Lightweight Multicast Address Discovery Problem Space
draft-ietf-mboned-addrdisc-problems-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 23, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

Typically applications developers have requested static IANA assignments for their applications, even if the applications would typically be only used within a site, between consenting sites, or would not eventually even use multicast at all. This memo describes this problem space, and summarizes a number of proposed approaches to mitigating these problems.
Table of Contents

1. Introduction ...................................................... 3
2. Problem Statement ................................................ 4
3. Mitigation Techniques ............................................ 5
   3.1. Locally Scoped Address Assignment by a Registry .......... 5
   3.2. Single Administration Address Discovery with Server
        Configuration ........................................... 6
   3.3. Zero-configuration Single Administration Address
        Discovery .............................................. 7
   3.4. Global Multiple Administration Address Discovery ...... 7
4. DNS As a Means of Indirection .................................... 8
5. Acknowledgements ................................................ 9
6. IANA Considerations ............................................. 9
7. Security Considerations ......................................... 9
8. References ...................................................... 9
   8.1. Normative References ..................................... 9
   8.2. Informative References ................................... 9
Author’s Address ................................................... 10
Intellectual Property and Copyright Statements .................. 10
1. Introduction

There are a lot of different challenges relating to the discovery and use of an appropriate multicast address as described below. This document only addresses the second one.

a. Getting a list of all the available (public) sessions which one could join (and possibly send to), similar to a "TV guide". That is, having to know everything before you can decide if you’re interested in something or not; this is out of scope for this memo.

b. Discovering the multicast address used by a particular application for particular purpose, within or crossing a scope. I.e., you know what you’re looking for, but don’t know if the session has been created already and what its address would be.

c. The different sources (unicast addresses) participating in a session. For ASM, there is no need for such discovery. For SSM, this is expected to happen out-of-band or following separate requirements [I-D.lehtonen-mboned-dynssm-req].

Many applications have been written which leverage or could leverage multicast routing infrastructures, in one or more of the following scopes: (We’ll get back to these later.)

1. link-local scope,

2. [geographical] site scope,

3. organization-local scope,

4. global scope, used between consenting sites/enterprises, also including cases like "inside a country", or

5. a truly global scope.

Multicast-leveraging applications are often designed in such a manner that each multicast group has a "server", "session creator" or some other node(s) (or persons operating the nodes) which are in some way in control of the application.

Both the "server" and "client end" of an application are currently typically provisioned with the group address using static IANA assignment [I-D.ietf-mboned-addrarch]. Only rarely these apps are manually configured e.g. with locally scoped addresses even in cases where using local addresses would be feasible.
It would be highly desirable (as described in Section 2) that the applications could easily use more dynamic, and more scoping-friendy mechanisms for discovering the appropriate addresses to use.

All of these issues are only relevant to Any Source Multicast (ASM), as SSM requires this information is known a priori.

2. Problem Statement

The current IANA static assignment to applications is a problem for multiple reasons:

1. This messes up the multicast scoping plans which the site may have. Each application’s global address must be individually scoped and filtered in all the routers and in their access lists. Scoping should be easier.

2. Static IANA assignments are required for each application; a permanent global assignment for each potentially multicast-using application depletes the resource quickly.

3. This has issues with IPv6, because such IPv6 addresses can not be scalably routed in inter-domain routing; in intra-domain, this requires manual configuration or running BSR (for ff01::/16 or ff02::/16 or the like)

4. "Intended for local only use" applications typically leak through to the IPv4 MSDP because there is no clear logic which ones should be global and which ones are local.

There are at least four different proposed ways to mitigate this, from the least to most extensive:

a. Smaller-than-global single-administration address assignment by a registry (from 239/8 or elsewhere).

b. Smaller-than-global single-administration discovery, with the expectation that a locally scoped address is manually configured on the "server end".

c. Smaller-than-global single-administration discovery with complete zero-configuration.

d. Global (but restricted) multi-administration discovery with some amount of manual configuration.

