updates received by R1 from R5 will be propagated to the R2, R4, and R7 routers
B. The EBGP routing updates received by R3 from R6 will be propagated to the R2 and R4 routers
C. The EBGP routing updates received by R1 from R5 will be propagated to the R2 and R4 routers
D. The IBGP routing updates received by R3 from R2 will be propagated to the R6 router
E. The IBGP routing updates received by R2 from R1 will be propagated to the R3 router
F. The IBGP routing updates received by R1 from R4 will be propagated to the R5, R7, and R2 routers

**Answer:** ABD

**NEW QUESTION 39**
To which three IP multicast groups can a multicast MAC address "01-00-5E-4D-62-B1" listen? (Choose three.)

A. 231.205.98.177
B. 231.205.99.177
C. 239.77.98.177
D. 239.205.99.177
E. 224.205.98.177
F. 224.205.99.177

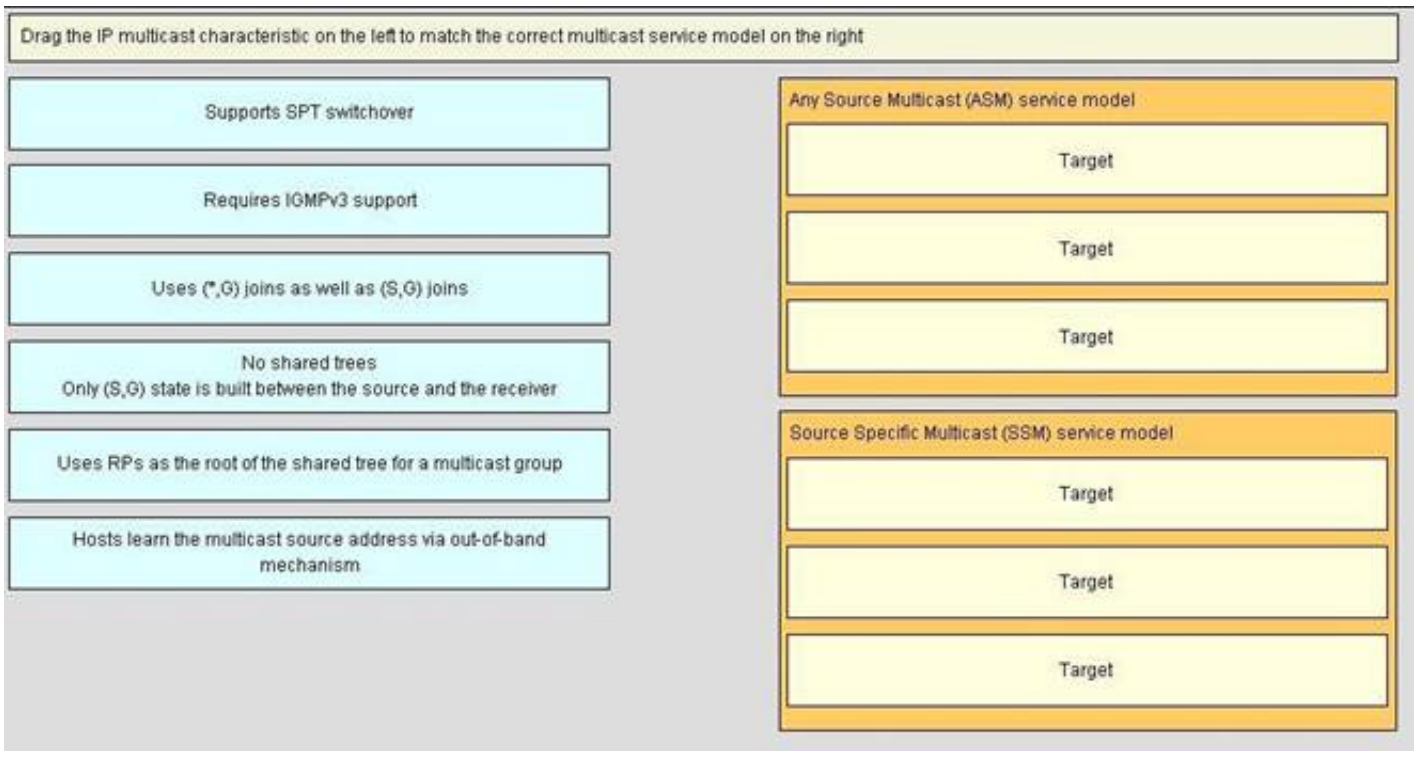
**Answer:** ACE

**NEW QUESTION 42**
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 47**
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 50**
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 53**
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 56**
A network architect is responsible for the company's multicast network domain design. Which multicast component acts as a meeting place for sources and receivers?

A. multicast shared tree
B. multicast distribution point
C. multicast rendezvous point
D. multicast source tree

**Answer:** C

**NEW QUESTION 58**
Which command set is used to implement an IPv6 PIM with the global scope embedded RP address of 2001:DB8::1 on a Cisco IOS XE router?

A. ipv6 unicast-routing ipv6 multicast-routingipv6 pim rp-address 2001:DB8::1 bidir
B. ipv6 multicast-routingipv6 pim rp-address 2001:DB8::1
C. ipv6 unicast-routing ipv6 multicast-routingipv6 pim rp-address FF7E:0120:2001:DB8:1111::4321
D. ipv6 unicast-routing ipv6 multicast-routing int Lo0ipv6 mld join-group FF7E:0120:2001:DB8:1111::4321
E. ipv6 unicast-routing ipv6 multicast-routing int Lo0ipv6 mld join-group FF75:0120:2001:DB8:1111::4321

**Answer:** D

**NEW QUESTION 62**
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 66**
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 68**
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 71**
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. If a certain command or command option is not supported, please try to use a different command that is supported.**

