IPv6 multicast address assignment with DHCPv6
draft-jdurand-assign-addr-ipv6-multicast-dhcpv6-01

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

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 August 19, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

This document proposes a simple solution to solve IPv6 multicast address assignment problem using the DHCPv6 protocol.
Table of Contents

1. Introduction ................................................. 3
   1.1 IPv6 multicast deployment status .................... 3
   1.2 Terminology .......................................... 3
   1.3 SSM: no solution needed ............................. 3
   1.4 Session announcement considerations ................. 4
2. State of the art for address assignment ..................... 4
3. Assignment with DHCPv6 ...................................... 4
   3.1 New DHCPv6 options .................................. 4
      3.1.1 IA_MA option for IPv6 Multicast Addresses .... 4
      3.1.2 Scope Option for IPv6 multicast address ........ 6
   3.2 Address timers ....................................... 6
   3.3 Assignment of a multicast prefix ..................... 7
   3.4 Client and server behavior ........................... 7
4. Group-ID consideration ....................................... 8
5. Deployment scenarios - Case studies .......................... 8
   5.1 Scenario 1: Site deployment ......................... 8
   5.2 Scenario 2: Campus deployment ....................... 9
   5.3 Scenario 3: ISP deployment ........................... 9
6. Security considerations ..................................... 9
7. Acknowledgement .......................................... 10
8. Discussions .............................................. 10
9. Changes from -00 ......................................... 10
10. References .............................................. 10
   10.1 Normative references ................................ 10
   10.2 Informative references .............................. 11
      Author’s Address .................................... 12
      Intellectual Property and Copyright Statements .... 13
1. Introduction

Embedded-RP [11] is the only available solution for IPv6 interdomain ASM. Embedded-RP requires an IPv6 multicast address assignment mechanism, as multicast addresses mapping to the RP cannot be guessed and manually built by users. This is depicted in section 2.1.2 of the IETF working group document draft-ietf-mboned-addrarch [13].

This document proposes a simple solution to assign IPv6 multicast addresses or prefixes using the DHCPv6 protocol [8].

1.1 IPv6 multicast deployment status

The document draft-jdurand-ipv6-multicast-ra [14] recalls the following:

"The deployment of IPv6 multicast is expanding. Some networks have already put the service in production. Some gateways have been deployed, making it possible to have interoperability between IPv4 and IPv6 multicast. Some sites have even stopped IPv4 multicast, due to its complexity (due to NAT and MSDP for example) and only rely on IPv6 multicast, using the deployed gateways for interoperability with IPv4.

As of this writing, most sessions are created manually from unicast-prefix based address space [6], or use SDR to form a semi-random address. Nevertheless these addresses cannot fit with embedded-RP [11] which is the only existing solution for IPv6 interdomain ASM.

Some people argue that SSM solves the problem but there is nowadays a demand from customers to be capable to have multicast sessions (both IPv4 and IPv6) with multiple sources (e.g., conferencing) and it is not clear how to achieve this with SSM. While "multiple-source SSM" could potentially be done with the aid of SIP or RTP, this does not exist yet, and a simple solution for ASM is needed."

1.2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

1.3 SSM: no solution needed

In the SSM model, as the channel is defined by the tuple (source address, group address), a collision can only occur if a host would like to be a sender for 2 different groups having the same address.
Therefore, it is sufficient for a sender to choose different addresses for different channels, this is a decision local to the host. This document only considers the ASM model which is a bit more complex.

1.4 Session announcement considerations

This document does not address the session announcement problem. It only answers the question of large scale address assignment of IPv6 multicast addresses. Announcement of the sessions can still be done using web pages, emails, directories, SAP, etc.

2. State of the art for address assignment

MADCAP [2] solves, or could solve, the multicast address assignment problem for both IPv4 and IPv6. However, MADCAP is a fork of DHCP, it has only a couple of implementations which have not been widely deployed. We assume that a mechanism that would be a simple extension to a more widely available mechanism (DHCPv6) could be more deployed.

This proposal and draft-jdurand-ipv6-multicast-ra [14] simplify the assignment architecture since the unicast and multicast address assignment mechanisms become the same. We consider at this stage only IPv6 multicast since most of the key elements used are already defined, and interaction with IPv4 multicast is ensured. If felt needed by the community, this proposal could be extended to IPv4.

3. Assignment with DHCPv6

3.1 New DHCPv6 options

This section introduces new options for IPv6 multicast address assignment with DHCPv6.

3.1.1 IA_MA option for IPv6 Multicast Addresses

RFC 3315 [8] defines the following options for Identity Associations (IA):

- IA_TA option for Temporary Addresses
- IA_TA option for Temporary Addresses

This document introduces a third option: the IA_MA option for IPv6 Multicast Addresses. This option is used to carry an IA_MA, the parameters associated with the IA_MA, and the addresses associated with the IA_MA. The format of the IA_MA option is:
option-code: OPTION_IA_MA (TBD)

option-len: 4 + length of IA_MA-options field

IAID: The unique identifier for this IA_MA; the IAID must be unique among the identifiers for all of this client’s IA_MAs. The number space for IA_MA IAIDs is separate from the number space for IA_NA and IA_TA IAIDs

IA_MA-Options: Options associated with this IA_MA

The IA_MA-options field encapsulates those options that are specific to this IA_MA. For example, all of the IA Address Options carrying the multicast addresses associated with this IA_MA are in the IA_MA-options field.