We’ll outline each proposed mitigation technique briefly below.
NOTE: David Meyer’s experience from being the designated expert for IANA assignments is that almost all of the requested multicast addresses have been such that the requestors would not have been satisfied if their application would only be restricted to operate within a site.

If people agree on this, the first three mitigation techniques won’t have significant impact, because the application developers won’t implement the discovery in any case. They will _still_ want to get the globally scoped addresses from IANA, instead of implementing the "service discovery inside an organization" -shim.

3. Mitigation Techniques

The generic goals from the application/deployment perspective are:

- Not depending on any uncommon external infrastructure besides the application itself (e.g., a MADCAP [RFC2730] server), so that the application can be deployed where MADCAP server is not present. I.e., this should be sufficiently lightweight to be coded in the application or be used by a simple application shim library.

- The application should "just work" from perspective of "client end" without any configuration. "Server end" may or may not require configuration of an address.

- The presence of applications should be easily filterable at least at the edges of the network.

- Preferably it should also be easy to segment the use of application into the smallest possible scopes within the network, to avoid undue state and confusion in the network.

- We’ll look at using DNS as an additional component in Section 4.

3.1. Locally Scoped Address Assignment by a Registry

If we ignore requirements for different levels of scoping, the simplest approach would be to make globally unique assignments within a well known local scoped address block. Group address assignments could be made by IANA (or some other registry) to applications on a first come first serve basis, much like what is done for port numbers used in protocols such as SCTP, TCP and UDP. This well defined range could then be scoped at the public Internet boundaries to ensure private usage remains private.

Theoretically, reserved space within the administratively scoped
address range (239/8) defined by RFC 2365 [RFC2365] that could be used for such a purpose. This address range should even be scoped at public Internet boundaries already. However, many organizations are already making use of the entire administratively scoped range. For better or worse, we feel that it is now too late to reclaim the reserved address space within the administratively scoped range for the problem case described here even if it were to be appropriate to do so.

If we consider multiple levels of scoping, using static address assignments may be problematic for sites with the need to separate applications between their local boundaries. If no other scoping mechanism is used, the network would have to create and maintain complex forwarding and filtering rules to ensure group membership for the well defined group address does not leak outside the desired local scope.

Even if a well defined local scope address range could be used and additional levels of scoping were not an issue, it is not clear that multicast application developers would accept a local scoped address over a globally routable one. Given the choice of a local scoped assignment and a global one, what incentive is there for an application developer to choose a locally scoped one if there is even a faint chance of global usage?

IANA is not the only option for such a registry; for example, Regional Internet Registries could perform assignments if there was demand, as described by the "eGLOP" proposal [RFC3138]. No registry has yet taken up the offer though, and doing so would be useful only if IANA ceased making assignments itself.

An additional, fundamental question with static address assignment in the IPv4 multicast address space (224/4) is, how big of an address range should be reserved? Existing multicast applications in use have been written to use an address block as large as a /8. Any allocation on this order is clearly diminishing the limited pool of already limited IPv4 multicast addresses.

3.2. Single Administration Address Discovery with Server Configuration

The second mitigation technique would be to specify and implement a mechanism, requiring no infrastructure in the network, where the "server end" would be manually configured with appropriately selected locally-scoped addresses which the clients would use to discover the group address.

The client ends should discover the smallest possible scope where the application is supported.
A few notes on this method:

- One could characterize a potential solution as an easily implementable server shim at "server end" listening to a set well-known locally-scoped multicast addresses (e.g., SAP scope-relative addresses), which would respond to queries by "client end".

- How can the servers demultiplex "queries" sent to these addresses? Are these messages in SAP format or something simpler? The query must have an identifier (e.g., done by hashing a name?) which the server uses to know the client is interested in the server’s multicast transmission.

- How should the servers communicate back to the clients? By replying with unicast (issues after bootup with lots of nodes) or do the clients also join the address (DoS potential, a very crowded group which all the servers at least need to subscribe to)?