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

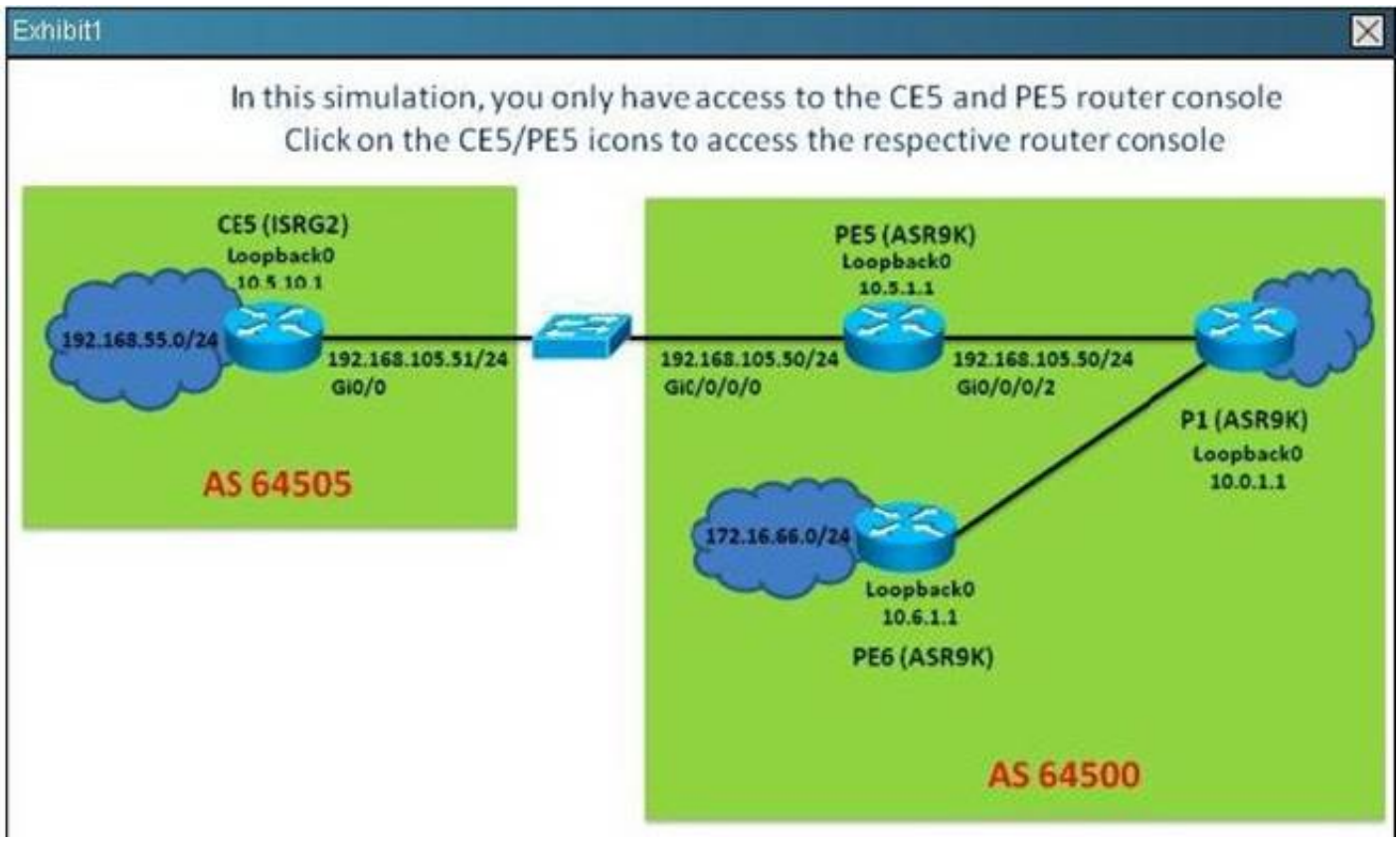
All the devices in this simulation have been pre-configured and you are not required to enter in any configurations.

Scenario

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

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

Exhibit1




CE5

CE5#


On the PE5 router, which statementis correct regarding the learned BGP prefixes?

A. The 209.165.201.0/27 prefix is received from the 10.0.1.1 IBGP peer which is a route reflector
B. The 172.16.66.0/24 prefix BGP next-hop points to the route reflector
C. All prefixes learned on PE5 has the default local preference value
D. The 209.165.202.128/27 prefix is originated by the 10.0.1.1 IBGP peer

**Answer:** C

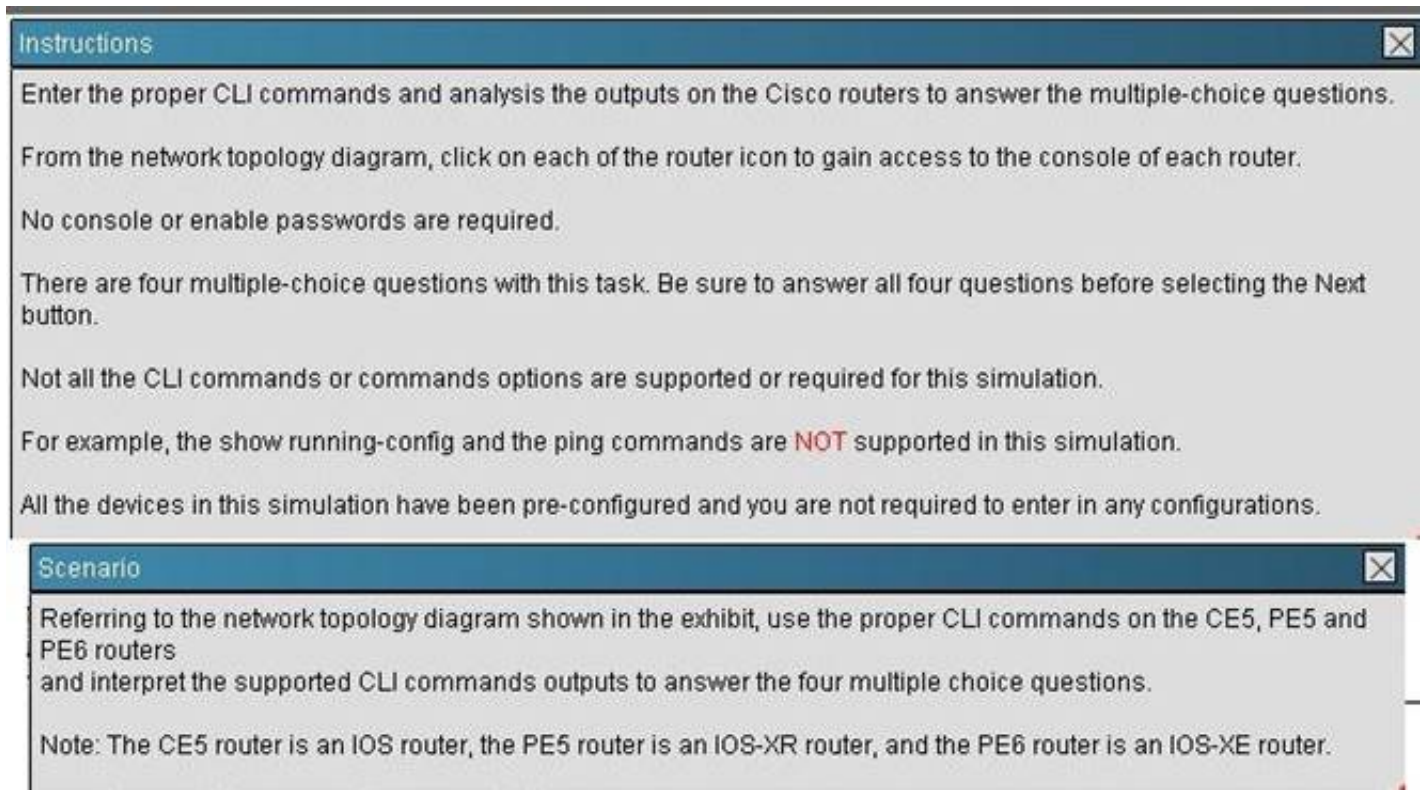
**Explanation:** #show ip bgp -- check i tag for PE5

