Softwire WG
Internet-Draft
Intended status: Standards Track
Expires: August 5, 2017

M. Boucadair
Orange
C. Qin
Cisco
C. Jacquenet
Orange
Y. Lee
Comcast
Q. Wang
China Telecom
February 1, 2017

Delivery of IPv4 Multicast Services to IPv4 Clients over an IPv6 Multicast Network
draft-ietf-softwire-dslite-multicast-17

Abstract

This document specifies a solution for the delivery of IPv4 multicast services to IPv4 clients over an IPv6 multicast network. The solution relies upon a stateless IPv4-in-IPv6 encapsulation scheme and uses an IPv6 multicast distribution tree to deliver IPv4 multicast traffic. The solution is particularly useful for the delivery of multicast service offerings to DS-Lite serviced customers.

Status of This Memo

This Internet-Draft will expire on August 5, 2017.

Copyright Notice

Table of Contents

1. Introduction

DS-Lite [RFC6333] is an IPv4 address-sharing technique that enables operators to multiplex public IPv4 addresses while provisioning only IPv6 to users. A typical DS-Lite scenario is the delivery of an IPv4 service to an IPv4 user over an IPv6 network (denoted as a 4-6-4 scenario). [RFC6333] covers unicast services exclusively.

This document specifies a generic solution for the delivery of IPv4 multicast services to IPv4 clients over an IPv6 multicast network. The solution was developed with DS-Lite in mind (see more discussion below). The solution is however not limited to DS-Lite; it can be applied in other deployment contexts, such as [RFC7596][RFC7597].

If customers have to access IPv4 multicast-based services through a DS-Lite environment, Address Family Transition Router (AFTR) devices will have to process all the Internet Group Management Protocol (IGMP) Report messages [RFC2236] [RFC3376] that have been forwarded by the Customer Premises Equipment (CPE) into the IPv4-in-IPv6 tunnels. From that standpoint, AFTR devices are likely to behave as a replication point for downstream multicast traffic, and the multicast packets will be replicated for each tunnel endpoint that IPv4 receivers are connected to.

This kind of DS-Lite environment raises two major issues:

1. The IPv6 network loses the benefits of the multicast traffic forwarding efficiency because it is unable to deterministically replicate the data as close to the receivers as possible. As a consequence, the downstream bandwidth in the IPv6 network will be vastly consumed by sending multicast data over a unicast infrastructure.

2. The AFTR is responsible for replicating multicast traffic and forwarding it into each tunnel endpoint connecting IPv4 receivers

that have explicitly asked for the corresponding contents. This process may significantly consume the AFTR's resources and overload the AFTR.

This document specifies an extension to the DS-Lite model to deliver IPv4 multicast services to IPv4 clients over an IPv6 multicast-enabled network.

This document describes a stateless translation mechanism that supports either Source Specific Multicast (SSM) or Any Source Multicast (ASM) operation. The recommendation in Section 1 of [RFC4607] is that multicast services use SSM where possible; the operation of the translation mechanism is also simplified when SSM is used, e.g., considerations for placement of the IPv6 the Rendezvous Point (RP) are no longer relevant.

1.1. Requirements Language

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 [RFC2119].

2. Terminology

This document makes use of the following terms:

IPv4-embedded IPv6 address: an IPv6 address which embeds a 32-bit-encoded IPv4 address. An IPv4-embedded IPv6 address can be unicast or multicast.

mPrefix64: a dedicated multicast IPv6 prefix for constructing IPv4-embedded IPv6 multicast addresses. mPrefix64 can be of two types: ASM_mPrefix64 used in Any Source Multicast (ASM) mode or SSM_mPrefix64 used in Source Specific Multicast (SSM) mode [RFC4607]. The size of this prefix is /96.

> Note: "64" is used as an abbreviation for IPv6-IPv4 interconnection.

uPrefix64: a dedicated IPv6 unicast prefix for constructing IPv4-embedded IPv6 unicast addresses [RFC6052]. This prefix may be either the Well-Known Prefix (i.e., 64:ff9b::/96) or a Network-Specific Prefix (NSP).