Each IA_MA carries one "set" of multicast addresses; that is, at most one address per session created by the client requiring an address.

An IA_MA option may only appear in the options area of a DHCP message. A DHCP message may contain multiple IA_MA options. The status of any operations involving this IA_MA is indicated in a Status Code option in the IA_MA-options field.

Note that an IA has no explicit "lifetime" or "lease length" of its own. When the valid lifetimes of all of the addresses in an IA_MA have expired, the IA can be considered as having expired.

An IA_MA option does not include values for T1 and T2 (see RFC 3315 [8]). A client MAY request that the lifetimes of multicast addresses be extended by including the addresses in a IA_MA option sent in a Renew or Rebind message to a server. For example, a client would request an extension on the lifetime of a multicast address to allow an application to continue a multicast session.

The client obtains new multicast addresses by sending an IA_MA option...
with a new IAID to a server. The server will generate new multicast addresses and return them to the client. In case the clients needs to extend the multicast session, it sends a Renew message to the server with the IA_MA and addresses in parameters.

### 3.1.2 Scope Option for IPv6 multicast address

The scope option for IPv6 multicast addresses is used by the clients to request multicast addresses with a certain scope. It is included in the IA address option IAaddr-options field defined in section 22.5 of RFC 3315 [8]. A user can attach more than one scope option for IPv6 multicast address to an IA address option if the client does not know exactly the scope it wants to request but has a set of adequate scope values.

```
<table>
<thead>
<tr>
<th>scope</th>
<th>res</th>
</tr>
</thead>
</table>
```

option-code: OPTION_SCOPE (TBD)

option-len: 1

scope: The scope value for the requested IPv6 multicast address, according to values defined in RFC 3513 [9]

res: This field is reserved for future use. The 4 bits of this field MUST be set to 0, and MUST be ignored on receipt

### 3.2 Address timers

NOTE: There have been some discussions about using some options for the timers. This is left to next releases of the document as this release really focuses on why an assignment based on DHCPv6 has an interest.

The IA address option defined in RFC 3315 [8] contains the following 32 bits fields:

- preferred-lifetime: The preferred lifetime for the IPv6 address in the option, expressed in units of seconds
- valid-lifetime: The valid lifetime for the IPv6 address in the
Internet-Draft    IPv6 multicast address assignment with DHCPv6        February 2005

option, expressed in units of seconds

We suggest to use these fields, usually defined for unicast addresses, for IPv6 multicast addresses, with the definition written above.

The maximum value for these lifetimes is $2^{32}$ seconds or 49710 days equivalent to 136 years. Therefore a host that wants to be assigned an address for a 2 days session occurring in 30 days can request an address with a preferred lifetime value of 32 days. According to the IPv6 multicast addressing space available, servers should allow this type of requests, or at least should permit a certain number of long-term assignment per host. The address is directly assigned by the DHCP server when the request is received. We suggest here not using the parameters \texttt{minDesiredStartTime} and \texttt{maxDesiredStartTime} specified in RFC 2771 [3] which bring too much complexity for the assignment and don’t really make sense for IPv6 where many addresses are available.

3.3 Assignment of a multicast prefix

The assignment of a multicast prefix can be needed in the following scenarios:

- An ISP needs to assign a block of IPv6 multicast address to an enterprise, assigning IPv6 multicast addresses to its hosts. This scenario will most likely occur when DHCPv6 prefix delegation [10] is already used to assign unicast prefixes to the enterprise.

- Also it is most likely that the multicast applications will not support at the beginning the API to request for an IPv6 multicast address via DHCPv6. Then, on startup, or when connected to a new network, a host could ask for an IPv6 multicast prefix. Applications could then choose locally multicast addresses in the prefix assigned to the host.

To fulfill this need, the prefix delegation mechanism described in RFC 3633 [10] is needed also for multicast prefixes. The actual specifications of the IPv6 prefix Options for DHCPv6 do not need to be changed to support multicast prefix delegations. The only thing to keep in mind is that multicast prefix delegation can also occur between a router and a host to fulfill the second requirement mentioned above.

3.4 Client and server behavior

The procedures to request an IPv6 multicast address is more or less the same than the ones described in RFC 3315 [8] to request a
temporary IPv6 address. The differences are following:

- The client uses IA-type IA_MA described above to ask for IPv6 multicast addresses.

- The client SHOULD use the Scope Option in solicit and request messages to tell the server the scope wanted for the IPv6 multicast address requested. It can include more than one Scope Option for IPv6 multicast address per addresses requested in case the client does not know exactly the scope it wants to request but has a set of adequate scope values.