**NEW QUESTION 75**
R1 is designated as the PIM RP within the SP core. Which two configuration parameters must be used to enable and activate R1 as the BSR and RP for the core environment? (Choose two.)

A. ip pim send-rp-announce loopback0 scope 16
B. ip pim bsr-candidate loopback0
C. ip pim send-rp-discovery loopback0 scope 16
D. ip pim rp-candidate loopback0
E. ip pim send-RP-announce loopback0 scope 16 group-list 1

**Answer:** BD

**NEW QUESTION 78**
Refer to the exhibit.



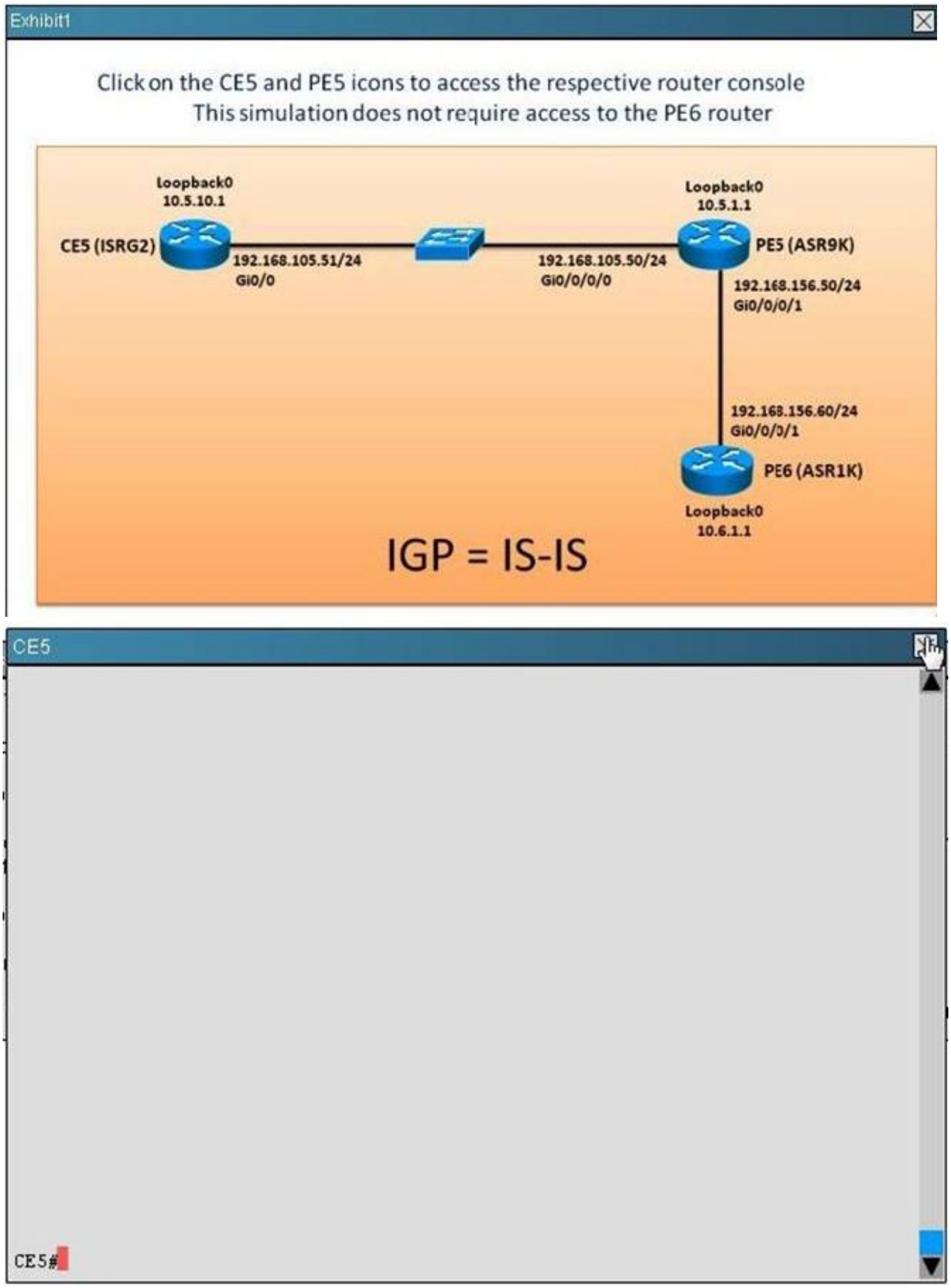


Exhibit1
Click on the CE5 and PE5 icons to access the respective router console
This simulation does not require access to the PE6 router
Loopback0
10.5.10.1
CE5 (ISRG2)
192.168.105.51/24
Gi0/0
192.168.105.50/24
Gi0/0/0/0
Loopback0
10.5.1.1
PE5 (ASR9K)
192.168.156.50/24
Gi0/0/0/1
192.168.156.60/24
Gi0/0/0/1
PE6 (ASR1K)
Loopback0
10.6.1.1
IGP = IS-IS
CE5
CE5#


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 81**
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 83**
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 85**
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.

