

Mboned  
Internet-Draft  
Intended status: Best Current Practice  
Expires: September 4, 2018

M. Abrahamsson  
T-Systems  
T. Chown  
Jisc  
L. Giuliano  
Juniper Networks, Inc.  
March 3, 2018

Deprecating ASM for Interdomain Multicast  
draft-acg-mboned-deprecate-interdomain-asm-00

Abstract

This document recommends the deprecation of the use of Any-Source Multicast (ASM) for interdomain multicast. It therefore implicitly recommends the use of Source-Specific Multicast (SSM) for interdomain multicast applications, and that hosts and routers that are expected to handle such applications fully support SSM. The recommendations in this document do not preclude the continued use of ASM within a single organisation or domain.

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 <https://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 September 4, 2018.

Copyright Notice

Copyright (c) 2018 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 (<https://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
2. Multicast routing protocols . . . . .	3
2.1. ASM routing protocols . . . . .	3
2.2. SSM Routing protocols . . . . .	4
3. Discussion . . . . .	4
3.1. Observations on ASM and SSM deployments . . . . .	4
3.2. Advantages of SSM for interdomain multicast . . . . .	5
4. Recommendations . . . . .	6
4.1. Deprecating use of ASM for interdomain multicast . . . . .	6
4.2. Including network support for IGMPv3 / MLDv2 . . . . .	6
4.3. Building application support for SSM . . . . .	7
4.4. Standardising an ASM/SSM protocol mapping mechanism . . . . .	7
4.5. Not filtering ASM addressing between domains . . . . .	8
4.6. Not precluding Intradomain ASM . . . . .	8
5. Security Considerations . . . . .	8
6. IANA Considerations . . . . .	8
7. Acknowledgments . . . . .	9
8. References . . . . .	9
8.1. Normative References . . . . .	9
8.2. Informative References . . . . .	10
Authors' Addresses . . . . .	11

## 1. Introduction

IP Multicast has been deployed in various forms, both within private networks and on the wider Internet. While a number of service models have been published, and in many cases revised over time, there has been no strong recommendation made on the appropriateness of those models to certain scenarios. This document addresses this gap by making a BCP-level recommendation to deprecate the use of ASM for interdomain multicast, and thus implicitly also that all hosts and routers that are expected to support such multicast applications fully support SSM.

This document does not make any statement on the use of ASM within in a single domain or organisation, and therefore does not preclude its use. Indeed, there may be a number of application contexts for which ASM is currently still considered well-suited within a single domain.

## 2. Multicast routing protocols

The general IP multicast service model [RFC1112] is that sender(s) send to a multicast group address, receivers express an interest in traffic sent to a given multicast group address, and that routers use multicast routing protocols to determine how to deliver traffic from the sender(s) to the receivers.

Two high-level flavours of this service model have evolved over time. In Any-Source Multicast (ASM), any number of sources may transmit multicast packets, and those sources may come and go over the course of a multicast session without being known a priori. In ASM, receivers express interest only in a given multicast group address, and the multicast routing protocol facilitates source discovery at the network layer. In contrast, with Source-Specific Multicast (SSM) the specific source(s) that may send traffic to the group are known in advance, or may be determined during a session, typically through an out-of-band protocol sitting above the network layer. Thus in SSM, receivers express interest in both a multicast group address and specific associated source address(es).

IANA has reserved specific ranges of IPv4 and IPv6 address space for multicast addressing. Guidelines for IPv4 multicast address assignments can be found in [RFC5771], while guidelines for IPv6 multicast address assignments can be found in [RFC2375] and [RFC3307]. The IPv6 multicast address format is described in [RFC4291].

### 2.1. ASM routing protocols

The most commonly deployed ASM routing protocol is Protocol Independent Multicast - Sparse Mode, or PIM-SM, as detailed in [RFC7761]. PIM-SM, as the name suggests, was designed to be used in scenarios where the subnets with receivers are sparsely distributed throughout the network. Because it does not know sender addresses in advance, PIM-SM uses the concept of a Rendezvous Point (RP) to 'marry up' senders and receivers, where all routers in a PIM-SM domain are configured to use specific RP(s).

To enable PIM-SM to work between multiple domains, i.e. to allow an RP in one domain to learn the existence of a source in another domain, an inter-RP signalling protocol known as Multicast Source Discovery Protocol (MSDP) [RFC3618] is used. Deployment scenarios for MSDP are given in [RFC4611]. MSDP has remained an Experimental protocol since its publication in 2003, and was not replicated or carried forward for IPv6.

