INTERNET-DRAFT
draft-giuliano-mboned-v6mcast-framework-01.txt

Leonard Giuliano
Juniper Networks
Greg Shepherd
Procket Networks
Matthew Davy
Indiana University

Expires: December 2003

June 2003

Framework for Deploying Interdomain IPv6 Multicast
<draft-giuliano-mboned-v6mcast-framework-01.txt>

Status of this Document

Copyright Notice

Abstract

This document describes an architectural framework for deploying interdomain multicast for IPv6 with simplicity, scalability, efficiency and security as the primary goals, applying the lessons learned from deploying IPv4 multicast. In order to achieve this objective, the deprecation of network-based source discovery, and therefore Any Source Multicast, is proposed. Source-Specific Multicast is proposed as the service model supported for deploying interdomain IPv6 multicast. The architectural components responsible for providing source discovery are also discussed.

Table of Contents

1. Introduction

The deployment of IPv4 multicast has been much slower than initially predicted. While there are many reasons for this slow adoption, one of the dominant factors has been the complexity involved in implementing and deploying multicast. In the past, interim workarounds were applied to address short-term deficiencies in the architecture. Unfortunately, many of these temporary fixes have become integral components that have proven difficult to "undeploy" and have stifled future developments and enhancements. This document proposes an architecture for IPv6 that applies the lessons learned from deploying IPv4 multicast, rather than repeating the mistakes of the past.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

2. Source Discovery

The majority of the complexity involved in multicast comes from the assumption that the network is responsible for the discovery of sources. The receiver of multicast traffic merely requests data for a given group address. It is the network's job to find all the sources for this group and deliver their packets to the receiver. This original model of multicast, where source discovery is a function of the network layer, is known as Any Source Multicast (ASM) [RFC1112].

However, with the Source-Specific Multicast [SSM] service model, the receiving host determines the address of the source(s) through out-of-band means and requests data for a group from the specified source(s). By specifying the source in addition to the group, the network no longer needs to determine all the sources, thus the function of the network becomes much simpler.

2.1. Network-based vs. Application-based Source Discovery

It should be noted that in the vast majority of cases, the end result of ASM and SSM is functionally identical. That is, since the

predominant implementations and deployments of Protocol Independent Multicast- Sparse Mode (PIM-SM) [PIM-SM] on the Internet today (the de facto standard protocol for ASM multicast routing) switchover from the shared tree to the shortest path tree (SPT) immediately, traffic is delivered from source to receiver along the SPT. Therefore, since the end result of ASM and SSM is the same (ie, SPTs), the debate is not ASM vs. SSM. Rather, the issue is network-based vs. out-of-band source discovery. For the sake of this discussion, we will assume the application layer provides this out-of-band function.

Since the original vision of multicast assumes the network will provide source discovery, multicast protocols have required mechanisms to support this vision, and these mechanisms generally have introduced sub-optimal properties. For example, dense protocols like Distance Vector Multicast Routing Protocol (DVMRP) [DVMRP] and PIM-DM periodically flood data throughout the domain to inform routers in the domain of active sources. Sparse protocols like PIM-SM employ rendezvous points (RPs) so that one router in the domain will be responsible for being aware of active sources for a given group range. The mechanisms needed to provision an RP, inform routers throughout the domain of the identity of the RP, register sources with the RP, and exchange source information between different RPs have each contributed a significant amount of complexity to the architecture. In each case, the primary disadvantages of these protocols (ie, lack of scalability of flooding in dense protocols, and the complexity of RP behavior in sparse protocols) can be attributed to source discovery. Furthermore, IPv4 uses MSDP [MSDP] to distribute active source information between RPs. With MSDP, all speakers of the protocol must maintain a cache containing information about every active source on the Internet. MSDP relies upon an extremely complex set of peer-RPF rules which are not well understood, are very challenging to troubleshoot and are often circumvented (for example, by using mesh-groups).

Long ago it was determined that maintaining a list of all the hostnames or all the websites on the Internet was unwise. This task was deemed unsuitable even for hosts to provide. However, when the network provides multicast source discovery, we assume that routers will provide this exact function.

The main reason why network-based source discovery was deemed necessary was because it was believed that some multi-source applications (eg, videoconferencing, online gaming) could only be supported in this manner. However, Section 1 of [SSM] describes how even these applications can be supported with application-based source discovery:

> 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.