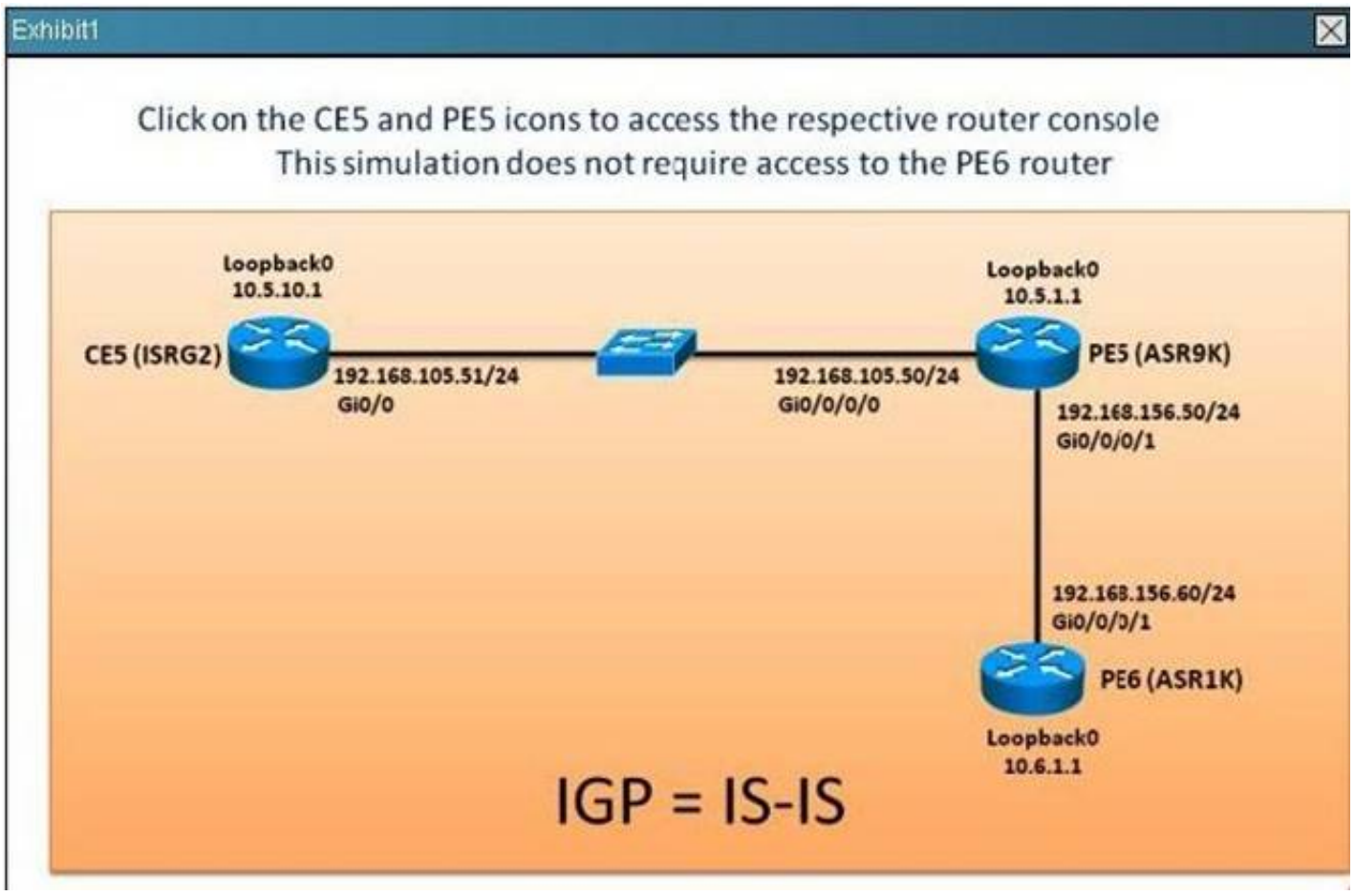
All the devices in this simulation have been pre-configured and you are not required to enter in any configurations.

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




CE5

CE5#


On the PE, which two statements are correct regarding the(192.168.156.60,224.1.1.1) entry? (Choose two,)

A. The RPF neighbor points towards the RP
B. The RPF neighbor is reachable overthe Gi0/0/0/1 interface
C. The OIL contains the GiO/0/0/0 interface
D. The IIL is Null

**Answer:** AC

**Explanation:** #show ip mroute

**NEW QUESTION 90**
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 95**
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 97**
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 98**
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 103**
A network engineer must configure a Cisco IOS XR router with BGP dampening. Which configuration meets these parameters?

A. router bgp 60 bgp dampening
B. router bgp 60 neighbor 10.0.0.2 bgp dampening
C. router bgp 60address-family ipv4 unicast bgp dampening
D. route-policy dampening_specific drop!router bgp 60address-family ipv4 unicastbgp dampening route-policy dampening_specific
E. router bgp 60 address-family ipv4 bgp dampening