Multicast AFTR (mAFTR): a functional entity which supports an IPv4-IPv6 multicast interworking function (refer to Figure 3). It receives and encapsulates the IPv4 multicast packets into IPv4-in-

IPv6 packets. Also, it behaves as the corresponding IPv6 multicast source for the encapsulated IPv4-in-IPv6 packets.

Multicast Basic Bridging BroadBand (mB4): a functional entity which supports an IGMP-MLD interworking function (refer to Section 6.1) that translates the IGMP messages into the corresponding Multicast Listener Discovery (MLD) messages, and sends the MLD messages to the IPv6 network. In addition, the mB4 decapsulates IPv4-in-IPv6 multicast packets.

PIMv4: refers to Protocol Independent Multicast (PIM) when deployed in an IPv4 infrastructure (i.e., IPv4 transport capabilities are used to exchange PIM messages).

PIMv6: refers to PIM when deployed in an IPv6 infrastructure (i.e., IPv6 transport capabilities are used to exchange PIM messages).

Host portion of the MLD protocol: refers to the part of MLD that applies to all multicast address listeners (Section 6 of [RFC3810]). As a reminder, MLD specifies separate behaviors for multicast address listeners (i.e., hosts or routers that listen to multicast packets) and multicast routers.

Router portion of the IGMP protocol: refers to the part of IGMP that is performed by multicast routers (Section 6 of [RFC3376]).

DR: refers to the Designated Router as defined in [RFC7761].

3. Scope

This document focuses only on the subscription to IPv4 multicast groups and the delivery of IPv4-formatted content to IPv4 receivers over an IPv6-only network. In particular, only the following case is covered:

> IPv4 receivers access IPv4 multicast contents over IPv6-only multicast-enabled networks.

This document does not cover the source/receiver heuristics, where IPv4 receivers can also behave as IPv4 multicast sources. This document assumes that hosts behind the mB4 are IPv4 multicast receivers only. Also, the document covers host built-in mB4 function.

4. Solution Overview

In the DS-Lite specification [RFC6333], an IPv4-in-IPv6 tunnel is used to carry bidirectional IPv4 unicast traffic between a B4 and an AFTR. The solution specified in this document provides an IPv4-in-IPv6 encapsulation scheme to deliver unidirectional IPv4 multicast traffic from an mAFTR to an mB4.

An overview of the solution is provided in this section which is intended as an introduction to how it works, but is not normative. For the normative specifications of the two new functional elements: mB4 and mAFTR (Figure 1), refer to Sections 6 and 7.

```
                            ------------
                          /              \
                         |  IPv4 network  |
                          \              /
                            ------------
              IPv4 multicast  :   |   ^  PIMv4 Join
                              v   |   :
                           +-------------+
                           |    mAFTR    |
                           +-------------+
             IPv6 multicast  |:|  |   ^  PIMv6 Join (PIMv6
             (IPv4 embedded) |:|  |   :   routers in between)
                            ------------
                          /              \
                         |  IPv6 network  |
                          \              /
                            ------------
                             |:|  |   ^  MLD Report
                             |v|  |   :
                            +-----------+
                            |    mB4    |
                            +-----------+
              IPv4 multicast  :   |   ^  IGMP Report
                              v   |   :
                            +-----------+
                            |   IPv4    |
                            | receiver  |
                            +-----------+
```

Figure 1: Functional Architecture

4.1. IPv4-Embedded IPv6 Prefixes

In order to map the addresses of IPv4 multicast traffic with IPv6 multicast addresses, an IPv6 multicast prefix (mPrefix64) and an IPv6 unicast prefix (uPrefix64) are provided to the mAFTR and the mB4 elements, both of which contribute to the computation and the maintenance of the IPv6 multicast distribution tree that extends the IPv4 multicast distribution tree into the IPv6 multicast network. The IPv4/IPv6 address mapping is stateless.

The mAFTR and the mB4 use mPrefix64 to convert an IPv4 multicast address (G4) into an IPv4-embedded IPv6 multicast address (G6). The mAFTR and the mB4 use uPrefix64 to convert an IPv4 source address (S4) into an IPv4-embedded IPv6 address (S6). The mAFTR and the mB4 must use the same mPrefix64 and uPrefix64, and also run the same algorithm for building IPv4-embedded IPv6 addresses. Refer to Section 5 for more details about the address mapping.

