Mboned
Internet-Draft
Intended status: Best Current Practice
Expires: April 25, 2019
M. Abrahamsson
T-Systems
T. Chown
Jisc
L. Giuliano
Juniper Networks, Inc.
T. Eckert
Huawei
October 22, 2018

Deprecating ASM for Interdomain Multicast
draft-ietf-mboned-deprecate-interdomain-asm-01

Abstract

This document recommends deprecation of the use of Any-Source Multicast (ASM) for interdomain multicast. It recommends the use of Source-Specific Multicast (SSM) for interdomain multicast applications and that hosts and routers in these deployments fully support SSM. The recommendations in this document do not preclude the continued use of ASM within a single organisation or domain and are especially easy to adopt in these existing intradomain ASM deployments.

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 "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

Status of This Memo

Table of Contents

1. Introduction 2
2. Multicast routing protocols 3
  2.1. ASM routing protocols 4
  2.2. SSM Routing protocols 4
3. Discussion 5
  3.1. Observations on ASM and SSM deployments 5
  3.2. Advantages of SSM for interdomain multicast 6
4. Recommendations 7
  4.1. Deprecating use of ASM for interdomain multicast 7
  4.2. Including network support for IGMPv3 / MLDv2 7
  4.3. Building application support for SSM 8
  4.4. Preferring SSM applications intradomain 8
  4.5. Documenting an ASM/SSM protocol mapping mechanism 8
  4.6. Not filtering ASM addressing between domains 9
  4.7. Not precluding Intradomain ASM 9
5. Security Considerations 9
6. IANA Considerations 9
7. Acknowledgments 10
8. References 10
  8.1. Normative References 10
  8.2. Informative References 11
Authors' Addresses 12

1. Introduction

IP Multicast has been deployed in various forms, within private networks, the wider Internet, and federated networks such as national or regional research networks. While a number of service models have been published, and in many cases revised over time, there has been no strong recommendation made by the IETF on the appropriateness of

those models to certain scenarios, even though vendors and federations have often made such recommendations.

This document addresses this gap by making a BCP-level recommendation to deprecate the use of ASM for interdomain multicast, leaving SSM as the recommended interdomain mode of multicast. This recommendation thus also implicitly states that all hosts and routers that are expected to support interdomain multicast applications fully support SSM.

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

The main issue in most cases with moving to SSM is application support. Many applications are initially deployed for intradomain use and are later deployed interdomain. Therefore, this document recommends applications support SSM, even when they are initially intended for intradomain use. As explained below, SSM applications are readily compatible with existing intradomain ASM deployments as SSM is merely a subset of ASM.

2. Multicast routing protocols

Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) are the two multicast service models in use today. In ASM, as originally described in [RFC1112], receivers express interest in joining a multicast group address and routers use multicast routing protocols to deliver traffic from the sender(s) to the receivers. If there are multiple senders for a given group, traffic from all senders will be delivered to the receiver. Since receivers specify only the group address, the network, and therefore the multicast routing protocols, are responsible for source discovery. In SSM, by contrast, receivers specify both group and source when expressing interest in joining a multicast stream. Source discovery in SSM is handled by some out-of-band mechanism (ie, the application layer), which drastically simplifies the network and how the multicast routing protocols operate.

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) as a 'meeting point' for sources and receivers, and all routers in a PIM-SM domain are configured to use specific RP(s), either explicitly or through dynamic RP discovery protocols.

To enable PIM-SM to work between multiple domains, an inter-RP signalling protocol known as Multicast Source Discovery Protocol (MSDP) [RFC3618] is used to allow an RP in one domain to learn the existence of a source in another domain. Deployment scenarios for MSDP are given in [RFC4611]. MSDP floods information about all active sources for all multicast streams to all RPs in all the domains - even if there is no receiver for a given application in a domain. As a result of this key scalability and security issue, along with other deployment challenges with the protocol, MSDP was never extended to support IPv6 and remains an Experimental protocol.