- The client SHOULD specify the lifetimes for every address it wants to be assigned in solicit, request, renew and rebind messages.

- The server MUST assign addresses only if it can assign an address matching one of the scope requested. In case the server can't assign an address with the requested scopes, it must include the Status Code Option NoAddrsAvail in the advertise and reply messages and should include a status message with the scopes that can be assigned by the server and their description.

- If no scope option is specified by the client, the server can assign a multicast address with any scope. It can be a default scope value configured by the DHCP server administrator.

4. Group-ID consideration

RFC 3307 [7] defines guidelines for the choice of IPv6 multicast group identifier (the last 32 bits of the IPv6 multicast address). It specifies that for dynamic IPv6 multicast address allocation, the group-ID MUST be in the range 0x80000000 to 0xFFFFFFF.

5. Deployment scenarios - Case studies

This section gives examples of DHCPv6 deployments for IPv6 multicast address assignment.

5.1 Scenario 1: Site deployment

Consider a site having configured a DHCPv6 server and having one RP for a site-local scope (scope 5). In this simple scenario, the DHCPv6 server can assign the complete set of addresses with a site-local scope.

We have the same scenario if the site configures one RP for global scope with embedded-RP technology. The DHCPv6 server of the site can...
assign the complete set of addresses derived from the RP’s address (see Embedded-RP [11]).

5.2 Scenario 2: Campus deployment

Consider a campus having configured one DHCPv6 server for the entire site, and having several labs (in different subnets) having each a multicast scope for their own usage. Every lab might have for example a scope admin-local (scope 4), and the campus may have the scope site-local (scope 5). The problem of the DHCPv6 server is to assign appropriate addresses to each of the labs.

The server can retrieve information about the location of the client according to the explanation given in section 11 of RFC 3315 [8]. The server can determine this way in which lab the client is and assign adequate addresses. This way a server can assign the same address twice to different clients in different labs.

5.3 Scenario 3: ISP deployment

Consider an ISP providing a global RP service to its customers. The ISP decided to use embedded-RP technology for this RP. Every customers having configured a DHCPv6 server would like to assign IPv6 multicast addresses based on the RP of their ISP. The problem is to avoid overlap between addresses assigned by every DHCPv6 servers.

In this scenario, the ISP having configured an RP would allocate a range of IPv6 multicast addresses based on its RP to every customer having subscribed for the service (as explained in section 5.2 of Embedded-RP [11]). This allocation could be typically hand-off allocation, as it is done between ISP and big customers (not end-users at home) for unicast or could be done with DHCPv6 prefix delegation as explained in this document. This way, every DHCPv6 server is then configured with a different multicast address range, all matching the same RP. This means that ISPs need to allocate IPv6 multicast addresses to their customers, as they do today for IPv6 unicast. Address allocation architectures are exactly the same. Nevertheless, we can note that any customer could deploy its own embedded-RP rather than using the one of its ISP, which simplifies this scenario.

6. Security considerations

The security considerations related to the DHCPv6 protocol are discussed in the security considerations section of [8].
7. Acknowledgement

The author would like to thank Bernard Tuy, Stig Venaas, Christian Strauf, Pekka Savola and Dave Thaler for their good contributions to this memo. The author would also like to thank Ralph Droms who took time to consider the IPv6 multicast assignment problem and introduced the concept of the identity association for IPv6 multicast addresses. The author would also like to thank all the people having worked on the 6NET Deliverable 3.4.3 [12], which was the initial document that raised the complete problematic of IPv6 multicast address assignment.

Pekka Savola, Dave Thaler, Stig Venaas and Bernard Tuy have contributed to better state the problem and mention why the proposal is of interest.

8. Discussions

Here are the current discussions and questions about this document:

- Timers could be specified with a new DHCPv6 option rather than overloading the timers of the address
- If the server cannot assign addresses for the required scopes, it could assign an address in any other scope it is configured for.

9. Changes from -00

- Clarification of the need for the proposal
- The multicast address assignment state of the art is now let to draft-ietf-mboned-addrarch [13].
- IPv6 multicast prefix delegation is now supported by this mechanism, from comments received in IETF 60th.

10. References

10.1 Normative references


10.2 Informative references

[12] 6NET project partners, "6NET D3.4.3 - IPv6 multicast address allocation study", May 2003.


Author’s Address

Jerome Durand
GIP RENATER
151 Bd de l’Hopital
Paris 75013
France

Phone: +33 1 53 94 20 30
EMail: Jerome.Durand@renater.fr
Internet-Draft    IPv6 multicast address assignment with DHCPv6        February 2005

Intellectual Property Statement

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 or might not be available; nor does it represent that it has
made any independent effort to identify any such rights. Information
on the IETF's procedures with respect to rights in IETF 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

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.

Disclaimer of Validity

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.

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.

Acknowledgment

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