MBONED Working Group
Internet-Draft
Intended status: Informational
Expires: December 07, 2013

C. Jacquenet
M. Boucadair
France Telecom Orange
Y. Lee
Comcast
J. Qin
Cisco Systems
T. Tsou
Huawei Technologies (USA)
Q. Sun
China Telecom
June 05, 2013

IPv4-IPv6 Multicast: Problem Statement and Use Cases
draft-ietf-mboned-v4v6-mcast-ps-03

Abstract

This document discusses issues and requirements raised by IPv4-IPv6 multicast interconnection and co-existence scenarios. It also discusses various multicast use cases which may occur during IPv6 transitioning.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 07, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
1.1. Terminology 4
1.2. Organization of the Document 4
2. Scope and Service Requirements 5
2.1. Scope 5
2.2. Service Requirements 5
3. Use Cases 6
3.1. IPv4 Receiver and Source Connected to an IPv6-Only Network 7
3.2. IPv6 Receiver and Source Connected to an IPv4-Only Network 9
3.3. IPv6 Receiver and IPv4 Source 10
3.4. IPv4 Receiver and IPv6 Source 11
3.5. Summary 13
4. Design Requirements 13
4.1. Group and Source Discovery Considerations 13
4.2. Subscription 14
4.3. Multicast Tree Computation 14
4.4. Multicast Adaptation Functions (AF) 14
4.4.1. AF For Control Flows 15
4.4.2. AF For Data Flows 16
4.4.3. Address Mapping 16
4.5. Combination of ASM and SSM Modes 17
5. IANA Considerations 17
6. Security Considerations 17
7. Acknowledgments 17
8. References 18
8.1. Normative References 18
8.2. Informative References 18
Authors' Addresses 18

1. Introduction

Global IPv4 address depletion inevitably challenges service providers who must guarantee IPv4 service continuity during the forthcoming transition period. In particular, access to IPv4 contents that are multicast to IPv4 receivers becomes an issue when the forwarding of multicast data assumes the use of global IPv4 addresses.

The rarefaction of global IPv4 addresses may indeed affect the multicast delivery of IPv4-formatted contents to IPv4 receivers. For example, the observed evolution of ADSL broadband access infrastructures from a service-specific, multi-PVC (Permanent Virtual Circuit) scheme towards a "service-agnostic", single PVC scheme, assumes the allocation of a globally unique IPv4 address on the WAN (Wide Area Network) interface of the CPE (Customer Premises Equipment), or to a mobile terminal), whatever the number and the nature of the services the customer has subscribed to.

Likewise, the global IPv4 address depletion encourages the development of IPv6 receivers while contents may very well remain IPv4-formatted. There is therefore a need to make sure such IPv6 receivers can access IPv4-formatted contents during the transition period.

During the transition period, the usage of the remaining global IPv4 address blocks will have to be rationalized for the sake of IPv4 service continuity. The current state-of-the-art suggests the introduction of NAT (Network Address Translation) capabilities (generally denoted as CGN, for Carrier-Grade NAT) in providers' networks, so that a global IPv4 address will be shared between several customers.

As a consequence, CPE or mobile UE (User Equipment) devices will no longer be assigned a dedicated global IPv4 address anymore, and IPv4 traffic will be privately-addressed until it reaches one of the CGN capabilities deployed in the network. From a multicast delivery standpoint, this situation suggests the following considerations:

- The current design of some multicast-based services like TV broadcasting often relies upon the use of a private IPv4 addressing scheme because of a walled garden approach. Privately-addressed IGMP [RFC2236][RFC3376] traffic sent by IPv4 receivers is generally forwarded over a specific (e.g., "IPTV") PVC towards an IGMP Querier located in the access infrastructure, e.g., in some deployments it is hosted by a BRAS (BRoadband Access Server) device that is the PPP (Point-to-Point Protocol) session endpoint and which may also act as a PIM DR (Protocol Independent Multicast Designated Router)[RFC4601]. This design does not suffer from global IPv4 address depletion by definition (since multicast traffic relies upon the use of a private IPv4 addressing scheme), but it is inconsistent with migrating the access infrastructure towards a publicly-addressed single PVC design scheme.

- Likewise, other deployments (e.g., cable operators' environments) rely upon the public CPE's address for multicast delivery and will therefore suffer from IPv4 address depletion.

- The progressive introduction of IPv6 as the only perennial solution to global IPv4 address depletion does not necessarily assume that multicast-based IPv4 services will be migrated accordingly. Access to IPv4 multicast contents when no global IPv4 address can be assigned to a customer raises several issues: (1) The completion of the IGMP-based multicast group subscription procedure, (2) The computation of the IPv4 multicast distribution tree, and (3) The IPv4-inferred addressing scheme to be used in a networking environment which will progressively become IPv6-enabled.

