MALLOC Working Group
Internet Draft
draft-haberman-malloc-ipv6-prefix-00.txt
February 2000
Expires August 2000

B. Haberma
Nortel Network

Dynamic Allocation Guidelines for Network Prefix-based IPv6 Multicast Addresses

Status of this Memo

Abstract

With the multicast address architecture proposed in [NEW ARCH], a set of guidelines is needed for multicast address allocation servers to use in assigning IPv6 multicast addresses. The purpose of these rules is to reduce the possibility of address collisions on layer 2 devices.

1. 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].

2. Introduction

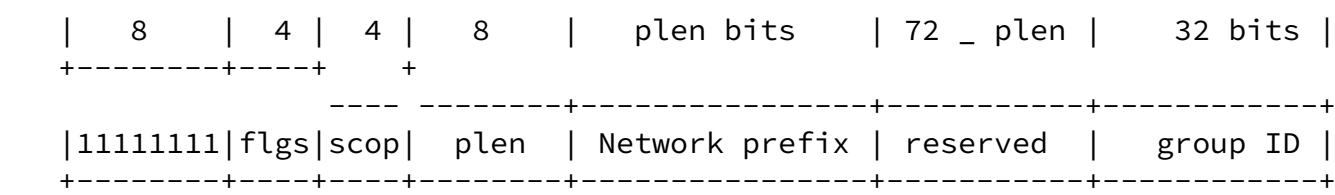
With the multicast address architecture proposed in [NEW ARCH], a set of guidelines is needed for multicast address allocation servers to use in assigning IPv6 multicast addresses. The purpose of these rules is to reduce the possibility of address collisions on layer 2 devices.

These guidelines specify how the lowest 32 bits of the IPv6 multicast address are chosen and assigned. The guidelines specify several mechanisms that can be used to determine the lowest 32 bits of the multicast address. By having several mechanisms of varying complexity, implementers and operators have the flexibility to choose a mechanism that is appropriate for their application.

3. Assignment of New IPv6 Multicast Addresses

The current approach [RFC 2464] to map IPv6 multicast addresses into IEEE 802 MAC addresses takes the low order 32 bits of the IPv6 multicast address and uses it to create a MAC address. Group ID's less than or equal to 32 bits will generate unique MAC addresses.

Due to this, new IPv6 multicast addresses that are network prefix-based have the following format:



The goal of this document is to present several mechanisms implementers and operators can use to select the group ID portion of the address so that the possibility of collisions at the IEEE 802 layer is reduced. The following section presents several different mechanism of varying complexity that can be used to select an appropriate group ID.

4. Group ID Selection Guidelines

The following guidelines assume that the upper 96 bits of the IPv6 multicast address have been set up. The set up of those bits is done in the following manner:

- An IPv6 multicast address prefix is initialized with the appropriate flags and scope fields
- The IPv6 Network Prefix is inserted into the address and the plen field is set. The Network Prefix is obtained from the periodic Router Advertisements.
- The reserved field in the IPv6 multicast address is set to zero

The group ID portion of the address is set using one of the following mechanisms.

4.1 Network Time Protocol (NTP) Rule

The Network Time Protocol [RFC 1305] defines a 64-bit network timestamp. The entity creating the IPv6 multicast address sets the group ID portion of the IPv6 multicast address to the upper 32 bits of the NTP timestamp. In order for a collision to occur at the IEEE 802 layer, two IPv6 multicast address allocations would have to occur at the same second.

4.2 Network Time Protocol and IPv6 Unicast Address

This mechanism adds some complexity to the NTP approach defined above. The entity creating the IPv6 multicast address once again obtains an NTP timestamp. It then logically OR's the upper 32 bits of the NTP timestamp with the lowest 32 bits of its IPv6 link-local address and places that value in the group ID portion of the IPv6 multicast

address. This approach addresses the scenario where two allocating entities allocate addresses in the same second.

4.3 MD5 Digest

In this approach, the group ID is created using the MD5 Message-Digest [RFC 1321]. The 64-bit IPv6 Network Prefix is appended with either the 64-bit NTP timestamp or a 64-bit value created using the guidelines in [RFC 1750]. The corresponding 128-bit value is then fed into MD5. The group ID portion of the IPv6 multicast address is set to the lowest 32 bits of the resulting MD5 digest value.

5. Security Considerations

This document does not have any direct impact on Internet infrastructure security.

6. References

[RFC 2026] S. Bradner, _The Internet Standards Process -- Revision 3_, BCP 9, RFC 2026, October 1996.

[NEW ARCH] B. Haberman, _IP Version 6 Multicast Addressing Architecture_, draft-haberman-ipngwg-mcast-arch-00.txt, December 1999.

[RFC 2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP14, March 1999.

[RFC 2464] M. Crawford, _Transmission of IPv6 Packets over Ethernet Networks_, RFC 2464, December 1998.

[RFC 1305] D. Mills, _Network Time Protocol (Version 3) Specification, Implementation_, RFC 1305, March 1992.

[RFC 1321] R. Rivest, _The MD5 Message-Digest Algorithm_, RFC 1321, April 1992.

[RFC 1750] D. Eastlake, S. Crocker, J. Schiller, _Randomness Recommendations for Security_, RFC 1750, December 1994.

Author's Address

Brian Haberman
Nortel Networks
4309 Emperor Blvd.
Suite 200
Durham, NC 27703
1-919-992-4439
Email : haberman@nortelnetworks.com