In the absence of MSDP, a new mechanism, Embedded-RP [RFC3956], was defined for IPv6 PIM-SM, which allows routers supporting the protocol to determine the RP for the group without any prior configuration, simply by observing the RP address that is embedded (included) in the IPv6 multicast group address. Embedded-RP allows PIM-SM operation across any IPv6 network in which there is an end-to-end path of routers supporting the protocol.

## 2.2. SSM Routing protocols

PIM-SSM is detailed in [RFC4607]. In contrast to PIM-SM, PIM-SSM benefits from sender source address(es) being known about in advance, i.e. a given source's IP address is known (by some out of band mechanism), and thus the receiver's router can send a PIM JOIN directly towards the sender, without needing to use an RP.

IPv4 addresses in the 232/8 (232.0.0.0 to 232.255.255.255) range are designated as source-specific multicast (SSM) destination addresses and are reserved for use by source-specific applications and protocols. For IPv6, the address prefix FF3x::/32 is reserved for source-specific multicast use.

## 3. Discussion

### 3.1. Observations on ASM and SSM deployments

In enterprise and campus scenarios, ASM in the form of PIM-SM is in relatively common use, and has generally replaced PIM-DM [RFC3973]. The configuration and management of an RP within a single domain is not onerous. However, if interworking with external PIM domains in IPv4 multicast deployments is needed, MSDP is required to exchange information between domain RPs about sources. MSDP remains an Experimental protocol, and can be a complex and fragile protocol to administer and troubleshoot.

PIM-SM is a general purpose protocol that can handle all use cases. In particular, it was designed for cases such as videoconferencing where multiple sources may come and go during a multicast session. But for cases where a single, persistent source is used, and receivers can be configured to know of that source, PIM-SM has unnecessary complexity.

MSDP was not taken forward to IPv6. Instead, IPv6 has Embedded-RP, which allows the RP address for a multicast group to be embedded in the group address, making RP discovery automatic, if all routers on the path between a receiver and a sender support the protocol. Embedded-RP can support lightweight ad-hoc deployments. However, it relies on a single RP for an entire group. Embedded-RP was run

successfully between European and US academic networks during the 6NET project in 2004/05. Its usage generally remains constrained to academic networks.

As stated in RFC 4607, SSM is particularly well-suited to dissemination-style applications with one or more senders whose identities are known (by some mechanism) before the application starts running. PIM-SSM is therefore very well-suited to applications such as classic linear broadcast TV over IP.

SSM requires hosts and their subnet routers using it support the new(er) IGMPv3 [RFC3376] and MLDv2 [RFC3810] protocols. While delayed delivery of support in some OSes has meant that adoption of SSM has also been slower than might have been expected, or hoped, and was a historical reason to use ASM rather than SSM, support for IGMPv3 and MLDv2 is now widespread in common OSes.

### 3.2. Advantages of SSM for interdomain multicast

A significant benefit of SSM is its reduced complexity through eliminating the network-based source discovery required in ASM. This means there are no RPs, shared trees, Shortest Path Tree (SPT) switchovers, PIM registers, MSDP or data-driven state creation elements to support. SSM is really just a small subset of PIM-SM, plus IGMPv3 / MLDv2.

This reduced complexity makes SSM radically simpler to manage, troubleshoot and operate, particularly for network backbone operators, and this is the main motivation for the recommendation to deprecate the use of ASM in interdomain scenarios. Interdomain ASM is widely viewed as complicated and fragile. By eliminating network-based source discovery for interdomain multicast, the vast majority of the complexity issues go away.

RFC 4607 details many benefits of SSM, including:

- "Elimination of cross-delivery of traffic when two sources simultaneously use the same source-specific destination address;

- Avoidance of the need for inter-host coordination when choosing source-specific addresses, as a consequence of the above;

- Avoidance of many of the router protocols and algorithms that are needed to provide the ASM service model."

Further discussion can also be found in [RFC3569].

SSM is considered more secure in that it supports access control, i.e. you only get packets from the sources you explicitly ask for, as opposed to ASM where anyone can decide to send traffic to a PIM-SM group address. This topic is expanded upon in [RFC4609].

#### 4. Recommendations

##### 4.1. Deprecating use of ASM for interdomain multicast

This document recommends that the use of ASM is deprecated for interdomain multicast, and thus implicitly that hosts and routers that are expected to support such interdomain applications fully support SSM. Best current practices for deploying interdomain multicast using SSM are documented in [RFC8313]

The recommendation applies to the use of ASM between domains where either MSDP (IPv4) or Embedded-RP (IPv6) is required for sharing knowledge of remote sources. It also recommends against the multi-domain use of an ASM group with a single RP in one domain, where multicast tunnels are used between domains.