This document does not make any assumption on the techniques used for the delivery of multicast traffic (e.g., native IP multicast with or without traffic isolation features, etc.)

This document elaborates on the context and discusses multicast-related issues and requirements.

1.1. Terminology

This document uses the following terms:

- Multicast Source: Source of contents that are multicast to receivers. A video streaming server is an example of such source.

- Multicast Receiver: Receiver, in short. A Set Top Box (STB) is an example of such receiver.

- Multicast Delivery Network: Network in short, covers the realm from First Hop Routers that are directly connected to sources to IGMP/MLD (Internet Group Management Protocol/Multicast Listener Discovery) Querier devices that process IGMP/MLD signalling traffic exchanged with receivers.

1.2. Organization of the Document

This document is organized as follows:

- Section 2 details basic requirements that should be addressed by providers involved in the delivery of multicast-based services during the transition period,

- Section 3 discusses several use cases that reflect issues raised by the forthcoming transition period,

- Section 4 details design considerations.

2. Scope and Service Requirements

2.1. Scope

Intra-domain only: The delivery of multicast services such as live TV broadcasting often relies upon walled garden designs that restrict the scope to the domain where such services can be subscribed. As a consequence, considerations about inter-domain multicast are out of the scope of this document.

Multicast-enabled networks only: This document assumes that the network is IP multicast-enabled. That is, whatever the IP address family of the content, this content will be multicast along distribution trees that should be terminated as close to the receivers as possible for the sake of bandwidth optimization. In other words, considerations about forwarding multicast traffic over unicast-only (access) networks are out of the scope of this document.

Multicast to the receivers, not from the receivers: This document only covers the case where multicast traffic is forwarded by the service provider network to the receivers. The draft does not consider multicast services that assume a source/receiver heuristic, e.g., videoconferencing services. The draft primarily focuses on residential multicast-based services, as per a typical 1:n group communication scheme.

2.2. Service Requirements

The delivery of multicast contents during the forthcoming transition period needs to address the following requirements. Note that some of these requirements are not necessarily specific to the IPv4-to-IPv6 transition context, but rather apply to a wide range of multicast-based services whatever the environmental constraints, but the forthcoming transition period further stresses these requirements (see Section 4.4.1 for more details).

- Optimize bandwidth. Contents should not be multicast twice (i.e., using both versions of IP) to optimize bandwidth usage. Injecting multicast content using both IPv4 and IPv6 raises some dimensioning issues that should be carefully evaluated by service providers during network planning operations. For instance, if only few IPv6-enabled receivers are in use, it can be more convenient to convey multicast traffic over IPv4 rather than doubling the consumed resources for few users. IPv4/IPv6 co-existence solutions should be designed to optimize network resource utilization.

- Zap rapidly. The time it takes to switch from one content to another must be as short as possible. For example, zapping times between two TV channels should be comparable to an IPv4 case, i.e., less than a second so that translation does not significantly affect the overhead, whatever the conditions to access the multicast network. A procedure called "IGMP fast-leave" is sometimes used to minimize this issue so that the corresponding multicast stream is stopped as soon as the IGMP Leave message is received by the Querier. In current deployments, IGMP fast-leave often assumes the activation of the IGMP Proxy function in DSLAMs. The complexity of such design is aggravated within a context where IPv4 multicast control messages are encapsulated in IPv6.

- Preserve the integrity of contents that the user sees, i.e., not the contents of IP packets. Some contract agreements may prevent a service provider from altering the content owned by the content provider, because of copyright, confidentiality and SLA assurance reasons. Multicast streams should be delivered without altering their content.

- Preserve service quality. Crossing a CGN or performing multicast packet encapsulation may lead to fragmentation or extra delays and may therefore impact the perceived quality of service. Such degradation must be avoided.

- Optimize IPv4-IPv6 inter-working design. In some operational networks, a source-based stateful NAT function is sometimes used for load balancing purposes, for example. Because of the operational issues raised by such a stateful design, the deployment of stateless IPv4-IPv6 interworking functions should be privileged.

3. Use Cases

During the IPv4-to-IPv6 transition period, there might be a mix of multicast receivers, sources, and networks running in different address families. However, service providers must guarantee the delivery of multicast services to IPv4 receivers and, presumably, IPv6 receivers. Because of the inevitable combination of different IP version-related environments (sources, receivers and networks), service providers should carefully plan and choose the appropriate technique that will optimize the network resources to deliver multicast-based services.