4.2. Multicast Distribution Tree Computation

When an IPv4 receiver connected to the device that embeds the mB4 capability wants to subscribe to an IPv4 multicast group, it sends an IGMP Report message towards the mB4. The mB4 creates the IPv6 multicast group (G6) address using mPrefix64 and the original IPv4 multicast group address. If the receiver sends a source-specific IGMPv3 Report message, the mB4 will create the IPv6 source address (S6) using uPrefix64 and the original IPv4 source address.

The mB4 uses the G6 (and both S6 and G6 in SSM) to create the corresponding MLD Report message. The mB4 sends the Report message towards the IPv6 network. The PIMv6 Designated Router receives the MLD Report message and sends the PIMv6 Join message to join the IPv6 multicast distribution tree. It can send either PIMv6 Join (*,G6) in ASM or PIMv6 Join (S6,G6) in SSM to the mAFTR.

The mAFTR acts as the IPv6 DR to which the uPrefix64-derived S6 is connected. The mAFTR will receive the source-specific PIMv6 Join message (S6,G6) from the IPv6 multicast network. If the mAFTR is the Rendezvous Point (RP) of G6, it will receive the any-source PIMv6 Join message (*,G6) from the IPv6 multicast network. If the mAFTR is not the RP of G6, it will send the PIM Register message to the RP of G6 located in the IPv6 multicast network. For the sake of simplicity, it is recommended to configure the mAFTR as the RP for the IPv4-embedded IPv6 multicast groups it manages; no registration procedure is required under this configuration.

When the mAFTR receives the PIMv6 Join message (*,G6), it will extract the IPv4 multicast group address (G4). If the mAFTR is the

RP of G4 in the IPv4 multicast network, it will create a (*,G4) entry (if such entry does not already exist) in its own IPv4 multicast routing table. If the mAFTR is not the RP of G4, it will send the corresponding PIMv4 Join message (*,G4) towards the RP of G4 in the IPv4 multicast network.

When the mAFTR receives the PIMv6 Join message (S6,G6), it will extract the IPv4 multicast group address (G4) and IPv4 source address (S4) and send the corresponding (S4,G4) PIMv4 Join message directly to the IPv4 source.

A branch of the multicast distribution tree is thus constructed, comprising both an IPv4 part (from the mAFTR upstream) and an IPv6 part (from mAFTR downstream towards the mB4).

The mAFTR advertises the route of uPrefix64 with an IPv6 Interior Gateway Protocol (IGP), so as to represent the IPv4-embedded IPv6 source in the IPv6 multicast network, and to allow IPv6 routers to run the Reverse Path Forwarding (RPF) check procedure on incoming multicast traffic. Injecting internal /96 routes is not problematic given the recommendation in [RFC7608] that requires that forwarding processes must be designed to process prefixes of any length up to /128.

4.3. Multicast Data Forwarding

When the mAFTR receives an IPv4 multicast packet, it will encapsulate the packet into an IPv6 multicast packet using the IPv4-embedded IPv6 multicast address as the destination address and an IPv4-embedded IPv6 unicast address as the source address. The encapsulated IPv6 multicast packet will be forwarded down the IPv6 multicast distribution tree and the mB4 will eventually receive the packet.

The IPv6 multicast network treats the IPv4-in-IPv6 encapsulated multicast packets as native IPv6 multicast packets. The IPv6 multicast routers use the outer IPv6 header to make their forwarding decisions.

When the mB4 receives the IPv6 multicast packet (to G6) derived by mPrefix64, it decapsulates it and forwards the original IPv4 multicast packet to the receivers subscribing to G4.

Note: At this point, only IPv4-in-IPv6 encapsulation is defined; however, other types of encapsulation could be defined in the future.