While MSDP is an Experimental level standard, this document does not propose making MSDP Historic, given its use may be desirable for intradomain multicast use cases.

##### 4.2. Including network support for IGMPv3 / MLDv2

This document recommends that all host and router platforms supporting multicast, and any security appliances that may handle multicast traffic, support IGMPv3 [RFC3376] and MLDv2 [RFC3810]. The updated IPv6 Node Requirements RFC [I-D.ietf-6man-rfc6434-bis] states that MLDv2 support is a MUST in all implementations. Such support is already widespread in common host and router platforms.

Further guidance on IGMPv3 and MLDv2 is given in [RFC4604].

It is sometimes desirable to limit the propagation of multicast messages in a layer 2 network, typically through a layer 2 switch device. In such cases multicast snooping can be used, by which the switch device observes the IGMP/MLD traffic passing through it, and then attempts to make intelligent decisions on which physical ports to forward multicast. Typically, ports that have not expressed an interest in receiving multicast for a given group would not have traffic for that group forwarded through them. Such snooping capability should support IGMPv3 and MLDv2. There is further discussion in [RFC4541].

#### 4.3. Building application support for SSM

There will be a wide range of applications today that only support ASM, whether as software packages, or code embedded in devices such as set-top boxes.

The implicit recommendation to use SSM for interdomain multicast means that applications should use SSM, and operate correctly in an SSM environment, triggering IGMPv3/MLDv2 messages to signal use of SSM.

It is often thought that ASM is required for multicast applications where there are multiple sources. However, RFC 4607 also describes how SSM can be used instead of PIM-SM for multi-party applications:

"SSM can be used to build multi-source applications where all participants' identities are not known in advance, but the multi-source "rendezvous" functionality does not occur in the network layer in this case. Just like in an application that uses unicast as the underlying transport, this functionality can be implemented by the application or by an application-layer library."

Given all common OSes support SSM, it is then down to the programming language and APIs used as to whether the necessary SSM APIs are available. SSM support is generally quite ubiquitous, with the current exception of websockets used in web-browser based applications.

It is desirable that applications also support appropriate congestion control, as described in [RFC8085], with appropriate codecs, to achieve the necessary rate adaption.

Some useful considerations for multicast applications can still be found in the relatively old [RFC3170].

#### 4.4. Standardising an ASM/SSM protocol mapping mechanism

In the case of existing ASM applications that cannot readily be ported to SSM, it may be possible to use some form of protocol mapping, i.e., to have a mechanism to translate a (\*,G) join or leave to a (S,G) join or leave, for a specific source, S. The general challenge in performing such mapping is determining where the configured source address, S, comes from.

There are some existing vendor-specific mechanisms to achieve this function, but none are documented in IETF standards. This appears to be a useful area for the IETF to work on, but it should be noted that any such effort would only be an interim transition mechanism, and

such mappings do not remove the requirement for applications to be allocated ASM group addresses for the communications.

#### 4.5. Not filtering ASM addressing between domains

A key benefit of SSM is that the multicast application does not need to be allocated a specific multicast group by the network, rather as SSM is inherently source-specific, it can use any group address, G, in the reserved range of IPv4 or IPv6 SSM addresses for its own source address, S.

In principle, if interdomain ASM is deprecated, backbone operators could begin filtering the ranges of group addresses used by ASM. In practice, this is not recommended given there will be a transition period from ASM to SSM, where some form of ASM-SSM mappings may be used, and filtering may preclude such operations.

#### 4.6. Not precluding Intradomain ASM

The use of ASM within a single multicast domain, such as an enterprise or campus, with an RP for the site, is still relatively common today. The operators of such a site may choose to use Anycast-RP [RFC4610] or MSDP for internal RP resilience, at the expense of the extra complexity in managing that configuration.

This document does not preclude continued use of ASM in the intradomain scenario. If an organisation, or AS, wishes to use multiple multicast domains within its own network border, that is a choice for that organisation to make, and it may then use MSDP or Embedded-RP internally within its own network.

### 5. Security Considerations

This document adds no new security considerations. RFC 4609 describes the additional security benefits of using SSM instead of ASM.

### 6. IANA Considerations

This document makes no request of IANA.

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



## 7. Acknowledgments

The authors would like to thank members of the IETF mboned WG for discussions on the content of this document, with specific thanks to the following people for their contributions to the document: Hitoshi Asaeda, Dale Carder, Toerless Eckert, Jake Holland, Albert Manfredi, Mike McBride, Per Nihlen, Greg Shepherd, James Stevens, Stig Venaas, Nils Warnke, and Sandy Zhang.