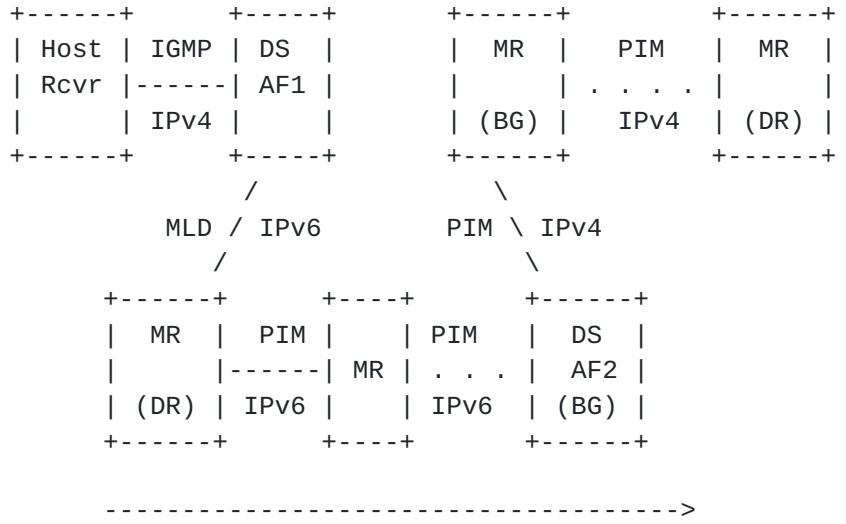
Concretely, several use cases can be considered during the IPv4/ IPv6 co-existence period. Some of them are depicted in the following sub-sections.

Note that the following diagrams are meant to illustrate the conceptual model. As such, they do not necessarily mean that the Adaptation Functions (AF) are embedded in a separate device and that messages need to be explicitly translated into new messages.

3.1. IPv4 Receiver and Source Connected to an IPv6-Only Network

We refer to this scenario as 4-6-4. An example of such use case is a DS-Lite environment, where customers will share global IPv4 addresses. IPv4 receivers are connected to CPE devices that are provisioned with an IPv6 prefix only. Delivering multicast content sent by an IPv4 source to such receivers requires the activation of some adaptation functions (AFs). These may operate at the network layer (interworking functions (IWF) or at the application layer (application level gateways (ALGs)).

The signalling flow for the 4-6-4 use case is shown in Figure 1.



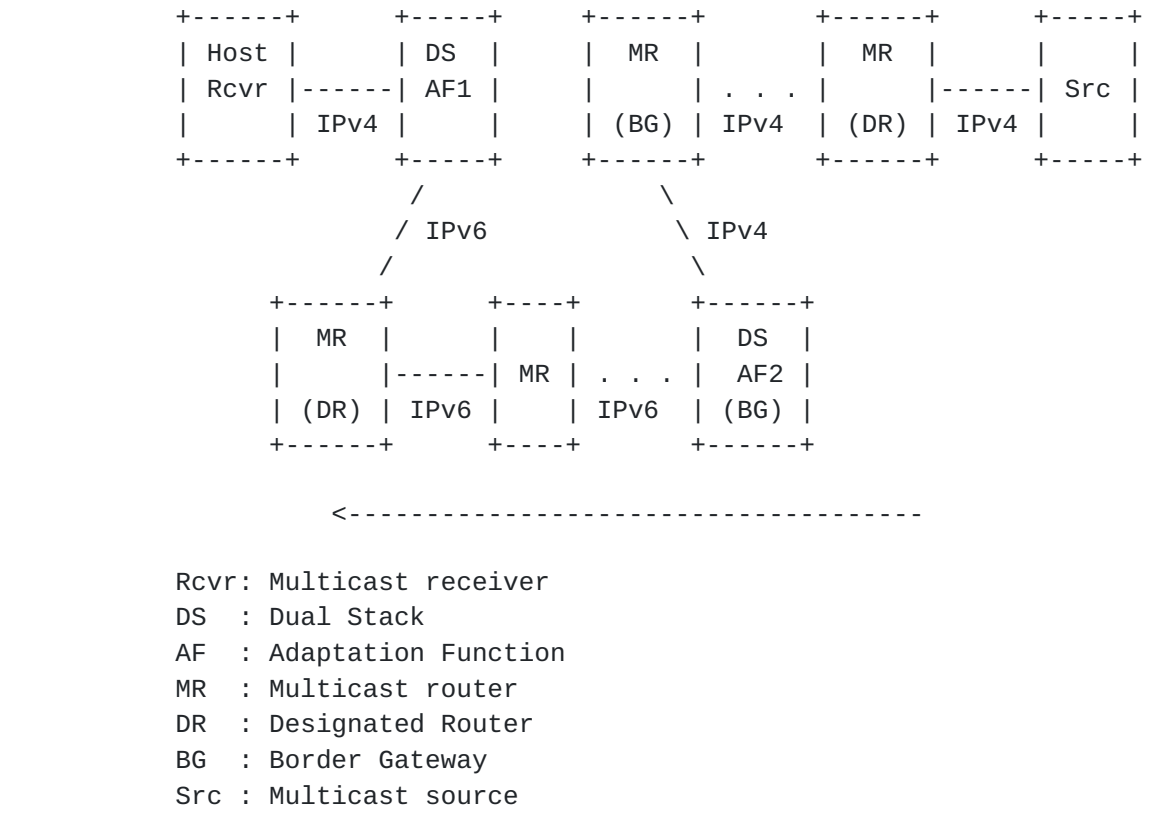
Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function (ALG or IWF)
MR : Multicast Router
DR : Designated Router
BG : Border Gateway

Figure 1: Signalling Path for the 4-6-4 Scenario.

