Abstract

Typically applications developers have requested static IANA assignments for the 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 IANA ........... 5  
   3.2 Single Administration Address Discovery with Server  
       Configuration ........................................... 6  
   3.3 Zero-configuration Single Administration Address  
       Discovery ............................................... 6  
   3.4 Global Multiple Administration Address Discovery ...... 7  
4. Acknowledgements ........................................ 8  
5. IANA Considerations ....................................... 8  
6. Security Considerations ................................... 8  
7. References ............................................... 8  
   7.1 Normative References .................................. 8  
   7.2 Informative References ................................. 8  
Author’s Address ........................................... 9  
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, see 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-reg].

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 such 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, especially the ones with a large number of clients.
It would be highly desirable that the applications could easily use more dynamic, and more scoping-friendly 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 for these applications is a problem for multiple reasons:

- 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.

- Static IANA assignments are required for each application; a permanent global assignment for each application which could use multicast depletes the resource quickly.

- 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)

- "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 IANA (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.

3.1 Locally Scoped Address Assignment by IANA

If we ignore the first problem about local scoping, the easiest mitigation technique might be having IANA assign locally scoped addresses on FCFS basis (like UDP/TCP port numbers). This could be done inside or outside of 239/8.

This way the local applications could easily get a local assignment which could be easily filtered by site administrators at site borders.

This is slightly inflexible as the application developers could only tell whether the application’s scope is link-local (there are very few of these), global, or something in between. "Expanding ring
search" inside the site-local scopes would not be possible.

NOTE, based on DaveM’s experience, it is not clear why the application designers would accept a local range instead of a global assignment, even if the application would primarily be used within a local scope.

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, 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. 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.

5. IANA Considerations

This memo includes no request to IANA.

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

6. 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.

7. References

7.1 Normative References

[I-D.ietf-mboned-addrarch]
Savola, P., "Overview of the Internet Multicast Addressing Architecture",

7.2 Informative References

[I-D.lehtonen-mboned-dynssm-req]
Lehtonen, R., "Requirements for discovery of dynamic SSM sources",
Internet-Draft draft-lehtonen-mboned-dynssm-req-00, February 2005.

Author’s Address

Pekka Savola
CSC/FUNET
Espoo
Finland

Email: psavola@funet.fi