5. IPv4/IPv6 Address Mapping

5.1. Prefix Assignment

A dedicated IPv6 multicast prefix (mPrefix64) is provisioned to the mAFTR and the mB4. The mAFTR and the mB4 use the mPrefix64 to form an IPv6 multicast group address from an IPv4 multicast group address. The mPrefix64 can be of two types: ASM_mPrefix64 (a mPrefix64 used in ASM mode) or SSM_mPrefix64 (a mPrefix64 used in SSM mode). The mPrefix64 MUST be derived from the corresponding IPv6 multicast address space (e.g., the SSM_mPrefix64 must be in the range of multicast address space specified in [RFC4607]).

The IPv6 part of the multicast distribution tree can be seen as an extension of the IPv4 part of the multicast distribution tree. The IPv4 source address MUST be mapped to an IPv6 source address. An IPv6 unicast prefix (uPrefix64) is provisioned to the mAFTR and the mB4. The mAFTR and the mB4 use the uPrefix64 to form an IPv6 source address from an IPv4 source address as specified in [RFC6052]. The uPrefix-formed IPv6 source address will represent the original IPv4 source in the IPv6 multicast network. The uPrefix64 MUST be derived from the IPv6 unicast address space.

The multicast address translation MUST follow the algorithm defined in Section 5.2.

The mPrefix64 and uPrefix64 can be configured in the mB4 using a variety of methods, including an out-of-band mechanism, manual configuration, or a dedicated provisioning protocol (e.g., using DHCPv6 [I-D.ietf-softwire-multicast-prefix-option]).

The stateless translation mechanism described in Section 5 does not preclude use of Embedded-RP [RFC3956][RFC7371].

5.2. Multicast Address Translation Algorithm

IPv4-embedded IPv6 multicast addresses are composed according to the following algorithm:

- Concatenate the mPrefix64 96 bits and the 32 bits of the IPv4 address to obtain a 128-bit address.

The IPv4 multicast addresses are extracted from the IPv4-embedded IPv6 multicast addresses according to the following algorithm:

- If the multicast address has a pre-configured mPrefix64, extract the last 32 bits of the IPv6 multicast address.

An IPv4 source is represented in the IPv6 realm with its IPv4-converted IPv6 address [RFC6052].

5.3. Textual Representation

The embedded IPv4 address in an IPv6 multicast address is included in the last 32 bits; therefore, dotted decimal notation can be used.

5.4. Examples

Group address mapping example:

mPrefix64	IPv4 address	IPv4-Embedded IPv6 address
ff0x::db8:0:0/96	233.252.0.1	ff0x::db8:233.252.0.1

Source address mapping example when a /96 is used:

uPrefix64	IPv4 address	IPv4-Embedded IPv6 address
2001:db8::/96	192.0.2.33	2001:db8::192.0.2.33

IPv4 and IPv6 addresses used in this example are derived from the IPv4 and IPv6 blocks reserved for documentation, as per [RFC6676]. The unicast IPv4 address of the above example is derived from the documentation address block defined in [RFC6890].

6. Multicast B4 (mB4)

6.1. IGMP-MLD Interworking Function

The IGMP-MLD Interworking Function combines the IGMP/MLD Proxying function and the address synthesizing operations. The IGMP/MLD Proxying function is specified in [RFC4605]. The address translation is stateless and MUST follow the address mapping specified in Section 5.

The mB4 performs the host portion of the MLD protocol on the upstream interface. The composition of IPv6 membership in this context is constructed through address synthesizing operations and MUST synchronize with the membership database maintained in the IGMP domain. MLD messages are sent natively to the directly connected IPv6 multicast routers (it will be processed by the PIM DR). The mB4 also performs the router portion of the IGMP protocol on the downstream interface(s). Refer to [RFC4605] for more details.

```
         +----------+   IGMP  +-------+   MLD   +---------+
         |   IPv4   |---------|  mB4  |---------|   PIM   |
         | Receiver |         |       |         |    DR   |
         +----------+         +-------+         +---------+
```

Figure 2: IGMP-MLD Interworking

If SSM is deployed, the mB4 MUST construct the IPv6 source address (or retrieve the IPv4 source address) using the uPrefix64. The mB4 MAY create a membership database which associates the IPv4-IPv6 multicast groups with the interfaces (e.g., WLAN and Wired Ethernet) facing IPv4 multicast receivers.

