Mboned	T.J. Chown
Internet-Draft	University of Southampton
Intended status: Informational	July 12, 2011
Expires: January 13, 2012	

Multicast Filtering Practices
draft-chown-mboned-multicast-filtering-01

Abstract

Operators of multicast networks may apply various filters to multicast traffic at boundary routers or on MSDP peerings. The aim of this text is to document existing filtering practices, with a view to generating some discussion towards producing guidance on best filtering practice.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Multicast filtering can be applied at a multicast boundary or on an MSDP peering as a means to prevent unintended leakage of multicast traffic beyond its desired scope. An informal discussion of filtering practices suggested that those practices vary from organisation to organisation. The aim of this text is to gather and document commonly used existing filtering practices. Whether it is then possible to draw up a definitive best practice is to be determined; it is quite possible that due to the shifting nature of the target that a point-in-time recommendation would quickly be overtaken by events. For example, the recent addition of unicast prefix-based IPv4 multicast addresses [RFC6034] meant that filtering of all of 234.0.0.0/8 became undesirable. However, general principles may remain valid over time. For sites on academic research networks, some examples of filtering recommendations already exists, e.g. in documentation [I2multicast] from the Internet2 Multicast WG, and in the JANET IPv4 Multicast Guide [JANETmulticast]. There is also a more specific proposal for the Rutgers network [RutgersProposal], which includes a good discussion of organisational-local scope address usage within its network as a whole. When determining filtering policies, one needs to consider how strict to be; some ranges are not supposed to be used, but there may be no harm per se in accepting them. There are certainly some ranges that should not be filtered, such as the newly assigned 234.0.0.0/8 range mentioned above, and the GLOP range under 233.0.0.0/8.

An additional resource is the registry of IPv4 multicast address space held by IANA [IANAmulticast]. This registry should be a definitive guide to the formal use of ranges of addresses within the overall IPv4 multicast address space. A similar registry is maintained for IPv6 multicast address space [IANA6multicast].

This text is a very early draft, aimed at soliciting feedback, both on content and whether the goal of the draft is actually worthwhile. Different sites may have different requirements. There may also be issues with handling scope boundaries that need to be considered. So there may be general principles that could be captured in a document such as this, even if specific filtering rules are not included.

2. Border and MSDP Filtering

In this section we summarise IPv4 multicast addresses that are commonly filtered at site borders or on MSDP peerings. Based on responses we received from a couple of multicast community lists, it wasn't clear which filters are applied on border routers and which on MSDP SA messages. Some sites apply minimal traffic filters, but heavier MSDP filtering.

A site may choose to filter on addresses or on observed TTLs; it is now general practice to filter on addresses rather than the TTL filtering that was common a long time ago.

Some sites choose to route multicast around their unicast firewalls, for performance or other operational reasons, but this shouldn't alter the requirement to filter groups appropriately where necessary.

In this section we draw on the small number contributions so far; we hope to get more inputs in time. In general, many 224.0.0.* addresses that are used by infrastructure are typically blocked, as well as some addresses that are global scope but should not be, like Ghostcast.

The following list includes multicast IPv4 addresses that are being filtered based on the union of responses received so far (hence the apparent duplication of certain prefixes). The list of filters applied by all respondents would be somewhat shorter.

224.0.1.1	NTP
224.0.1.2	SGI-Dogfight
224.0.1.3	Rwhod
224.0.1.8	SUN NIS+
224.0.1.20	any private experiment
224.0.1.22	SVRLOC
224.0.1.24	microsoft-ds
224.0.1.25	nbc-pro
224.0.1.35	SVRLOC-DA
224.0.1.38	Retrospect
224.0.1.39	cisco-rp-announce
224.0.1.40	cisco-rp-discovery
224.0.1.41	gatekeeper
224.0.1.60	hp-device-disc
224.0.1.65	iapp
224.0.1.76	IAPP lucaent-avaya-ap
224.0.2.1	rwho
224.0.2.2	SUN RPC
224.0.2.3	EPSON-disc-set
224.0.23.1	Ricoh-device-ctrl
224.0.23.2	Ricoh-device-ctrl
224.1.0.1	Cisco Aironet
224.1.0.38	Retrospect
224.2.0.2	Altiris Rapideploy
224.2.0.3	Altiris Rapideploy
224.77.0.0/16	Norton Ghost
224.101.101.101	Sun Sunray
225.1.2.3	Altiris Development Server and Deployment Agent
226.77.0.0/16	Norton Ghost
229.55.150.208	Norton Ghost
231.0.0.0/8	?
234.21.81.1	Limewire
234.42.42.0/30	ImageCast
234.42.42.32/31	ImageCast
234.42.42.40/30	ImageCast
234.142.142.42/31	ImageCast
234.142.142.44/30	ImageCast
234.142.142.48/28	ImageCast
234.142.142.64/26	ImageCast
234.142.142.128/29	ImageCast
234.142.142.136/30	ImageCast
234.142.142.140/31	ImageCast
234.142.142.142	ImageCast
239.0.0.0/8	Scoped groups
239.252.0.0/14	Scoped groups
239.234.5.6	ECopy ShareScan

One site gave figures for matches/hits on its filters; it may be interesting to gather such statistics at other sites.