**Answer:** C

**NEW QUESTION 108**
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

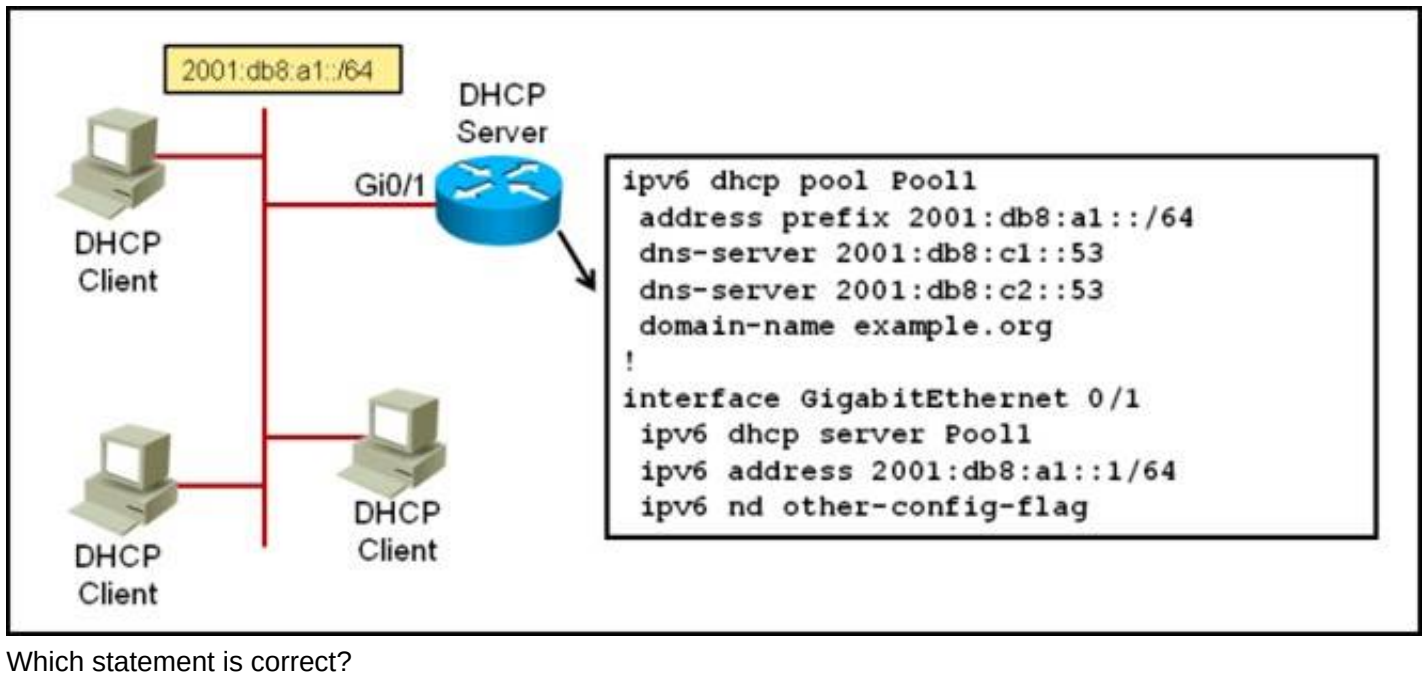
**Explanation:** Triggered joins are sent when the primary or the secondary RPF information changes. No RPF change prunes are sent for MoFRR streams.
mofrr
To perform a fast convergence (multicast-only fast reroute, or MoFRR) of specified routes/flows when a failure is detected on one of multiple equal-cost 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 110**
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 111**
Refer to the Cisco IOS DHCPv6 configuration shown in the exhibit.



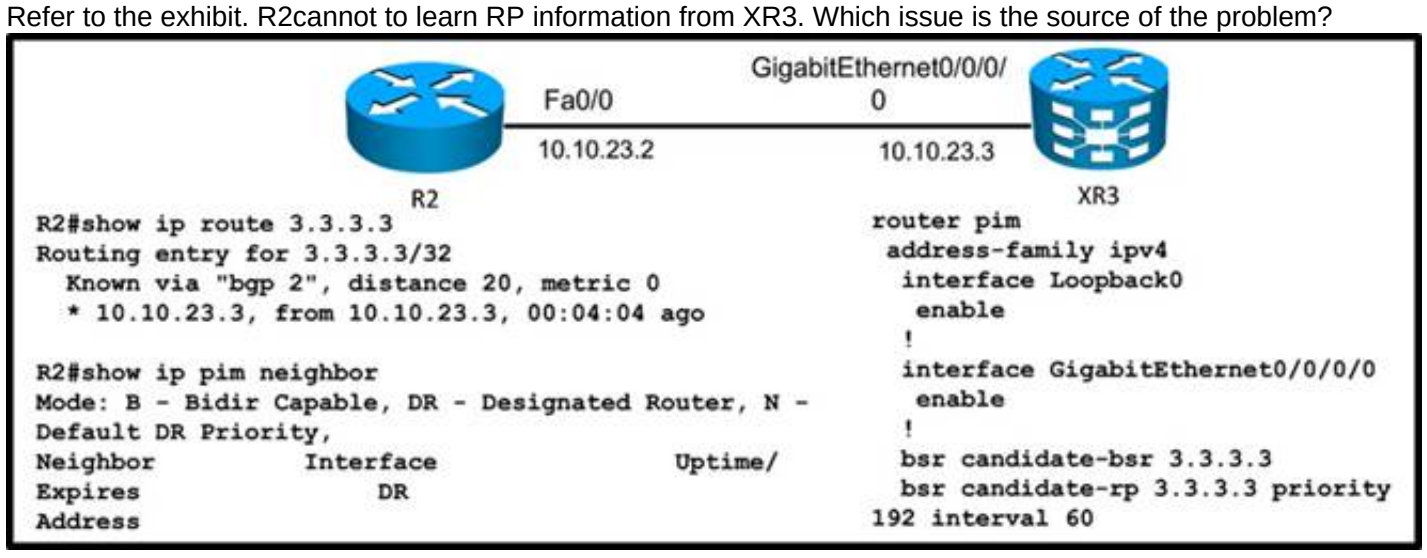

Which statement is correct?

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 114**
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 117**
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 122**
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 124**
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 127**
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.

