642-885 Q&As

Deploying Cisco Service Provider Advanced Routing

Pass Cisco 642-885 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/642-885.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

Correct Answer: C

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.

QUESTION 2

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.

Correct Answer: AC

QUESTION 3

Which multicast group range is reserved for SSM?

A. 224.0.0.0/8

B. 225.0.0.0/8

C. 232.0.0.0/8

D. 239.0.0.0/8

Correct Answer: C

PIM-SSM Operations PIM in Source Specific Multicast operation uses information found on source addresses for a multicast group provided by receivers and performs source filtering on traffic. ·By default, PIM-SSM operates in the 232.0.0.0/8 multicast group range for IPv4 and ff3x::/32 (where x is any valid scope) in IPv6. To configure these values, use the ssm range command. ·If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers must be upgraded with Cisco IOS XR software that supports the SSM feature. ·No MSDP SA messages within the SSM range are accepted, generated, or forwarded

QUESTION 4

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

Correct Answer: ACD

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).

QUESTION 5

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

Correct Answer: D