6.2. Multicast Data Forwarding

When the mB4 receives an IPv6 multicast packet, it MUST check the group address and the source address. If the IPv6 multicast group prefix is mPrefix64 and the IPv6 source prefix is uPrefix64, the mB4 MUST decapsulate the IPv6 header [RFC2473]; the decapsulated IPv4 multicast packet will be forwarded through each relevant interface following standard IPv4 multicast forwarding procedure. Otherwise, the mB4 MUST silently drop the packet.

As an illustration, if a packet is received from source 2001:db8::192.0.2.33 and needs to be forwarded to group ff3x:20:2001:db8::233.252.0.1, the mB4 decapsulates it into an IPv4 multicast packet using 192.0.2.33 as the IPv4 source address and using 233.252.0.1 as the IPv4 destination multicast group.

6.3. Fragmentation

Encapsulating IPv4 multicast packets into IPv6 multicast packets that will be forwarded by the mAFTR towards the mB4 along the IPv6 multicast distribution tree reduces the effective MTU size by the size of an IPv6 header. In this specification, the data flow is unidirectional from the mAFTR to the mB4. The mAFTR MUST fragment the oversized IPv6 packet after the encapsulation into two IPv6 packets. The mB4 MUST reassemble the IPv6 packets, decapsulate the IPv6 header, and forward the IPv4 packet to the hosts that have subscribed to the corresponding multicast group. Further considerations about fragmentation issues are documented in [RFC6333].

6.4. Host Built-in mB4 Function

If the mB4 function is implemented in the host which is directly connected to an IPv6-only network, the host MUST implement the behaviors specified in Sections 6.1, 6.2, and 6.3. The host MAY optimize the implementation to provide an Application Programming Interface (API) or kernel module to skip the IGMP-MLD Interworking Function. Optimization considerations are out of scope of this specification.

6.5. Preserve the Scope

When several mPrefix64s are available, if each enclosed IPv4-embedded IPv6 multicast prefix has a distinct scope, the mB4 MUST select the appropriate IPv4-embedded IPv6 multicast prefix whose scope matches the IPv4 multicast address used to synthesize an IPv4-embedded IPv6 multicast address (Section 8 of [RFC2365]).

The mB4 MAY be configured to not preserve the scope when enforcing the address translation algorithm.

Consider that an mB4 is configured with two mPrefix64s ff0e::db8:0:0/96 (Global scope) and ff08::db8:0:0/96 (Organization scope). If the mB4 receives an IGMP report from an IPv4 receiver to subscribe to 233.252.0.1, it checks which mPrefix64 to use in order to preserve the scope of the requested IPv4 multicast group. In this example, given that 233.252.0.1 is intended for global use, the mB4 creates the IPv6 multicast group (G6) address using ff0e::db8:0:0/96 and the original IPv4 multicast group address (233.252.0.1): ff0e::db8:233.252.0.1.

7. Multicast AFTR (mAFTR)

7.1. Routing Considerations

The mAFTR is responsible for interconnecting the IPv4 multicast distribution tree with the corresponding IPv6 multicast distribution tree. The mAFTR MUST use the uPrefix64 to build the IPv6 source addresses of the multicast group address derived from mPrefix64. In other words, the mAFTR MUST be the multicast source whose address is derived from uPrefix64.

The mAFTR MUST advertise the route towards uPrefix64 with the IPv6 IGP. This is needed by the IPv6 multicast routers so that they acquire the routing information to discover the source.

7.2. Processing PIM Messages

The mAFTR MUST interwork PIM Join/Prune messages for (*,G6) and (S6,G6) on their corresponding (*,G4) and (S4,G4). The following text specifies the expected behavior of the mAFTR for PIM Join messages.

```
                       +---------+
              ---------|  mAFTR  |---------
                PIMv6  |uPrefix64|  PIMv4
                       |mPrefix64|
                       +---------+
```

Figure 3: PIMv6-PIMv4 Interworking Function

The mAFTR contains two separate Tree Information Bases (TIBs): the IPv4 Tree Information Base (TIB4) and the IPv6 Tree Information Base (TIB6), which are bridged by one IPv4-in-IPv6 virtual interface. It should be noted that TIB implementations may vary (e.g., some may rely upon a single integrated TIB without any virtual interface), but they should follow this specification for the sake of global and functional consistency.