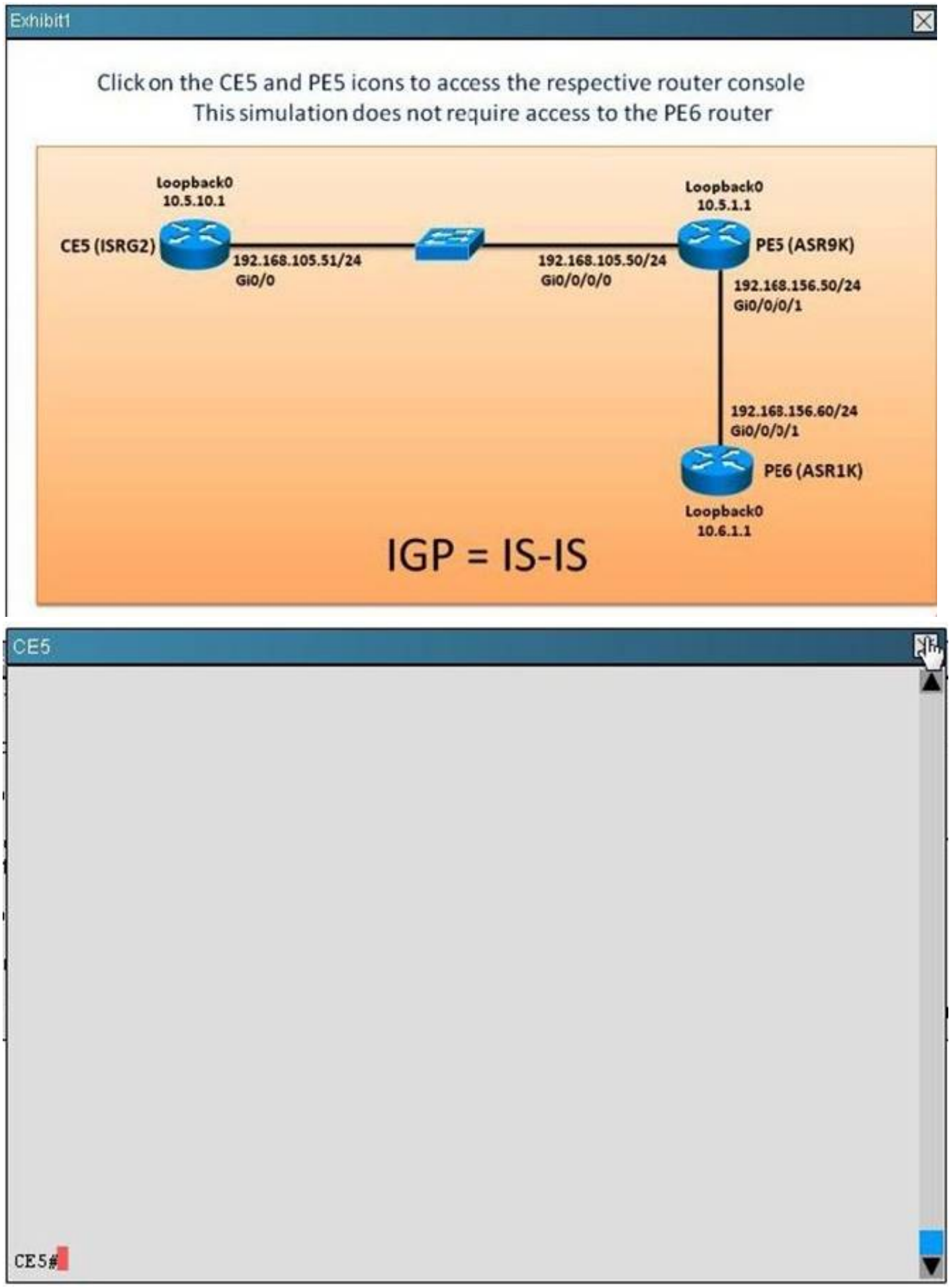


Exhibit1
Click on the CE5 and PE5 icons to access the respective router console
This simulation does not require access to the PE6 router
Loopback0
10.5.10.1
CE5 (ISRG2)
192.168.105.51/24
Gi0/0
192.168.105.50/24
Gi0/0/0/0
Loopback0
10.5.1.1
PE5 (ASR9K)
192.168.156.50/24
Gi0/0/0/1
192.168.156.60/24
Gi0/0/0/1
PE6 (ASR1K)
Loopback0
10.6.1.1
IGP = IS-IS
CE5
CE5#


Which router is configured as the RPforthe 234.1.1.1 multicast group and which Is the multicast source that is currently sending traffic to the 234.1.1.1 multicast group? (Choose two.)

A. CE5
B. PE5
C. PE6
D. 10.5.10.1
E. 10.5.1.1
F. 192.168.156.60

**Answer:** CE

**Explanation:** #show ip mroute234.1.1.1
#show ip route

**NEW QUESTION 129**
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.)

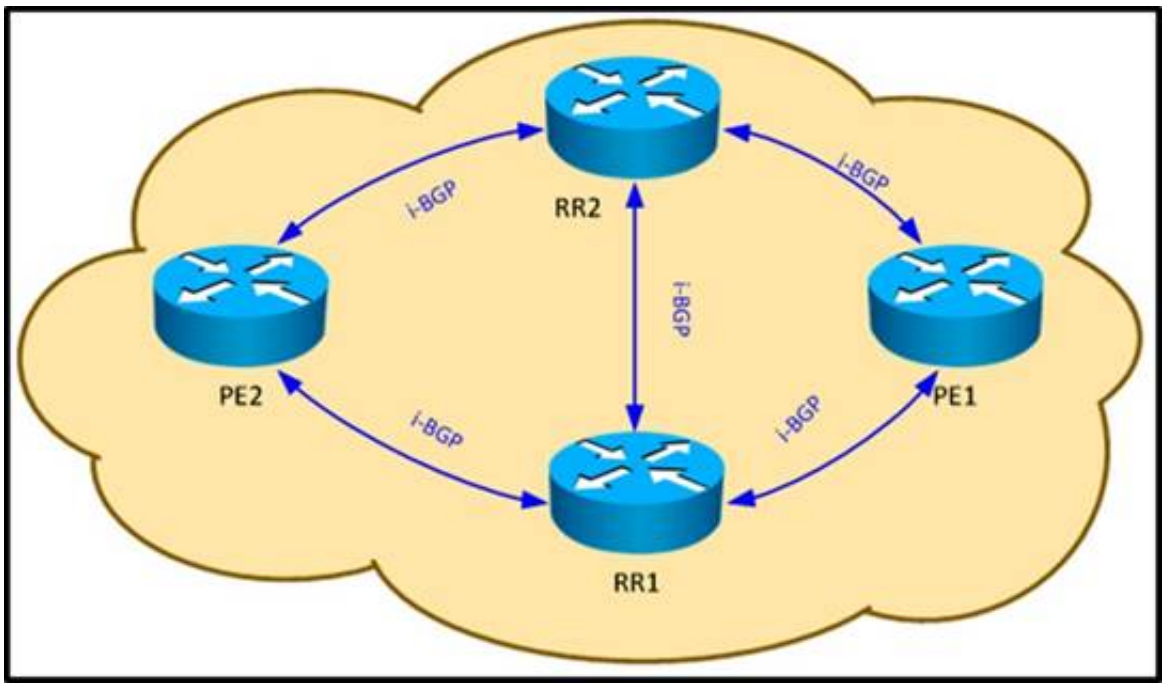
A. The neighbor-group efg is missing the ebgp-multihop 2 configuration
B. The ttl-security configuration command is missing the option to set the number of hops
C. The passall route policy is wrong

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 133**
Refer to the exhibit.




