Network Working Group
Request for Comments: 2365
BCP: 23
Category: Best Current Practice

D. Meyer
University of Oregon

July 1998

Administratively Scoped IP Multicast

Status of this Memo

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

Copyright Notice

1. Abstract

This document defines the "administratively scoped IPv4 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. Finally, it provides a mapping between the IPv6 multicast address classes [RFC1884] and IPv4 multicast address classes.

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

2. 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. Steve Casner, Mark Handley and Dave Thaler have also provided insightful comments on earlier versions of this document.

3. 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 a packet is not forwarded across the interface unless its remaining TTL is 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.

A more serious architectural problem concerns the interaction of TTL scoping with broadcast and prune protocols (e.g., DVMRP [DVMRP]). The particular problem is that in many common cases, TTL scoping can prevent pruning from being effective. Consider the case in which a packet has either had its TTL expire or failed a TTL threshold. The router which discards the packet will not be capable of pruning any upstream sources, and thus will sink all multicast traffic (whether or not there are downstream receivers). Note that while it might seem possible to send prunes upstream from the point at which a packet is discarded, this strategy can result in legitimate traffic being discarded, since subsequent packets could take a different path and arrive at the same point with a larger TTL.

On the other hand, administratively scoped IP multicast can provide clear and simple semantics for scoped IP multicast. The key properties 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.

4. Definition of the Administratively Scoped IPv4 Multicast Space

The administratively scoped IPv4 multicast address space is defined to be the range 239.0.0.0 to 239.255.255.255.

5. Discussion

In order to support administratively scoped IP multicast, a router should support the configuration of per-interface scoped IP multicast boundaries. Such a router, called a boundary router, does not forward packets matching an interface’s boundary definition in either direction (the bi-directional check prevents problems with multi-access networks). In addition, a boundary router always prunes the boundary for dense-mode groups [PIMDM], and doesn’t accept joins for sparse-mode groups [PIMSM] in the administratively scoped range.

6. The Structure of the Administratively Scoped Multicast Space

The structure of the IP version 4 administratively scoped multicast space is loosely based on the IP Version 6 Addressing Architecture described in RFC 1884 [RFC1884]. This document defines two important scopes: the IPv4 Local Scope and IPv4 Organization Local Scope. These scopes are described below.

6.1. The IPv4 Local Scope -- 239.255.0.0/16

239.255.0.0/16 is defined to be the IPv4 Local Scope. The Local Scope is the minimal enclosing scope, and hence is not further divisible. Although the exact extent of a Local Scope is site dependent, locally scoped regions must obey certain topological constraints. In particular, a Local Scope must not span any other scope boundary. Further, a Local Scope must be completely contained within or equal to any larger scope. In the event that scope regions overlap in area, the area of overlap must be in its own local scope. This implies that any scope boundary is also a boundary for the Local Scope. The more general topological requirements for administratively scoped regions are discussed below.

6.1.1. Expansion of the IPv4 Local Scope

The IPv4 Local Scope space grows "downward". As such, the IPv4 Local Scope may grow downward from 239.255.0.0/16 into the reserved ranges 239.254.0.0/16 and 239.253.0.0/16. However, these ranges should not be utilized until the 239.255.0.0/16 space is no longer sufficient.

6.2. The IPv4 Organization Local Scope -- 239.192.0.0/14

239.192.0.0/14 is defined to be the IPv4 Organization Local Scope, and is the space from which an organization should allocate sub-ranges when defining scopes for private use.

6.2.1. Expansion of the IPv4 Organization Local Scope

The ranges 239.0.0.0/10, 239.64.0.0/10 and 239.128.0.0/10 are unassigned and available for expansion of this space. These ranges should be left unassigned until the 239.192.0.0/14 space is no longer sufficient. This is to allow for the possibility that future revisions of this document may define additional scopes on a scale larger than organizations.

6.3. Other IPv4 Scopes of Interest

The other two scope classes of interest, statically assigned link-local scope and global scope already exist in IPv4 multicast space.

The statically assigned link-local scope is 224.0.0.0/24. The existing static global scope allocations are 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 [RFC1700] for current multicast address assignments (this list can also be found, possibly in a more current form, on ftp://ftp.isi.edu/in-notes/iana/assignments/multicast-addresses).

7. 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 constrained 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). However, it is important to note that if administratively scoped areas intersect topologically, then the outer scope must consist of its address space minus the address spaces of any intersecting scopes. This requirement prevents the problem that would arise when a path between two points in a convex region crosses the boundary of an intersecting region. For this reason, it is recommended that administrative scopes that intersect topologically should not intersect in address range.