[MULT-SSM] and [DISC-SSM] further examine and propose ways to support multi-source discovery in SSM.

Since network-based source-discovery significantly contributes to the cost and complexity of the network infrastructure without providing commensurate functionality and benefit, this document proposes to deprecate network-based multicast source discovery in IPv6. With source discovery provided by the application layer, SSM is proposed as the only service model supported for deploying interdomain IPv6 multicast.

3. Interdomain Multicast for IPv6

The primary issue with interdomain multicast in IPv6 today is the support for RPs in different domains. In IPv4, MSDP addresses this problem. However, because of the undesirable properties of MSDP mentioned earlier, there appears to be little interest for introducing MSDP to IPv6.

BGMP [BGMP] has been specified as a protocol to provide support for interdomain multicast in IPv6. Specifically, support for RPs in different domains is described. However, many believe BGMP is too complex to be a feasible option for deployment. There are currently no known implementations of BGMP.

[EMBED] has been proposed to address this issue by embedding the IP address of the RP within the multicast group address. However, this would require a new behavior for the PIM-SM protocol, specifically, sending PIM joins toward an RP in another domain, to be investigated and specified. And this new behavior would need to be deployed on all routers over which this multicast traffic would flow.

With network-based source discovery deprecated, there is no longer a need for PIM-SM RPs in IPv6. Interdomain multicast will work with a subset of PIM-SM functionality (namely, (S,G) Joins/Prunes). Thus, interdomain multicast for IPv6 requires no changes to any protocols and can be deployed with current implementations of PIM-SM.

4. Intradomain Multicast for IPv6

PIM-SM, as defined in [PIM-SM], requires no changes to operate within an IPv6 domain. Most current intradomain deployments of IPv4 multicast use Anycast RP to provide redundancy and load sharing. Since Anycast RP relies on MSDP, there is currently no way to provide this same functionality in IPv6. [Any-PIM] proposes an extension to the PIM-SM register process to accomplish the internal MSDP functionality of Anycast RP.

With network-based source discovery deprecated, there is no longer a need for PIM-SM RPs. Intradomain multicast for IPv6 requires no changes to any protocols and can be deployed with current implementations of PIM-SM or BiDir-PIM.

4.1. Other Service Models for Intradomain IPv6 Multicast

There may still be some desire to support other multicast service models such as ASM and Bidirectional-PIM (BiDir-PIM) [BIDIR] within a domain. Following the philosophy of "what one does inside one's own domain is one's own business", this document does not prohibit the use of ASM or BiDir-PIM for intradomain purposes as long as it does not leak out to the rest of the Internet. This is somewhat analogous to using RFC-1918 addressing within a domain.

5. Security Considerations

IP Multicast is inherently vulnerable to attack because it allows a host to create state within the control and data planes of the network. Network-based source discovery amplifies this problem, as the mechanisms that enable the network to discover sources generally increase the likelihood and impact of attacks.

In recent years, IPv4 RPs and other MSDP speakers have been the victims of DoS attacks during the Ramen and Slammer Worm attacks [MCAST-DOS]. In both cases, these attacks were not even targeting the multicast infrastructure. Rather, they inflicted damage accidentally. Little has been done to harden this infrastructure, and today IPv4 multicast networks remain vulnerable to attack. This is because the mechanisms that provide network-based source discovery are inherently prone to DoS attack.

5.1. Control Plane Vulnerabilities

If, for example, someone on an IPv4 multicast-enabled network performs a port scan on a /16 multicast range of addresses, the first hop PIM-SM router will create register messages for each packet sent to a different group and send these 65k PIM registers to an RP, which will have to decapsulate and create register state. The RP will then create MSDP SAs for each s-g tuple and flood 65k SAs to all other MSDP speakers on the Internet. Even with the strictest of filters in place, the ASM service model dictates that any host could validly source multicast traffic for 224.2/16 and 233/8. This means that a single source could validly create state for 16.8 million different groups, and the network would have to maintain this state. With filters in place, the best that could be hoped for is the decreased probability that an accidental attack (eg, a port scan on a random multicast address range) will have an impact. For this reason, some have suggested rate limiting. However, rate limiting control traffic creates a new vulnerability to DoS attack since it is not possible (or at least is very difficult) to tell the difference between bad sources and good ones, and they both must now contend for the configured limit of resources. Therefore, rate limits reduce the probability that a router will run out of memory and crash, but increase the probability that the multicast infrastructure will be unable to create and maintain state, causing black holes for valid sources during an attack.