To this day, there is no IETF Proposed Standard level interdomain solution for IPv4 ASM multicast because MSDP was the "best" component for the interdomain source discovery problem, and it is Experimental. Other protocol options where investigated at the same time but were never implemented or deployed and are now historic (e.g: [RFC3913]).

Due to the availability of more bits in an IPv6 address than in IPv4, an IPv6-specific mechanism was able to be designed in support of interdomain ASM with PIM-SM. Embedded-RP [RFC3956] allows routers supporting the protocol to determine the RP for the group without any prior configuration or discovery protocols, simply by observing the unicast 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 mechanism.

2.2. SSM Routing protocols

SSM is detailed in [RFC4607]. Note that there is no separate document for PIM-SSM as it merely leverages a subset of [RFC7761].

PIM-SSM expects that the sender's source address(es) is known in advance by receivers by some out-of-band mechanism (typically in the application layer), and thus the receiver's designated router can

send a PIM JOIN directly towards the source 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. See [RFC4607]. 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 likely the most commonly deployed multicast protocol. The configuration and management of an RP (including RP redundancy) within a single domain is a well understood operational practice. However, if interworking with external PIM domains is needed in IPv4 multicast deployments, interdomain MSDP is required to exchange information about sources between domain RPs. Deployment experience has shown MSDP to be a complex and fragile protocol to manage and troubleshoot (complex flooding RPF rules, state attack protection, filtering of undesired sources, ...).

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 for a group is used, and receivers can be configured to know of that source, PIM-SM has unnecessary complexity. Therefore, SSM eliminates the most components of PIM-SM.

As explained above, MSDP was not extended to support to IPv6. Instead, the proposed interdomain ASM solution for PIM-SM with IPv6 is Embedded-RP, which allows the RP address for a multicast group to be embedded in the group address, making RP discovery automatic for all routers on the path between a receiver and a sender. Embedded-RP can support lightweight ad-hoc deployments. However, it relies on a single RP for an entire group that could only be made resilient within one domain. While this approach solves the MSDP issues, it does not solve the problem of unauthorised sources sending traffic to ASM multicast groups; this security issues is one of biggest problem of interdomain multicast.

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 oob mechanism) before the application starts running or applications that utilize some signaling to

indicate the source address of the multicast stream (eg, electronic programming guide in IPTV applications). PIM-SSM is therefore very well-suited to applications such as classic linear broadcast TV over IP.

SSM requires applications, host operating systems and the designated routers connected to receiving hosts to support IGMPv3 [RFC3376] and MLDv2 [RFC3810]. Support for IGMPv3 and MLDv2 has become widespread in common OSes for several years (Windows, MacOS, Linux/Android) and is no longer an impediment to SSM deployment.

3.2. Advantages of SSM for interdomain multicast

A significant benefit of SSM is the reduced complexity that comes through eliminating the network-based source discovery required in ASM. Specifically, SSM eliminates the need for RPs, shared trees, Shortest Path Tree (SPT) switchovers, PIM registers, MSDP, dynamic RP discovery mechanisms (BSR/AutoRP) and data-driven state creation. SSM simply utilizes a small subset of PIM-SM, alongside the integration with IGMPv3 / MLDv2, where the source address signaled from the receiver is immediately used to create (S,G) state. Eliminating network-based source discovery for interdomain multicast means the vast majority of the complexity of multicast goes away.

This reduced complexity makes SSM radically simpler to manage, troubleshoot and operate, particularly for backbone network operators. This is the main motivation for the recommendation to deprecate the use of ASM in interdomain scenarios. Note that SSM operation is standardised in PIM-SM (RFC7761); there is no separate specification for PIM-SSM.

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 inherently supports access control. That is, receivers only get packets from the sources they explicitly specify, as opposed to ASM where any host can send traffic

to a group address and have it transmitted to all receivers. 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 support such interdomain applications fully support SSM and its associated protocols. 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 used.

An interdomain use of ASM multicast in the context of this document is one where PIM-SM with RPs/MSDP/Embedded-RP is run on routers operated by two or more separate administrative entities (domains, organisations).