Finally, note that any scope boundary is a boundary for the Local Scope. This implies that packets sent to groups covered by 239.255.0.0/16 must not be forwarded across any link for which a scoped boundary is defined.

8. Partitioning of the Administratively Scoped Multicast Space

The following table outlines the partitioning of the IPv4 multicast space, and gives the mapping from IPv4 multicast prefixes to IPv6 SCOP values:

IPv6 SCOP	RFC 1884 Description	IPv4 Prefix
0	reserved	
1	node-local scope	
2	link-local scope	224.0.0.0/24
3	(unassigned)	239.255.0.0/16
4	(unassigned)	
5	site-local scope	
6	(unassigned)	
7	(unassigned)	
8	organization-local scope	239.192.0.0/14
A	(unassigned)	
B	(unassigned)	
C	(unassigned)	
D	(unassigned)	
E	global scope	224.0.1.0-238.255.255.255
F	reserved	
	(unassigned)	239.0.0.0/10
	(unassigned)	239.64.0.0/10
	(unassigned)	239.128.0.0/10

9. Structure and Use of a Scoped Region

The high order /24 in every scoped region is reserved for relative assignments. A relative assignment is an integer offset from highest address in the scope and represents a 32-bit address (for IPv4). For example, in the Local Scope defined above, 239.255.255.0/24 is reserved for relative allocations. The de-facto relative assignment "0", (i.e., 239.255.255.255 in the Local Scope) currently exists for SAP [SAP]. The next relative assignment, "1", corresponds to the address 239.255.255.254 in the Local Scope. The rest of a scoped region below the reserved /24 is available for dynamic assignment (presumably by an address allocation protocol).

In is important to note that a scope discovery protocol [MZAP] will have to be developed to make practical use of scopes other than the Local Scope. In addition, since any use of any administratively scoped region, including the Local Scope, requires dynamically assigned addressing, an Address Allocation Protocol (AAP) will need to be developed to make administrative scoping generally useful.

9.1. Relative Assignment Guidelines

Requests for relative assignments should be directed to the IANA. The IANA will be advised by an area expert when making relative address assignments. The area expert will be appointed by the relevant Area Director.

In general, relative addresses will be used only for bootstrapping to dynamic address assignments from within the scope. As such, relative assignments should only be made to those services that cannot use a dynamic address assignment protocol to find the address used by that service within the desired scope, such as a dynamic address assignment service itself.

10. Security Considerations

It is recommended that organizations using the administratively scoped IP Multicast addresses not rely on them to prevent sensitive data from being transmitted outside the organization. Should a multicast router on an administrative boundary be mis-configured, have a bug in the administrative scoping code, or have other problems that would cause that router to forward an administratively scoped IP multicast packet outside of the proper scope, the organizations data would leave its intended transmission region.

Organizations using administratively scoped IP Multicasting to transmit sensitive data should use some confidentiality mechanism (e.g. encryption) to protect that data. In the case of many existing video-conferencing applications (e.g. vat), encryption is available as an application feature and merely needs to be enabled (and appropriate cryptographic keys securely distributed). For many other applications, the use of the IP Encapsulating Security Payload (ESP) [RFC-1825, RFC-1827] can provide IP-layer confidentiality though encryption.

Within the context of an administratively scoped IP multicast group, the use of manual key distribution might well be feasible. While dynamic key management for IP Security is a research area at the time this note is written, it is expected that the IETF will be extending the ISAKMP key management protocol to support scalable multicast key distribution in the future.

It is important to note that the "boundary router" described in this note is not necessarily providing any kind of firewall capability.

11. References

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

[DVMRP] Pusateri, T., "Distance Vector Multicast Routing Protocol", Work in Progress.

[MZAP] Handley, M., "Multicast-Scope Zone Announcement Protocol (MZAP)", Work in Progress.

[PIMDM] Deering, S, et. al., "Protocol Independent Multicast Version 2, Dense Mode Specification", Work in Progress.

[PIMSM] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P., and L. Wei, "Protocol Independent Multicast Sparse Mode (PIM-SM): Protocol Specification", RFC 2362, June 1998.

[RFC1700] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

[RFC1884] Hinden. R., and S. Deering, "IP Version 6 Addressing Architecture", RFC1884, December 1995.

[SAP] Handley, M., "SAP: Session Announcement Protocol", Work in Progress.

12. Author’s Address

David Meyer
Cisco Systems
San Jose, CA

EMail: dmm@cisco.com

13. Full Copyright Statement