AF1 refers to an IGMP/MLD Adaptation Function. Another Adaptation Function AF2 is needed at the border between the IPv6 multicast domain and the IPv4 multicast domain where the source resides. AF2 is typically embedded in a multicast router that either terminates or

propagates PIM signalling directed toward the IPv4 source in the IPv6 multicast domain.

On the IPv4 side, AF2 also acts as a multicast router, and uses PIMv4 signalling to join the IPv4 multicast group. The return path taken by multicast traffic is shown in Figure 2.



Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function
MR : Multicast router
DR : Designated Router
BG : Border Gateway
Src : Multicast source

Figure 2: Multicast Traffic Forwarding Path for the 4-6-4 Scenario.

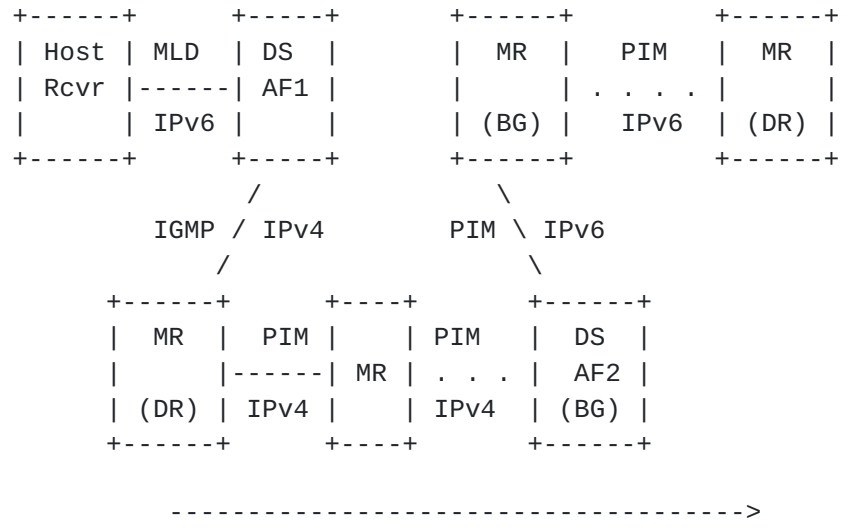
Again, adaptation functions are needed whenever the IP protocol version changes. The adaptation function instance AF2 at the boundary between the source network and the IPv6 network may either encapsulate or translate the headers of the IPv4 packets to allow the content to cross the IPv6 network. The adaptation function instance at the boundary between the IPv6 network and the receiver network performs the reverse operation to deliver IPv4 packets.

Given the current state-of-the-art where multicast content is likely to remain IPv4-formatted while receiver devices such as Set Top Boxes will also remain IPv4-only for quite some time, this scenario is prioritized by some service providers, including those that are deploying or will deploy DS-Lite CGN capabilities for the sake of IPv4 service continuity.

3.2. IPv6 Receiver and Source Connected to an IPv4-Only Network

We refer to this scenario as 6-4-6. Since providers who own the multicast content may not be ready for IPv6 migration beofre some time, the content is likely to remain IPv4-formatted. As a consequence, this 6-4-6 scenario is of lower priority than the 4-6-4 scenario.

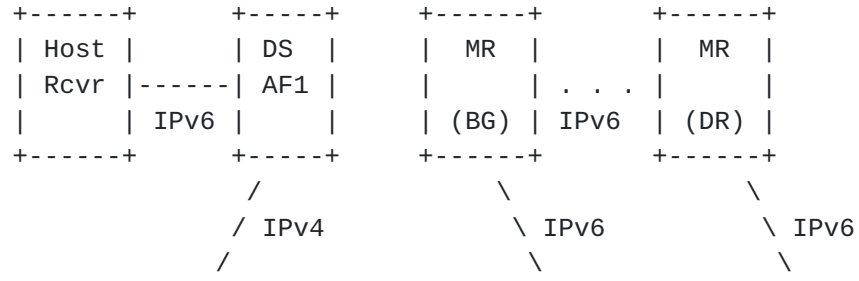
The signalling path for the 6-4-6 scenario is illustrated in Figure 3.



Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function
MR : Multicast Router
DR : Designated Router
BG : Border Gateway

Figure 3: Signalling Path For the 6-4-6 Scenario.

Figure 4 shows the path taken by multicast traffic flowing from the IPv6 source to the IPv6 receiver.



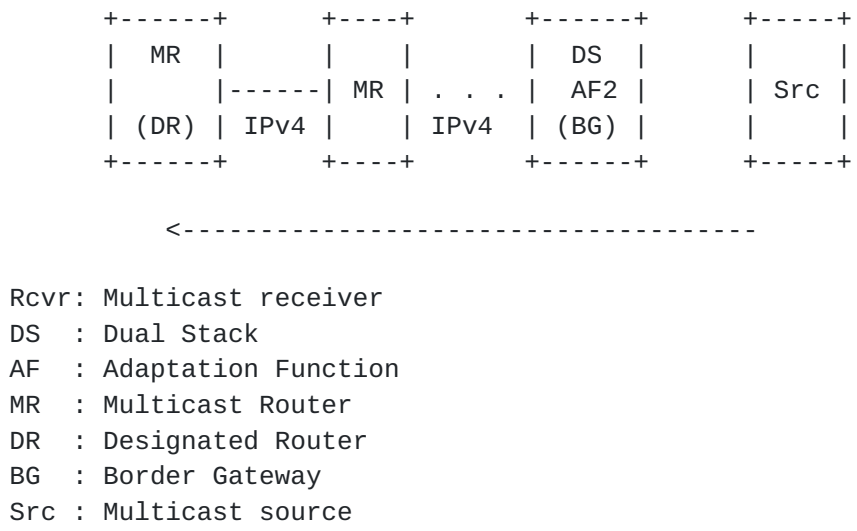
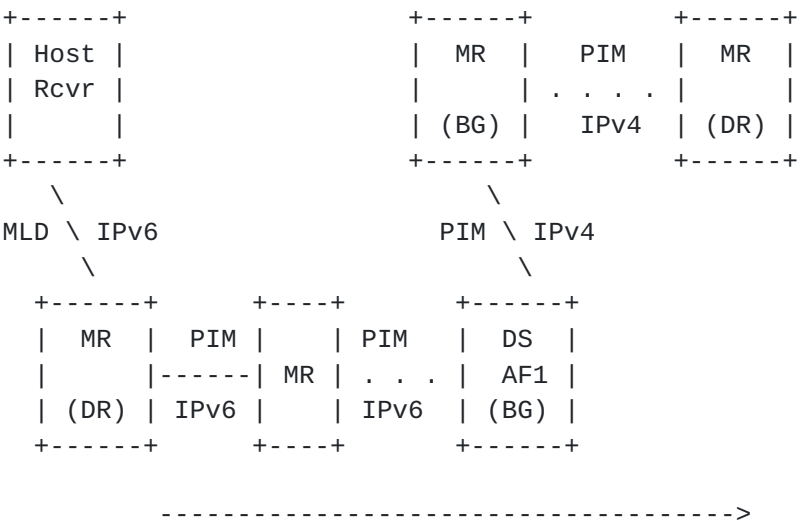


Figure 4: Multicast Traffic Forwarding Path For the 6-4-6 Scenario.

3.3. IPv6 Receiver and IPv4 Source

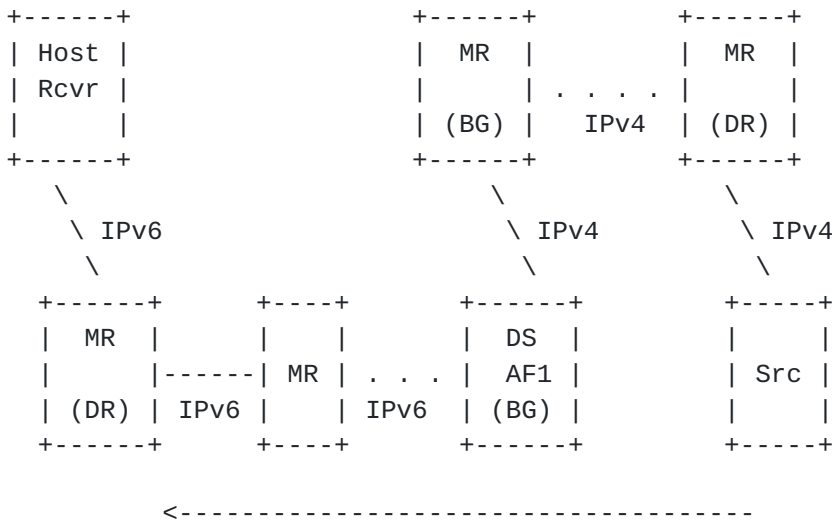
We refer to this scenario as 6-4. An example of such use case is the context of some mobile networks, where terminal devices are only provisioned with an IPv6 prefix. Accessing IPv4-formatted multicast content from an IPv6-only receiver requires additional functions to be enabled.