The more inclusive interpretation of this recommendation is that it also extends to the case where PIM may only be operated in a single operator domain, but where user hosts or non-PIM network edge devices are under different operator control. A typical example of this case is an SP providing IPTV (single operator domain for PIM) to subscribers operating an IGMP proxy home gateway and IGMPv3/MLDv2 hosts (computer, tablets, set-top boxes).

4.2. Including network support for IGMPv3 / MLDv2

This document recommends that all hosts, router platforms and security appliances supporting multicast support IGMPv3 [RFC3376] and MLDv2 [RFC3810] (based on the version IP they intend to support). 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].

Multicast snooping is often used limit the flooding of multicast traffic in a layer 2 network. With snooping, a L2 switch will monitor IGMP/MLD messages and only forward multicast traffic out host ports that have interested receivers connected. Such snooping capability should therefore support IGMPv3 and MLDv2. There is further discussion in [RFC4541].

4.3. Building application support for SSM

The recommendation to use SSM for interdomain multicast means that applications should properly trigger the sending of IGMPv3/MLDv2 messages. It should be noted, however, there is a wide range of applications today that only support ASM. In many cases this is due to application developers being unaware of the operational concerns of networks. This document serves to provide clear direction for application developers to support 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."

Some useful considerations for multicast applications can be found in [RFC3170].

4.4. Preferring SSM applications intradomain

If feasible, it is recommended for applications to use SSM even if they are initially only meant to be used in intradomain environments supporting ASM. Because PIM-SSM is a subset of PIM-SM, existing intradomain PIM-SM networks are automatically compatible with SSM applications. Thus, SSM applications can operate alongside existing ASM applications. SSM's benefits of simplified address management and significantly reduced operational complexity apply equally to intradomain use.

However, for some applications it may be prohibitively difficult to add support for source discovery, so intradomain ASM may still be appropriate.

4.5. Documenting 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 existing vendor-specific mechanisms deployed that achieve this function, but none are documented in IETF documents. This may be a useful area for the IETF to work on as an interim transition mechanism. However, these mechanisms would introduce additional administrative burdens, along with the need for some form of address management, neither of which are required in SSM. Hence, this should not be considered a a long-term solution.

4.6. Not filtering ASM addressing between domains

A key benefit of SSM is that the receiver specifies the source-group tuple when signaling interest in a multicast stream. Hence, the group address need not be globally unique, so there is no need for multicast address allocation as long the reserved SSM range is used.

Despite the deprecation of interdomain ASM, it is recommended that operators should not filter ASM group ranges at domain boundaries, as some form of ASM-SSM mappings may continue to be used for some time.

4.7. Not precluding Intradomain ASM

The use of ASM within a single multicast domain such as a campus or enterprise is still relatively common today. There are even global enterprise networks that have successfully been using PIM-SM for many years. The operators of such networks most often use Anycast-RP [RFC4610] or MSDP for RP resilience, at the expense of the extra operational complexity. These existing practices are unaffected by this document.

This document does not preclude continued use of ASM in the intradomain scenario. If an organisation chooses to operate multiple multicast domains within its own administrative borders, it may then use MSDP or Embedded-RP internally within its own network.

5. Security Considerations

This document adds no new security considerations. It instead removes security issues incurred by interdomain ASM with PIM-SM/MSDP such as infrastructure control plane attacks and application and bandwidth/congestion attacks from unauthorised sources sending to ASM multicast groups. 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, 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>.

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

[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>.

[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>.

[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

[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>.

[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>.

[RFC3913] Thaler, D., "Border Gateway Multicast Protocol (BGMP): Protocol Specification", RFC 3913, DOI 10.17487/RFC3913, September 2004, <https://www.rfc-editor.org/info/rfc3913>.

[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>.

[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-09 (work in progress), July 2018.

Authors' Addresses

Mikael Abrahamsson
T-Systems
Stockholm
Sweden

Email: 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

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

Email: lenny@juniper.net

Toerless Eckert
Futurewei Technologies Inc.
2330 Central Expy
Santa Clara 95050
USA

Email: tte+ietf@cs.fau.de