Which configuration ensures that RR2 does not send the same updates to PE2 that RR1 learns via PE1?

A. RR1 and RR2 should have different router IDs.
B. RR1 and RR2 should have different originator IDs.
C. RR1 and RR2 should have the same router IDs.
D. RR1 and RR2 should have the same cluster IDs.

**Answer:** D

**NEW QUESTION 136**
Which two statements regarding Auto RP operations and implementations are correct? (Choose two.)

A. Candidate RPs send RP announcements to the 224.0.1.39 multicast group, and the mapping agents send RP discovery messages to the 224.0.1.40 multicast group
B. Every PIM-SM router must be configured with the RP mapping agent IP address
C. Candidate RPs learn the IP address of the mapping agents via periodic RP discovery messages
D. Administrative scoping can be configured to limit the scope of the RP announcements
E. A Reverse Path Forwarding check is done on the RP discovery messages
F. RP discovery messages are flooded hop by hop throughout the network as multicast to the all PIM routers multicast group with a TTL of 1

**Answer:** AD

**Explanation:** Auto-RP
Automatic route processing (Auto-RP) is a feature that automates the distribution of group- to-RP mappings in a PIM network. This feature has these benefits:
It is easy to use multiple RPs within a network to serve different group ranges. It allows load splitting among different RPs.
It facilitates the arrangement of RPs according to the location of group participants.
It avoids inconsistent, manual RP configurations that might cause connectivity problems. Multiple RPs can be used to serve different group ranges or to serve as hot backups for each other. To ensure that Auto-RP functions, configure routers as candidate RPs so that they can announce their interest in operating as an RP for certain group ranges. Additionally, a router must be designated as an RP-mapping agent that receives the RP- announcement messages from the candidate RPs, and arbitrates conflicts. The RPmapping agent sends the consistent group-to-RP mappings to all remaining routers. Thus, all routers automatically determine which RP to use for the groups they support auto- rp candidate-rp
To configure a router as a Protocol Independent Multicast (PIM) rendezvous point (RP) candidate that sends messages to the well-known CISCO-RP-ANNOUNCE multicast group
(224.0.1.39), use the auto-rp candidaterp command in PIM configuration mode. To return to the default behavior, use the no form of this command. auto-rp candidate-rp type interface-path-id scope ttl-value [ group-list access-listname ] [ interval seconds ] [bidir] no auto-rp candidate-rp type interface-path-id scope ttl-value [ group-list access-listname] [ interval seconds ] [bidir]