When an mAFTR receives a PIMv6 Join message (*,G6) with an IPv6 multicast group address (G6) that is derived from the mPrefix64, it MUST check its IPv6 Tree Information Base (TIB6). If there is an entry for this G6 address, it MUST check whether the interface through which the PIMv6 Join message has been received is in the outgoing interface (oif) list. If not, the mAFTR MUST add the interface to the oif list. If there is no entry in the TIB6, the mAFTR MUST create a new entry (*,G6) for the multicast group. Whether or not the IPv4-in-IPv6 virtual interface is set as the incoming interface of the newly created entry is up to the implementation but it should comply with the mAFTR's multicast data forwarding behavior, see Section 7.4.

The mAFTR MUST extract the IPv4 multicast group address (G4) from the IPv4-embedded IPv6 multicast address (G6) contained in the PIMv6 Join message. The mAFTR MUST check its IPv4 Tree Information Base (TIB4). If there is an entry for G4, it MUST check whether the IPv4-in-IPv6 virtual interface is in the outgoing interface list. If not, the mAFTR MUST add the interface to the oif list. If there is no entry for G4, the mAFTR MUST create a new (*,G4) entry in its TIB4 and initiate the procedure for building the shared tree in the IPv4 multicast network without any additional requirement.

If the mAFTR receives a source-specific Join message, the (S6,G6) is processed rather than (*,G6). The procedures of processing (S6,G6) and (*,G6) are almost the same. Differences have been detailed in [RFC7761].

7.3. Switching from Shared Tree to Shortest Path Tree

When the mAFTR receives the first IPv4 multicast packet, it may extract the source address (S4) from the packet and send an Explicit PIMv4 (S4,G4) Join message directly to S4. The mAFTR switches from the shared Rendezvous Point Tree (RPT) to the Shortest Path Tree (SPT) for G4.

For IPv6 multicast routers to switch to the SPT, there is no new requirement. IPv6 multicast routers may send an Explicit PIMv6 Join to the mAFTR once the first (S6,G6) multicast packet arrives from upstream multicast routers.

7.4. Multicast Data Forwarding

When the mAFTR receives an IPv4 multicast packet, it checks its TIB4 to find a matching entry and then forwards the packet to the interface(s) listed in the outgoing interface list. If the IPv4-in-IPv6 virtual interface also belongs to this list, the packet is encapsulated with the mPrefix64-derived and uPrefix64-derived IPv4-embedded IPv6 addresses to form an IPv6 multicast packet [RFC2473]. Then another lookup is made by the mAFTR to find a matching entry in the TIB6. Whether the RPF check for the second lookup is performed or not is up to the implementation and is out of the scope of this document. The IPv6 multicast packet is then forwarded along the IPv6 multicast distribution tree, based upon the outgoing interface list of the matching entry in the TIB6.

As an illustration, if a packet is received from source 192.0.2.33 and needs to be forwarded to group 233.252.0.1, the mAFTR encapsulates it into an IPv6 multicast packet using ff3x:20:2001:db8::233.252.0.1 as the IPv6 destination multicast group and using 2001:db8::192.0.2.33 as the IPv6 source address.

7.5. Scope

The Scope field of IPv4-in-IPv6 multicast addresses should be valued accordingly (e.g, to "E" for Global scope) in the deployment environment. This specification does not discuss the scope value that should be used.

Nevertheless, when several mPrefix64s are available, if each enclosed IPv4-embedded IPv6 multicast prefix has a distinct scope, the mAFTR MUST select the appropriate IPv4-embedded IPv6 multicast prefix whose scope matches the IPv4 multicast address used to synthesize an IPv4-embedded IPv6 multicast address.

An mAFTR MAY be configured to not preserve the scope when enforcing the address translation algorithm.

