Cisco IOS Multicast Q&A

Multicast

Q. What is IP Multicast?

A. IP Multicast is a bandwidth-conserving technology specifically designed to reduce traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients or homes. By replacing copies for all recipients with the delivery of a single stream of information, IP Multicast is able to minimize the burden on both sending and receiving hosts and reduce overall network traffic. For more information visit http://www.cisco.com/go/multicast.

Q. Where are multicast addresses available?

A. For more information visit http://www.iana.org/cgi-bin/multicast.pl.

Q. What addresses should customers use?

A. For inter-domain multicast refer to RFC3180 GLOP Addressing and for intra-domain multicast refer to RFC2365 Administratively Scoped IP Multicast.

Q. Can dynamic multicast addresses be assigned within my domain?

A. Yes. Group addresses can be allocated with a protocol called MADCAP defined in RFC2730. This is similar to DHCP.

Q. Does multicast support Network Address Translation (NAT)?

A. Cisco supports multicast source address translation with multicast NAT. For more information visit http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a008009474d.shtml

The Multicast Service Reflection feature provides the capability for users to translate externally received multicast destination addresses to addresses that conform to their organization's internal addressing policy. For more information visit http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/mcastsrv.html

Q. What management options are available for a multicast network?

A. The Cisco Multicast Manager is a web-based software application that allows service providers and enterprise customers to monitor all critical components of the multicast network. For more information visit http://www.cisco.com/go/cmm

Multicast Protocols

Q. What is Source Specific Multicast?

A. Source Specific Multicast (SSM) is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

Q. Should I use PIM Sparse-Mode or Dense-Mode?

A. Cisco recommends PIM Sparse-Mode (PIM-SM). Cisco also recommends PIM-SSM for one-to-many applications and Bidirectional PIM (bidir-PIM) for many-to-many applications.

Q. What is Sparse-dense mode?

A. Sparse-dense is an interface configuration that allows both dense mode groups and sparse mode groups to flow across that interface. It is normally only applied when Auto-RP is used to send Rendezvous Point information.

Q. What is Bidirectional PIM (bidir-PIM)?

A. Bidir-PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast and is an extension of the PIM Sparse Mode (PIM-SM) feature. Traffic flows in both directions in case of a tree built by bidir-PIM as opposed to other multicast protocols that have trees rooted at either the source or at a Rendezvous Point (RP). Bidir-PIM is recommended for many-to-many applications because the amount of state required to be kept by the router is not related to the number of sources.

Q. What is Pragmatic General Multicast?

A. Pragmatic General Multicast (PGM) is a reliable multicast transport protocol. IP multicast uses UDP, not TCP, and is inherently unreliable. PGM performs the same function as TCP, while using negative acknowledgements (NAKs), rather than positive acknowledgements. This prevents an ACK implosion when large numbers of receivers reply.

The PGM Router Assist feature saves bandwidth by substantially reducing the number of NAKs to the source and by constraining the retransmissions to only those receivers that experience data loss.

Q. What is Multiprotocol Border Gateway Protocol?

A. Multiprotocol Border Gateway Protocol (MBGP) adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, multiprotocol BGP is an enhanced BGP that carries 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) to build data distribution trees. For more information visit http://www.cisco.com/en/US/tech/tk365/tk859/tsd_technology_support_sub-protocol_home.html

Rendezvous Point

Q. Where should the Rendezvous Point (RP) be placed?

A. Generally, RP placement is not an issue, as the default behavior of PIM-SM is to switch over to the shortest path tree when the first packet is received by the last hop router. The RP is therefore not normally within the data path and is not a limiting factor.

Q. What are the options for RP mapping?

A. There are number of different options for RP mapping. For more information visit http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/whitepaper_c11-508498.html

Q. What is Anycast RP?

A. 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. For more information visit http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/anycast.html

Reverse Path Forwarding

Q. What is Reverse Path forwarding?

A. Reverse Path Forwarding (RPF) provides loop avoidance. It is an algorithm used to forward multicast packets. 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 whether 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 is forwarded.
- **Step 3.** If the RPF check in Step 2 fails, the packet is dropped.

Q. How does RPF work for Shared trees?

A. The RPF check is conducted differently for data flowing via the shared tree, which is routed at the RP, not the Source. In this instance, the RPF is successful when data arrives at the interface that it would use to reach the RP.

Multicast VPNs

Q. What is Multicast VPN?

A. Multicast VPN (MVPN) provides the ability to dynamically provide multicast support over MPLS networks. MVPN introduces an additional set of protocols and procedures that help enable a provider to support multicast traffic in a VPN. For more information visit http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd802aea84.html

Miscellaneous

Q. Can I use Hot Standby Router Protocol for Multicast?

A. Hot Standby Router Protocol (HSRP) is a redundancy protocol for establishing a fault-tolerant default gateway. It is not generally recommended to use HSRP for IP multicast routing. For more information visit http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094aab.shtml

Q. How does HSRP interact with Cisco Group Management Protocol?

A. If HSRP and CGMP leave processing are both in use, then in certain topologies, unicast flooding can occur. Frames addressed to HSRP are not flooded across the virtual LAN (VLAN), but are intercepted and forwarded to the switch CPU. When a packet is identified as not being IGMP, it is forwarded to all router ports, but if a host is not locally connected to the switch where the HSRP routers are located, then unicast flooding can occur.

Q. Does Cisco IOS Firewall support IP Multicast?

A. Both Cisco IOS Firewall and PIX Firewall 7.0 can operate with full PIM functionality.

Q. How do I prevent a state explosion with IPTV?

A. Each IPTV client provides feedback to the same group on which it receives data; therefore, each client becomes a source and may have a corresponding (S, G) entry. The client must be prevented from sourcing data to the group address in order to mitigate this issue.

Q. Can IP Multicast be load-balanced?

A. IP Multicast uses the RPF check to ensure that the data has arrived via the most efficient path. The RPF check chooses only one interface for incoming data for a particular source; therefore, per flow multicast can be load balanced. If packet load balancing is required, then a unicast tunnel must be created between the two ends for which load balancing is required.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-597679-00 04/10