## 8. References

### 8.1. Normative References

- [RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, DOI 10.17487/RFC1112, August 1989, <<https://www.rfc-editor.org/info/rfc1112>>.
- [RFC2375] Hinden, R. and S. Deering, "IPv6 Multicast Address Assignments", RFC 2375, DOI 10.17487/RFC2375, July 1998, <<https://www.rfc-editor.org/info/rfc2375>>.
- [RFC3170] Quinn, B. and K. Almeroth, "IP Multicast Applications: Challenges and Solutions", RFC 3170, DOI 10.17487/RFC3170, September 2001, <<https://www.rfc-editor.org/info/rfc3170>>.
- [RFC3307] Haberman, B., "Allocation Guidelines for IPv6 Multicast Addresses", RFC 3307, DOI 10.17487/RFC3307, August 2002, <<https://www.rfc-editor.org/info/rfc3307>>.
- [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, <<https://www.rfc-editor.org/info/rfc3376>>.
- [RFC3569] Bhattacharyya, S., Ed., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, DOI 10.17487/RFC3569, July 2003, <<https://www.rfc-editor.org/info/rfc3569>>.
- [RFC3618] Fenner, B., Ed. and D. Meyer, Ed., "Multicast Source Discovery Protocol (MSDP)", RFC 3618, DOI 10.17487/RFC3618, October 2003, <<https://www.rfc-editor.org/info/rfc3618>>.
- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <<https://www.rfc-editor.org/info/rfc3810>>.

- [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, <<https://www.rfc-editor.org/info/rfc3956>>.
- [RFC3973] Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, DOI 10.17487/RFC3973, January 2005, <<https://www.rfc-editor.org/info/rfc3973>>.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <<https://www.rfc-editor.org/info/rfc4291>>.
- [RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, DOI 10.17487/RFC4607, August 2006, <<https://www.rfc-editor.org/info/rfc4607>>.
- [RFC4610] Farinacci, D. and Y. Cai, "Anycast-RP Using Protocol Independent Multicast (PIM)", RFC 4610, DOI 10.17487/RFC4610, August 2006, <<https://www.rfc-editor.org/info/rfc4610>>.
- [RFC5771] Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for IPv4 Multicast Address Assignments", BCP 51, RFC 5771, DOI 10.17487/RFC5771, March 2010, <<https://www.rfc-editor.org/info/rfc5771>>.
- [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, <<https://www.rfc-editor.org/info/rfc7761>>.

## 8.2. Informative References

- [RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, DOI 10.17487/RFC4541, May 2006, <<https://www.rfc-editor.org/info/rfc4541>>.
- [RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, DOI 10.17487/RFC4604, August 2006, <<https://www.rfc-editor.org/info/rfc4604>>.

- [RFC4609] Savola, P., Lehtonen, R., and D. Meyer, "Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements", RFC 4609, DOI 10.17487/RFC4609, October 2006, <<https://www.rfc-editor.org/info/rfc4609>>.
- [RFC4611] McBride, M., Meylor, J., and D. Meyer, "Multicast Source Discovery Protocol (MSDP) Deployment Scenarios", BCP 121, RFC 4611, DOI 10.17487/RFC4611, August 2006, <<https://www.rfc-editor.org/info/rfc4611>>.
- [RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <<https://www.rfc-editor.org/info/rfc8085>>.
- [RFC8313] Tarapore, P., Ed., Sayko, R., Shepherd, G., Eckert, T., Ed., and R. Krishnan, "Use of Multicast across Inter-domain Peering Points", BCP 213, RFC 8313, DOI 10.17487/RFC8313, January 2018, <<https://www.rfc-editor.org/info/rfc8313>>.
- [I-D.ietf-6man-rfc6434-bis]  
Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", draft-ietf-6man-rfc6434-bis-05 (work in progress), February 2018.

#### Authors' Addresses

Mikael Abrahamsson  
T-Systems  
Stockholm  
Sweden

Email: [mikael.abrahamsson@t-systems.se](mailto:mikael.abrahamsson@t-systems.se)

Tim Chown  
Jisc  
Lumen House, Library Avenue  
Harwell Oxford, Didcot OX11 0SG  
United Kingdom

Email: [tim.chown@jisc.ac.uk](mailto:tim.chown@jisc.ac.uk)

Lenny Giuliano  
Juniper Networks, Inc.  
2251 Corporate Park Drive  
Hemdon, Virginia 20171  
United States

Email: [lenny@juniper.net](mailto:lenny@juniper.net)