Again, this does not solve the root problem; why would an application designer implement this mechanism when he/she wants to support global scoping as well? IANA assignment will be requested in any case.

3.3. Zero-configuration Single Administration Address Discovery

A slightly more extensive problem is the same as above, but assuming that the application must be completely zero-configurable. That is, it must work without having to manually configure anything on the server end.

This could be achieved e.g., by adding to the above a SAP-like address segments from which the addresses could be dynamically reserved. This might not sit well on the organization’s local scoping plans, however.

However, it is worth considering whether this is really needed. For link-local scope, this may be desirable as such requires no set-up of multicast routing. But for larger scopes, is this really useful? If there is no administrator to configure the address, likely there is no multicast infrastructure in the first place, or desire to run the application in multicast mode!

Again, this does not solve the root problem.

3.4. Global Multiple Administration Address Discovery

Most applications are such that they _can_ be run over site/organization boundaries (even if they typically would not be), so the
application developers will want to support the most extensive scope. There is no common local scope (even between organization-local and global) which could cover these disjoint global interconnections, so the applications must use global scope addresses.

To get away from static IANA assignments, there should be a lightweight multicast address discovery function which could be used e.g., in the embedded devices to discover the appropriate multicast address they should use.

Obviously, the result could also be that the application should be restricted to a local scope, and use local scope addresses, but wider discovery should also be supported.

This approach has a number of challenges, however. It’s difficult to visualize how multiple administrative domains could perform discovery in a desired manner automatically -- we have to assume that the sites might not want to tell about all of their local sessions to all the other sites (i.e., you may want to allow site A to discover session 1, and site B to discover session 2, but not mix these). In other words, there will likely need to be some manual control of what gets seen to the outside and what not. This makes the mechanism more complicated, and requires more network operator management.

Further attributes and requirements for this kind of approach remain to be figured out.

4. DNS As a Means of Indirection

DNS could be leveraged as an additional configuration mechanism with varying usefulness in any of the preceding approaches. The relevant information could be stored in the DNS in mainly two different ways:

1. Using local information (e.g., DNS search path, reverse IP addresses, etc.); these have been analyzed in Section 3.2 of [I-D.palet-v6ops-tun-auto-disc], or

2. By global information, for example having IANA assign an application-specific DNS entry (e.g., "_dogfight.apps.mcast.net") instead of an address. The sites could either use a default value (which might point to e.g., scoped address space) or make their DNS servers authoritative for that zone and insert their own addresses.

Both assume the ability to (e.g., manually) insert records in the local DNS and perform DNS lookups. The former additionally assumes the capability to discover where to find the local information. If
these assumptions are acceptable, DNS could be used as an additional mechanism at least with the first two classes of mitigation techniques.

5. Acknowledgements

This memo grew out of the discussions in MBONED WG, where the participants were, among others, Beau Williamson, Albert Manfredi, Marshall Eubanks, John Kristoff, David Meyer, Stig Venaas, Rami Lehtonen, and Leonard Giuliano.

6. IANA Considerations

This memo includes no request to IANA.

[[Note to the RFC-Editor: this section should be removed prior to publication.]]

7. Security Considerations

As section Section 3.4 describes, the organizations will not want to expose all their sessions, or even knowledge that the organization is using a particular application, to the outside. The confidentiality needs must be considered when designing a solution to solve one of the problems in this problem space.

8. References

8.1. Normative References

[I-D.ietf-mboned-addrarch]

8.2. Informative References

[I-D.lehtonen-mboned-dynssm-req]
Lehtonen, R., "Requirements for discovery of dynamic SSM sources", draft-lehtonen-mboned-dynssm-req-00 (work in progress), February 2005.

[I-D.palet-v6ops-tun-auto-disc]
Palet, J. and M. Diaz, "Analysis of IPv6 Tunnel End-point


Author’s Address

Pekka Savola
CSC/FUNET
Espoo
Finland

Email: psavola@funet.fi

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might be available; nor does it represent that it has
made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.