8. Deployment Considerations

8.1. Other Operational Modes

8.1.1. The IPv6 DR is Co-Located with the mAFTR

The mAFTR can embed the MLD Querier function (as well as the PIMv6 DR) for optimization purposes. When the mB4 sends a MLD Report message to this mAFTR, the mAFTR should process the MLD Report message that contains the IPv4-embedded IPv6 multicast group address and then send the corresponding PIMv4 Join message (Figure 4).

```
                         +---------+
                ---------|  mAFTR  |---------
                   MLD   |uPrefix64|  PIMv4
                         |mPrefix64|
                         +---------+
```

Figure 4: MLD-PIMv4 Interworking Function

Discussions about the location of the mAFTR capability and related ASM or SSM multicast design considerations are out of the scope of this document.

8.1.2. The IPv4 DR is Co-Located with the mAFTR

If the mAFTR is co-located with the IPv4 DR connected to the original IPv4 source, it may simply use the uPrefix64 and mPrefix64 prefixes to build the IPv4-embedded IPv6 multicast packets, and the sending of PIMv4 Join messages becomes unnecessary.

8.2. Load Balancing

For robustness and load distribution purposes, several nodes in the network can embed the mAFTR function. In such case, the same IPv6 prefixes (i.e., mPrefix64 and uPrefix64) and algorithm to build IPv4-embedded IPv6 addresses must be configured on those nodes.

8.3. mAFTR Policy Configuration

The mAFTR may be configured with a list of IPv4 multicast groups and sources. Only multicast flows bound to the configured addresses should be handled by the mAFTR. Otherwise, packets are silently dropped.

8.4. Static vs. Dynamic PIM Triggering

To optimize the usage of network resources in current deployments, all multicast streams are conveyed in the core network while only the most popular ones are forwarded in the aggregation/access networks (static mode). Less popular streams are forwarded in the access network upon request (dynamic mode). Depending on the location of the mAFTR in the network, two modes can be envisaged: static and dynamic.

Static Mode: the mAFTR is configured to instantiate permanent (S6,G6) and (*,G6) entries in its TIB6 using a pre-configured (S4,G4) list.

Dynamic Mode: the instantiation or withdrawal of (S6,G6) or (*,G6) entries is triggered by the receipt of PIMv6 messages.

9. Security Considerations

Besides multicast scoping considerations (see Section 6.5 and Section 7.5), this document does not introduce any new security concern in addition to what is discussed in Section 5 of [RFC6052], Section 10 of [RFC3810] and Section 6 of [RFC7761].

Unlike solutions that map IPv4 multicast flows to IPv6 unicast flows, this document does not exacerbate Denial-of-Service (DoS) attacks.

An mB4 SHOULD be provided with appropriate configuration information to preserve the scope of a multicast message when mapping an IPv4 multicast address into an IPv4-embedded IPv6 multicast address and vice versa.

9.1. Firewall Configuration

The CPE that embeds the mB4 function SHOULD be configured to accept incoming MLD messages and traffic forwarded to multicast groups subscribed by receivers located in the customer premises.

10. Acknowledgments

The authors would like to thank Dan Wing for his guidance in the early discussions which initiated this work. We also thank Peng Sun, Jie Hu, Qiong Sun, Lizhong Jin, Alain Durand, Dean Cheng, Behcet Sarikaya, Tina Tsou, Rajiv Asati, Xiaohong Deng, and Stig Venaas for their valuable comments.

Many thanks to Ian Farrer for the review.

Thanks to Zhen Cao, Tim Chown, Francis Dupont, Jouni Korhonen, and Stig Venaas for the directorates review.

11. IANA Considerations

This document includes no request to IANA.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2365] Meyer, D., "Administratively Scoped IP Multicast", BCP 23, RFC 2365, DOI 10.17487/RFC2365, July 1998, <http://www.rfc-editor.org/info/rfc2365>.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, DOI 10.17487/RFC2473, December 1998, <http://www.rfc-editor.org/info/rfc2473>.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, DOI 10.17487/RFC3376, October 2002, <http://www.rfc-editor.org/info/rfc3376>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <http://www.rfc-editor.org/info/rfc3810>.

[RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, DOI 10.17487/RFC4605, August 2006, <http://www.rfc-editor.org/info/rfc4605>.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, DOI 10.17487/RFC4607, August 2006, <http://www.rfc-editor.org/info/rfc4607>.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <http://www.rfc-editor.org/info/rfc6052>.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix Length Recommendation for Forwarding", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015, <http://www.rfc-editor.org/info/rfc7608>.

[RFC7761] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., Parekh, R., Zhang, Z., and L. Zheng, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", STD 83, RFC 7761, DOI 10.17487/RFC7761, March 2016, <http://www.rfc-editor.org/info/rfc7761>.

12.2. Informative References

[I-D.ietf-softwire-multicast-prefix-option] Boucadair, M., Qin, J., Tsou, T., and X. Deng, "DHCPv6 Option for IPv4-Embedded Multicast and Unicast IPv6 Prefixes", draft-ietf-softwire-multicast-prefix-option-12 (work in progress), January 2017.

[RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, DOI 10.17487/RFC2236, November 1997, <http://www.rfc-editor.org/info/rfc2236>.

[RFC3956] Savola, P. and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", RFC 3956, DOI 10.17487/RFC3956, November 2004, <http://www.rfc-editor.org/info/rfc3956>.

[RFC6676] Venaas, S., Parekh, R., Van de Velde, G., Chown, T., and M. Eubanks, "Multicast Addresses for Documentation", RFC 6676, DOI 10.17487/RFC6676, August 2012, <http://www.rfc-editor.org/info/rfc6676>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <http://www.rfc-editor.org/info/rfc6890>.

[RFC7371] Boucadair, M. and S. Venaas, "Updates to the IPv6 Multicast Addressing Architecture", RFC 7371, DOI 10.17487/RFC7371, September 2014, <http://www.rfc-editor.org/info/rfc7371>.

[RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596, July 2015, <http://www.rfc-editor.org/info/rfc7596>.

[RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <http://www.rfc-editor.org/info/rfc7597>.

Appendix A. Use Case: IPTV

IPTV generally includes two categories of service offerings:

- Video on Demand (VoD) that unicast video content to receivers.

- Multicast live TV broadcast services.

Two types of provider are involved in the delivery of this service:

- Content Providers, who usually own the contents that is multicast to receivers. Content providers may contractually define an agreement with network providers to deliver contents to receivers.

- Network Providers, who provide network connectivity services (e.g., network providers are responsible for carrying multicast flows from head-ends to receivers).

Note that some contract agreements prevent a network provider from altering the content as sent by the content provider for various reasons. Depending on these contract agreements, multicast streams should be delivered unaltered to the requesting users.

Many current IPTV contents are likely to remain IPv4-formatted and out of control of the network providers. Additionally, there are numerous legacy receivers (e.g., IPv4-only Set Top Boxes (STB)) that can't be upgraded or be easily replaced to support IPv6. As a consequence, IPv4 service continuity must be guaranteed during the transition period, including the delivery of multicast services such as Live TV Broadcasting to users.

Appendix B. Older Versions of Group Membership Management Protocols

Given the multiple versions of group membership management protocols, mismatch issues may arise at the mB4 (refer to Section 6.1).

If IGMPv2 operates on the IPv4 receivers while MLDv2 operates on the MLD Querier, or if IGMPv3 operates on the IPv4 receivers while MLDv1 operates on the MLD Querier, the version mismatch issue will be encountered. To solve this problem, the mB4 should perform the router portion of IGMP which is similar to the corresponding MLD version (IGMPv2 as of MLDv1, or IGMPv3 as of MLDv2) operating in the IPv6 domain. Then, the protocol interaction approach specified in Section 7 of [RFC3376] can be applied to exchange signaling messages with the IPv4 receivers on which the different version of IGMP is operating.

Note that the support of IPv4 SSM requires to enable MLDv2 in the IPv6 network.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Chao Qin
Cisco
Shanghai
P.R. China

Email: jacni@jacni.com

Christian Jacquenet
Orange
Rennes 35000
France

Email: christian.jacquenet@orange.com

Yiu L. Lee
Comcast
United States of America

Email: yiu_lee@cable.comcast.com
URI: http://www.comcast.com

Qian Wang
China Telecom
P.R. China

Phone: +86 10 58502462
Email: 13301168516@189.cn