This scenario is privileged by mobile operators who deploy NAT64 capabilities in their network. It is illustrated in Figures 5 (signalling path) and 6 (forwarding of multicast traffic). Only one adaptation function instance is needed, and it will be located at the IPv4/IPv6 multicast domain boundary.



Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function
MR : Multicast Router
DR : Designated Router
BG : Border Gateway

Figure 5: Signalling Path For the 6-4 Scenario.



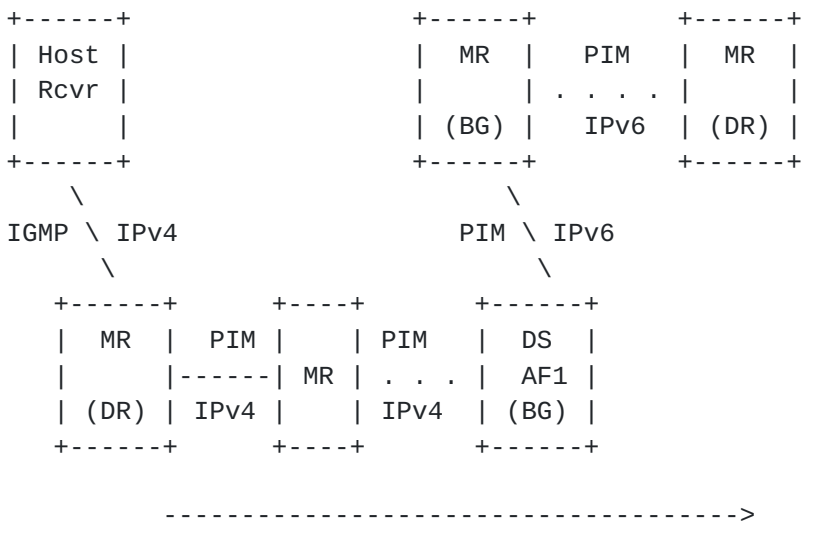
Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function
MR : Multicast Router
DR : Designated Router
BG : Border Gateway
Src : Multicast source

Figure 6: Multicast Traffic Forwarding Path For the 6-4 Scenario.

3.4. IPv4 Receiver and IPv6 Source

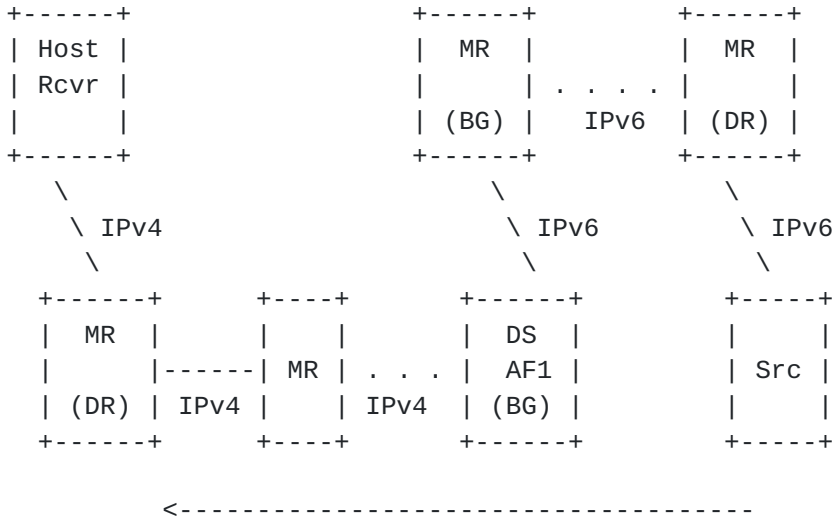
We refer to this scenario as 4-6. Yet, multicast sources are likely to remain IPv4-enabled in a first stage; therefore, the content is likely to remain IPv4-formatted. As a consequence, this scenario is unlikely to occur during the first years of the transition period.

The signalling path for this scenario is shown in Figure 7. The multicast traffic forwarding path is shown in Figure 8. There are similarities with the 6-4 scenario but address mapping across IP version boundaries is more challenging.



Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function
MR : Multicast Router
DR : Designated Router
BG : Border Gateway

Figure 7: Signalling Path For the 4-6 Scenario.



Rcvr: Multicast receiver
DS : Dual Stack
AF : Adaptation Function
MR : Multicast Router
DR : Designated Router
BG : Border Gateway

Src : Multicast source

Figure 8: Multicast Traffic Forwarding Path For the 4-6 Scenario.

3.5. Summary

To summarize, the use cases of highest priority are those involving IPv4 sources, i.e., the 4-6-4 and 6-4 scenarios.