MSDP has not yet been defined, implemented or deployed for use in

IPv6, however the DR-RP PIM register process is the same for IPv6 and IPv4 ASM. Of course the IPv6 group range is much larger. For example, the IPv6 group range is FF::0/8, so a single host could validly source to nearly 2^120 groups and the network would be responsible for maintaining this state.

With network-based source discovery deprecated, there is no need for PIM-SM RPs, MSDP or the PIM-SM register process. This significantly reduces the opportunities for a malicious attack. While state creation is driven both by sources and receivers in ASM, only receivers can create state in the network with SSM. SSM, like ASM, is still vulnerable to an (S,G) flood attack, but is not vulnerable to any of the other control plane attacks mentioned above.

5.2. Data Plane Vulnerabilities

In addition to the control plane vulnerabilities mentioned above, ASM and BiDir-PIM provide easy targets for DoS attacks in the data plane. When a receiving host reports interest in a group, it requests and is delivered packets from ALL sources for that group. There is no way to prevent delivery of unwanted sources. For example, one malicious attacker (or misconfigured host) could transmit a high data rate of unwanted traffic to a group, and all receivers of this group would be flooded with this traffic.

Since an SSM subscriber explicitly specifies the source, data from unwanted sources will not be delivered. In order to launch a data plane attack, a malicious host must spoof the source address of the SSM channel AND must be on the shortest path from the subscriber to the source. While this is technically possible, it is significantly less likely.

6. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of

claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. Acknowledgments

The authors would like to thank Vijay Gill, John Zwiebel, Tom Pusateri, Nidhi Bhaskar and Toerless Eckert for their input. Dave Meyer provided extensive comments on the initial version of this draft.

8. References

8.1. Normative References

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

[SSM] Holbrook, H., and B. Cain, "Source-Specific Multicast for IP", draft-ietf-ssm-arch-03.txt. Work in Progress.

8.2. Informative References

[RFC1112] S. Deering, "Host Extensions for IP Multicasting", RFC 1112, August 1989

[PIM-SM] B. Fenner, et. al., "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)", Work in Progress.

[MSDP] Meyer, D., and B. Fenner (Editors), "The Multicast Source Discovery Protocol (MSDP)", draft-ietf-msdp-spec-20.txt. Work in Progress.

[BIDIR] M. Handley, et. al., "Bi-directional Protocol Independent Multicast", draft-ietf-pim-bidir-05.txt, Work in Progress.

[BGMP] D. Thaler, "Border Gateway Multicast Protocol (BGMP): Protocol Specification", draft-ietf-bgmp-spec-05.txt, Work in Progress.

[EMBED] Savola, P., and B. Haberman, "Embedding the Address of RP in IPv6 Multicast Address", draft-savola-mboned-mcast-rpaddr-03.txt, Work in Progress

[Any-PIM] Farinacci, D., and Y. Cai, "Anycast-RP using PIM", draft-farinacci-pim-anycast-rp-00.txt, Work in Progress

[MULT-SSM] M. Hoerdt, et al., "Multi-source communications over SSM networks", draft-hoerdt-mboned-multisource-ssm-00.txt, Work in

Progress

[DISC-SSM] F. Beck, et al., "Source Discovery Protocol in SSM Networks", draft-beck-mboned-ssm-source-discovery-protocol-00.txt, Work in Progress

[MCAST-DOS] T. Pusateri, "Multicast DoS", In Proceedings of MBONED Working Group, IETF56, March 2003

[DVMRP] T. Pusateri, "Distance Vector Multicast Routing Protocol", draft-ietf-idmr-dvmrp-v3-10.txt, Work in Progress

9. Author's Addresses

Leonard Giuliano
Juniper Networks
Email: lenny@juniper.net

Greg Shepherd
Procket Networks
Email: shep@procket.com

Matthew Davy
Indiana University
Email: mpd@iu.edu

10. Full Copyright Statement