**NEW QUESTION 141**
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

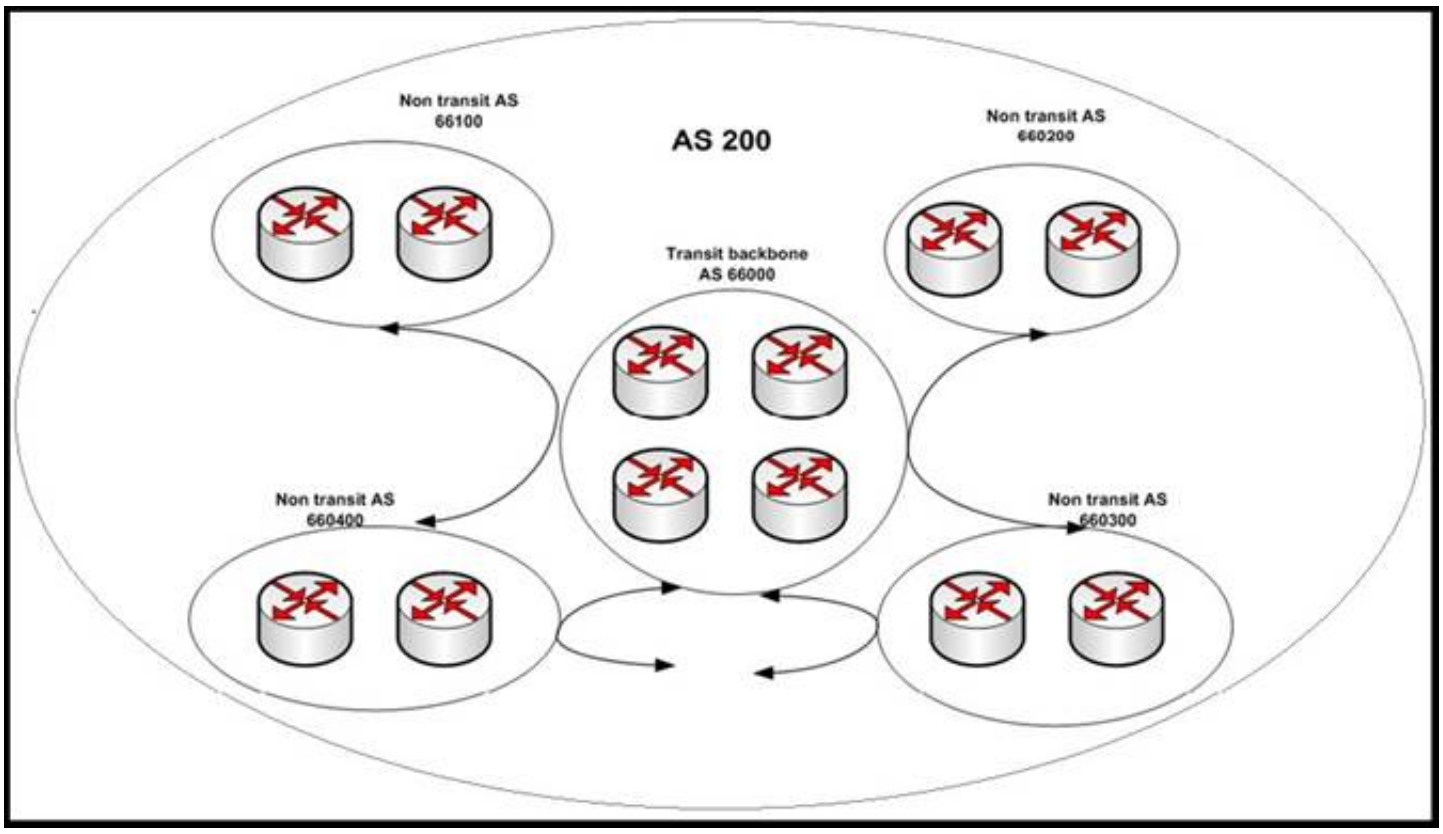
**Answer:** B

**NEW QUESTION 146**
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 148**
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 152**
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 154**
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 156**
Which three statements are correct regarding PIM-SM? (Choose three.)

A. There are three ways to configure the RP: Static RP, Auto-RP, or BSR
B. PIM-SM only uses the RP rooted shared tree and has no option to switch over to the shortest path tree
C. Different RPs can be configured for different multicast groups to increase RP scalability
D. Candidate RPs and RP mapping agents are configured to enable Auto-RP
E. PIM-SM uses the implicit join model

**Answer:** ACD

**NEW QUESTION 157**
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 159**
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 160**
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 161**
Which command set is used to configure BFD support for a BGP neighbor that is reachable through GigabitEthernet 0/0/0/0 on Cisco IOS XR?

A. router bgp 300 bfd multiplier 2bfd minimum-interval 20neighbor 10.20.20.2remote-as 200
B. router bgp 300 bfd multiplier 2bfd minimum-interval 20neighbor 10.20.20.2remote-as 200 bfd fast-detect
C. bfdecho disable router bgp 300neighbor 10.20.20.2remote-as 200
D. bfdrouter bgp 300neighbor 10.20.20.2remote-as 200
E. interface Gi0/0/0/0ipv4 verify unicast source reachable-via rx router bgp 300bfd multiplier 2bfd minimum-interval 20neighbor 10.20.20.2remote-as 200 bfd fast-

detect
F. interface Gi0/0/0/0ipv4 verify unicast source reachable-via rx bfdinterface Gi0/0/0/0 echo disable router bgp 300bfd multiplier 2bfd minimum-interval 20neighbor 10.20.20.2remote-as 200

**Answer:** B

**NEW QUESTION 166**
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 167**
A network engineer must deploy an iBGP-based cloud region configuration by means of templates to reduce the overall BGP CLI required. Which three commands represent a basic configuration for a BGP peer session template on a regular Cisco IOS instance? (Choose three.)

A. template peer-session session-template-name
B. remote-as as-number
C. neighbor-family config template
D. peer-family config template
E. as-override
F. timers keepalive-interval hold-time

**Answer:** ABF

**NEW QUESTION 170**
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 171**
Which mechanism is used by an IPv6 multicast receiver to join an IPv6 multicast group?

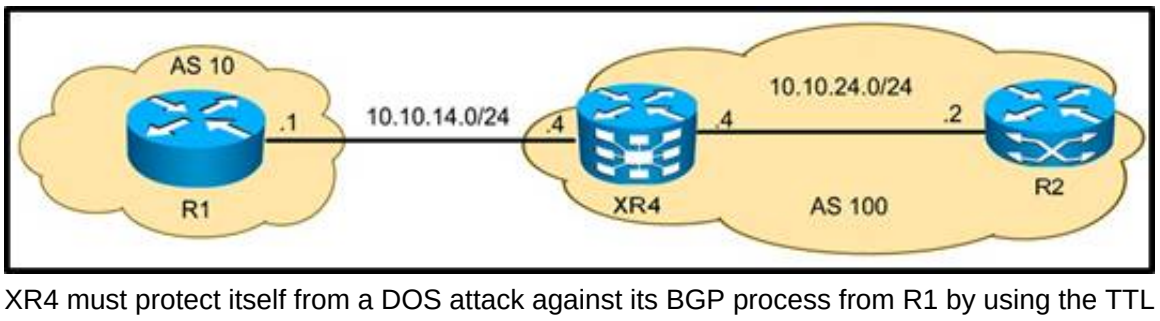
A. IGMP report
B. IGMP join
C. MLD report
D. General query
E. PIM join

**Answer:** C

**Explanation:** MLD Reports

The processing of MLDv1 join messages is essentially the same as with IGMPv2. When no IPv6 multicast routers are detected in a VLAN, reports are not processed or forwarded from the switch.
When IPv6 multicast routers are detected and an MLDv1 report is received, an IPv6 multicast group address and an IPv6 multicast MAC address are entered in the VLAN MLD database. Then all IPv6 multicast traffic to the group within the VLAN is forwarded using this address. When MLD snooping is disabled, reports are flooded in the ingress VLAN.
When MLD snooping is enabled, MLD report suppression, called listener message suppression, is automatically enabled. With report suppression, the switch forwards the first MLDv1 report received by a group to IPv6 multicast routers; subsequent reports for the group are not sent to the routers. When MLD snooping is disabled, report suppression is disabled, and all MLDv1 reports are flooded to the ingress VLAN.
The switch also supports MLDv1 proxy reporting. When an MLDv1 MASQ is received, the switch responds with MLDv1 reports for the address on which the query arrived if the group exists in the switch on another port and if the port on which the query arrived is not the last member port for the address.

**NEW QUESTION 172**
Refer to the exhibit.




XR4 must protect itself from a DOS attack against its BGP process from R1 by using the TTL security feature. Which configuration achieves this goal?

A. router bgp 100neighbor 10.10.14.1 ttl-security
B. router bgp 100neighbor 10.10.14.1 ttl-security hops 1
C. router bgp 100neighbor 10.10.14.1 ttl-security hops 254
D. router bgp 100neighbor 10.10.14.1 ttl-security hops 255

**Answer:** A

**NEW QUESTION 174**
.....

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your 642-885 Exam with Our Prep Materials Via below:

https://www.certleader.com/642-885-dumps.html