4. Design Requirements

4.1. Group and Source Discovery Considerations

Multicast applications that embed address information in the payload may require Application Level Gateway (ALG) during the transition period. An ALG is application-specific by definition, and may therefore be unnecessary depending on the nature of the multicast service.

Such ALG (Application Level Gateway) may also be required to help an IPv6 receiver select the appropriate multicast group address when only the IPv4 address is advertised (e.g., when the SDP (Session Description Protocol) protocol is used to advertise some contents); otherwise, access to IPv4 multicast content from an IPv6 receiver may be compromised.

ALGs may be located upstream in the network. As a consequence, these ALGs do not know in advance whether the receiver is dual-stack or IPv6-only. In order to avoid the use of an ALG in the path, an IPv4-only source can advertise both an IPv4 multicast group address and the corresponding IPv4-embedded IPv6 multicast group address [I-D.ietf-mboned-64-multicast-address-format].

However, a dual-stack receiver may prefer to use the IPv6 address to receive the multicast content. The selection of the IPv6 multicast address would then require multicast flows to cross an IPv4-IPv6 interworking function.

The receiver should therefore be able to unambiguously distinguish an IPv4-embedded IPv6 multicast address from a native IPv6 multicast address.

4.2. Subscription

Multicast distribution trees are receiver-initiated. IPv4 receivers that want to subscribe to an IPv4 multicast group will send IGMP Report messages accordingly. In case the underlying access network is IPv6, the information conveyed in IGMP messages should be relayed by corresponding MLD messages.

4.3. Multicast Tree Computation

Grafting to an IPv4 multicast distribution tree through an IPv6 multicast domain suggests that IPv4 multicast traffic will have to be conveyed along an "IPv6-equivalent" multicast distribution tree. That is, part of the multicast distribution tree along which IPv4 multicast traffic will be forwarded should be computed and maintained by means of the PIMv6 machinery, so that the distribution tree can be terminated as close to the IPv4 receivers as possible for the sake of the multicast forwarding efficiency.

This assumes a close interaction between the PIM designs enforced in both IPv4 and IPv6 multicast domains, by means of specific Inter-Working Functions that are further discussed in Section 4.4.

Such interaction may be complicated by different combinations: the IPv4 multicast domain is SSM-enabled (with no RP (Rendezvous Point) routers), while the IPv6 multicast domain may support both ASM (Any Source Multicast) and SSM (Source Specific Multicast) [RFC3569] modes.

4.4. Multicast Adaptation Functions (AF)

IPv4-IPv6 multicast interworking functions are required for both translation (one address family to another) and traversal (one address family over another) contexts.

Given the multiple versions of Group Membership management protocols, issues may be raised when, for example, IGMPv2 is running in the IPv4 multicast domain that is connected to the IPv6 multicast domain by means of an IWF, while MLDv2 is running in the IPv6 multicast domain. To solve these problems, the design of the IWF function should adhere to the IP version-independent, protocol interaction approach documented in Section 8 of [RFC3810] and Section 7 of [RFC3376].

Note that, for traversal cases, to improve the efficiency of the multicast service delivery, traffic will be multicast along distribution trees that should be terminated as close to the receivers as possible for bandwidth optimization purposes. As a reminder, the traversal of unicast-only (access) networks is not considered in this document.

4.4.1. AF For Control Flows

The IWF to process multicast signalling flows (such as IGMP or MLD Report messages) should be independent of the IP version and consist mainly of an IPv4-IPv6 adaptation element and an IP address translation element. The message format adaptation must follow what is specified in [RFC3810] or [RFC4601], and the device that embeds the IWF device must be multicast-enabled, i.e., support IGMP, MLD and /or PIM, depending on the context (address family-wise) and the design (e.g., this device could be a PIM DR in addition to a MLD Querier).

The IWF can then be operated in the following modes: IGMP-MLD, PIMv4-PIMv6, MLD-PIMv4 and IGMP-PIMv6. In particular, Source-Specific Multicast (SSM) must be supported (i.e., IGMPv3/MLDv2 signalling traffic as well as the ability to directly send PIM (S, G) Join messages towards the source).

The following sub-sections describe some interworking functions which may be solicited, depending on the environment. Note that it may not be a stand-alone IWF that simply translates messages, but, for example, the combination of IPv4 and IPv6 states that would trigger the forwarding of aggregated MLD Report messages upstream that would include IPv6 groups based upon IPv4 states.

4.4.1.1. IGMP-MLD Interworking

The IGMP-MLD Interworking Function combines the IGMP/MLD Proxying function specified in [RFC4605] and the IGMP/MLD adaptation function which is meant to reflect the contents of IGMP messages into MLD messages, and vice versa.