Different networks make different use of the scoped address space under 239.0.0.0/8, which may lead to different organisational filters in different scenarios. Organisation-local scope IPv4 multicast addressing is described in [RFC2365].

The SSM range 232.0.0.0/8 should not be carried in MSDP peerings; this is an example of different policy applied at the site border to an MSDP peering. Usually the filters are probably the same though.

As a general principle, multicast sourced from private address ranges [RFC1918] or from 169.254.0.0/16, 192.0.2.0/24 or 127.0.0.0/8 should be dropped, regardless of the multicast destination.

In certain cases, rate limiting may be desirable, where complete filtering might not, e.g. in mitigating against SAP [RFC2974] storms, or against unintended MSDP SA bursts.

Where BSR is deployed, a site should consider dropping BSR packets at its border, both BSR messages and C-RP messages. Except for Embedded-RP it probably makes sense to drop PIM register messages at the site border, unless a site's RP is external.

3. Organisational filtering

As described in [RutgersProposal], a site may use multiple organisational scopes within its site, which may use different blocks from 239.0.0.0/8, and thus require appropriate filtering at boundaries, e.g. between metropolitan campuses.

4. Subnet filtering

Two respondents are currently filtering uPNP between subnets, and one is filtering mDNS. One reason for the uPNP filtering was due to issues with errant Ricoh printers which flood announcements with too-large TTLs.

Subnet filtering may help protect against other forms of misconfigured client subnets. One site has networks that consist of multiple edge routers, where the outside 'LAN side' is strictly meant to be for local subnets only, and all intranet comms are to go through the 'WAN interface'. They have had cases where multihomed client networks were misconfigured, cross-connecting IP subnets with layer 2 boxes. To prevent multiplication of multicasts, they configure all edge routers in the intranet to accept multicast packets from the 'LAN side' only if the source IP of the multicast packets belongs to the IP subnet of that LAN. So it's a simple filter, with no scaling issues.

At least one site is filtering multicast traffic from its wireless links; this is presumably streamed video or audio content. Multicast support is required on wireless links for IPv6 operation. At layer 2, multicast IPv6 Router Advertisements may be filtered on ports that do not have known routers attached.

One site is running per-subnet boundary filters on its wired multicast-enabled subnets. The list below reflects these. One could add local scope relative addresses, though in practice the latter would all fall under 239.255.0.0/16 if it is the smallest scope group applied to a subnet.

224.0.1.1	NTP
224.0.1.2	SGI-Dogfight
224.0.1.3	Rwhod
224.0.1.8	SUN NIS+
224.0.1.24	microsoft-ds
224.0.1.25	nbc-pro
224.0.1.60	hp-device-disc
224.0.1.76	IAPP
224.0.2.1	rwho
224.0.2.2	SUN RPC
234.21.81.1	Limewire
239.255.0.0/16	subnet scope

The importance of such subnet filtering may depend on TTLs used.

5. Conclusions

This text is a very drafty first version of a document aimed to summarise the use of multicast filtering practices in the wild. It includes filters at various boundaries as well as MSDP SA filters. Further feedback on the text, and the practices reported to date is welcomed.

6. Security Considerations

There are no extra security consideration for this document.

7. IANA Considerations

There are no extra IANA consideration for this document.

8. Acknowledgments

The author would like to thank the following people for their contributions to this text: Scott Bertilson, Alan Buxey, Bruce Curtis, Andy Gatward, Bob Gerdes, Jeffry J. Handal, Lonnie Leger, Bert Manfredi, Garry Peirce, William F. Maton Sotomayor, and Stig Venaas.

9. References

[RFC1918]	Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G. and E. Lear, "Address Allocation for

	Private Internets", BCP 5, RFC 1918, February 1996.
[RFC2365]	Meyer, D., "Administratively Scoped IP Multicast", BCP 23, RFC 2365, July 1998.
[RFC2974]	Handley, M., Perkins, C. and E. Whelan, "Session Announcement Protocol", RFC 2974, October 2000.
[RFC6034]	Thaler, D., "Unicast-Prefix-Based IPv4 Multicast Addresses", RFC 6034, October 2010.
[JANETmulticast]	Price, D., "IPv4 Multicast on JANET", 2006.
[IANA6multicast]	, , "IPv6 Multicast Address Space Registry", .
[IANAmulticast]	, , "IPv4 Multicast Address Space Registry", .
[RutgersProposal]	, , "iDRAFT Proposal for RUNet Administratively Scoped Multicast", .
[I2multicast]	, , "Enabling IP Multicast with Internet2", .

Author's Address

Tim Chown Chown University of Southampton Highfield Southampton ,
Hampshire SO17 1BJ United Kingdom EMail: tjc@ecs.soton.ac.uk