INTERNET-DRAFT
draft-ietf-mboned-admin-ip-space-01.txt
Category:Best Current Practice

David Meyer
University of Oregon
December 1996

Administratively Scoped IP Multicast

Status of this Memo

This document specifies an Internet Best Current Practice for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Internet Drafts

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document defines the "administratively scoped IP multicast space" to be the range 239.0.0.0 to 239.255.255.255 . In addition, it describes a simple set of semantics for the implementation of Administratively Scoped IP Multicast.

This memo is a product of the MBONE Deployment Working Group (MBONED) in the Operational Requirements area of the Internet Engineering Task Force. Submit comments to <mboned@ns.uoregon.edu> or the author.

Acknowledgments

Much of this memo is taken from "Administratively Scoped IP Multicast", Van Jacobson and Steve Deering, presented at the 30th IETF, Toronto, Canada, 25 July 1994. Mark Handley and Dave Thaler also made insightful comments on the orignal draft.

Introduction

Most current IP multicast implementations achieve some level of scoping by using the TTL field in the IP header. Typical MBONE (Multicast Backbone) usage has been to engineer TTL thresholds that confine traffic to some administratively defined topological region. The basic forwarding rule for interfaces with configured TTL thresholds is that for a packet is not forwarded across the interface unless its remaining TTL greater than the threshold.

TTL scoping has been used to control the distribution of multicast traffic with the objective of easing stress on scarce resources (e.g., bandwidth), or to achieve some kind of improved privacy or scaling properties. In addition, the TTL is also used in its traditional role to limit datagram lifetime. Given these often conflicting roles, TTL scoping has proven difficult to implement reliably, and the resulting schemes have often been complex and difficult to understand.

On the other hand, by using administratively scoped IP multicast, one can achieve locally scoped multicast with simple, clear semantics. The key properties of any implementation of administratively scoped IP multicast are that (i). packets addressed to administratively scoped multicast addresses do not cross configured administrative boundaries, and (ii). administratively scoped multicast addresses are locally assigned, and hence are not required to be unique across administrative boundaries. These properties are sufficient to implement administrative scoping.

Allocation of the Administratively Scoped IP Multicast Address Space

IANA should allocate the range 239.0.0.0 to 239.255.255.255 to be the "Administratively Scoped IP Multicast" address space.

Discussion

In order to support administratively scoped IP multicast, a router should support the configuration of scoped IP multicast boundaries. Such a router, called a boundary router, does not forward packets matching its boundary definition in either direction across its border (the bi-directional check prevents problems with multicaccess networks). In addition, a boundary router always prunes the boundary for dense-mode groups, or doesn't accept joins for sparse-mode groups [PIMSM] in the administratively scoped range.

Structure of the IPv4 Administratively Scoped Multicast Space

The structure of the IP version 4 administratively scoped multicast space is loosely based on the IP Version 6 Multicast Addresses [RFC1884] assignments, and is partitioned into the following scope classes:

unassigned	239.0.0.0/10
unassigned	239.64.0.0/10
organization-local scope	239.128.0.0/10
site-local scope	239.192.0.0/10

The other two scope classes of interest, link-local scope and global scope, already exist to some extent in IP version 4 multicast space. In particular, the link-local scope is 224.0.0.0/24. The existing global scope allocations are currently somewhat more granular, and include

224.1.0.0-224.1.255.255	ST Multicast Groups
224.2.0.0-224.2.127.253	Multimedia Conference Calls
224.2.127.254	SAPv1 Announcements
224.2.127.255	SAPv0 Announcements (deprecated)
224.2.128.0-224.2.255.255	SAP Dynamic Assignments
224.252.0.0-224.255.255.255	DIS transient groups
232.0.0.0-232.255.255.255	VMTP transient groups

See ftp://ftp.isi.edu/in-notes/iana/assignments/multicast-addresses for current multicast address assignments.

Topological Requirements for Administrative Boundaries

An administratively scoped IP multicast region is defined to be a topological region in which there are one or more boundary routers with common boundary definitions. Such a router is said to be a boundary for scoped addresses in the range defined in its configuration.

Network administrators may configure a scope region whenever local multicast scope is required. In addition, an administrator may configure overlapping scope regions (networks can be in multiple scope regions) where convenient, with the only limitations being that a scope region must be connected (there must be a path between any two nodes within a scope region that doesn't leave that region), and convex (i.e., no path between any two points in the region can cross a region boundary).

Example: DVMRP

DVMRP [DVMRP] implementations could be extended to support a boundary attribute in the interface configuration [ASMA]. The boundary attribute that includes a prefix and mask, and has the semantics that packets matching the prefix and mask do not not pass the boundary. As mentioned above, the implementation would also prune the boundary.

Security Considerations

While security considerations are not explicitly discussed in this memo, it is important to note that a boundary router as described here should not be considered to provide any kind of firewall functionality.

References

[ASMA] V. Jacobson, S. Deering, "Administratively Scoped IP Multicast", , presented at the 30th IETF, Toronto, Canada, 25 July 1994.

[DVMRP] T. Pusateri, "Distance Vector Multicast Routing Protocol", draft-ietf-idmr-dvmrp-v3-03, September, 1996.

[RFC1884] R. Hinden. et. al., "IP Version 6 Addressing Architecture", RFC1884, December 1995.

[PIMSM] Estrin, D, et. al., "Protocol Independent Multicast Sparse Mode (PIM-SM): Protocol Specification", draft-ietf-idmr-PIM-SM-spec-09.ps, October, 1996.

Author's Address

David Meyer
Advanced Network Technology Center
University of Oregon
1225 Kincaid St.
Eugene, OR 97403

phone: +1 541.346.1747
email: meyer@antc.uoregon.edu