For example, when an IGMP Report message is received to subscribe to a given multicast group (which may be associated to a source address if SSM mode is used), the IGMP-MLD Interworking Function must send an MLD Report message to subscribe to the corresponding IPv6 multicast group.

4.4.1.2. IPv4-IPv6 PIM Interworking

[RFC4601] allows the computation of PIM-based IPv4 or IPv6 distribution trees; PIM is IP version agnostic. There is no specific IPv6 PIM machinery that would work differently than an IPv4 PIM machinery. The new features needed for the IPv4-IPv6 PIM Interworking Function consist in dynamically triggering the PIM message of Address Family 1 upon receipt of the equivalent PIM message of Address Family 2.

The address mapping must be performed similarly to that of the IGMP-MLD Interworking Function.

4.4.1.3. MLD-IPv4 PIM Interworking

This IWF function is required when the MLD Querier is connected to an IPv4 PIM domain.

The address mapping must be performed similarly to that of the IGMP-MLD Interworking Function.

4.4.1.4. IGMP-IPv6 PIM Interworking

The address mapping must be performed similarly to that of the IGMP-MLD Interworking Function.

4.4.2. AF For Data Flows

The IWF to be used for multicast data flows is operated at the boundary between IPv4 and IPv6 multicast networks. Either encapsulation/de-capsulation or translation modes can be enforced, depending on the design. Note that translation operations must follow the algorithm specified in [RFC6145].

4.4.3. Address Mapping

The address mapping mechanisms to be used in either a stateful or stateless fashion need to be specified for the translation from one address family to the other.

The address formats can be those defined in [I-D.ietf-mboned-64-multicast-address-format] and [RFC6052] for IPv4-embedded IPv6 multicast and unicast addresses. Mapping operations are performed in a stateless manner by the algorithms specified in the aforementioned documents.

In this context, the IPv6 prefixes required for embedding IPv4 addresses can be assigned to devices that support IWF features by various means (e.g., static or dynamic configuration, out-of-band mechanisms, etc.).

If stateful approaches are used, it is recommended to carefully investigate the need to synchronize mapping states between multiple boxes, and the coordination of the IWF and source/group discovery elements is also required, at the cost of extra complexity.

4.5. Combination of ASM and SSM Modes

The ASM (Any Source Multicast) mode could be used to optimize the forwarding of IPv4 multicast traffic sent by different sources into the IPv6 multicast domain by selecting RP routers that could be located at the border between the IPv6 and the IPv4 multicast domains. This design may optimize the multicast forwarding efficiency in the IPv6 domain when access to several IPv4 multicast sources needs to be granted.

5. IANA Considerations

This document makes no request to IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

Access to contents in a multicast-enabled environment raises different security issues that have been already documented. In particular:

- When translating ASM-SSM there are certain security expectations from SSM (only receiving from the single specified sender), which are not the same expectations that come from ASM.

- If mappings are not stateful, it may be harder to monitor and troubleshoot the traffic.

- There are concepts of IPv4 and IPv6 multicast scopes. When translating, it must be taken into account how to reasonably map between scopes, and it is important that the scopes are configured appropriately on the routers so that a scope intended to be within a site for IPv4 (for example), doesn't leak outside the site due to translation to IPv6 inside the site.

7. Acknowledgments

Special thanks to T. Taylor for providing the figures and some of the text that illustrate the use cases depicted in Section 3. Thanks also to H. Asaeda, M. Blanchet, M. Eubanks, B. Haberman, N. Leymann, S. Perrault and S. Venaas for their valuable comments and support.

8. References

8.1. Normative References

[RFC2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC3569] Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[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, August 2006.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

8.2. Informative References

[I-D.ietf-mboned-64-multicast-address-format] Boucadair, M., Qin, J., Lee, Y., Venaas, S., Li, X., and M. Xu, "IPv6 Multicast Address With Embedded IPv4 Multicast Address", draft-ietf-mboned-64-multicast-address-format-05 (work in progress), April 2013.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

Authors' Addresses

Christian Jacquenet
France Telecom Orange
4 rue du Clos Courtel
Cesson-Sevigne 35512
France

Phone: +33 2 99 12 43 82
Email: christian.jacquenet@orange.com

Mohamed Boucadair
France Telecom Orange
4 rue du Clos Courtel
Cesson-Sevigne 35512
France

Phone: +33 2 99 12 43 71
Email: mohamed.boucadair@orange.com

Yiu Lee
Comcast
US

Email: Yiu_Lee@Cable.Comcast.com

Jacni Qin
Cisco Systems
People's Republic of China

Email: jacni@jacni.com

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: tena@huawei.com

Qiong Sun
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing 100035
People's Republic of China

Phone: >+86-10-58552936
Email: sunqiong@ctbri.com.cn