Network Working Group
Request for Comments: 5135
BCP: 135
Category: Best Current Practice

D. Wing
T. Eckert
Cisco Systems, Inc.

February 2008

IP Multicast Requirements for a Network Address Translator (NAT) and a Network Address Port Translator (NAPT)

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Abstract

This document specifies requirements for a for a Network Address Translator (NAT) and a Network Address Port Translator (NAPT) that support Any Source IP Multicast or Source-Specific IP Multicast. An IP multicast-capable NAT device that adheres to the requirements of this document can optimize the operation of IP multicast applications that are generally unaware of IP multicast NAT devices.

Table of Contents

1. Introduction

In order for IP multicast applications to function well over NATs, multicast UDP must work as seamlessly as unicast UDP. However, NATs have little consistency in IP multicast operation, which results in inconsistent user experiences and failed IP multicast operation.

This document targets requirements intended to enable correct operations of Any Source Multicast and Source-Specific Multicast in devices running Internet Group Management Protocol (IGMP) proxy routing and NAT and without applying NAT to IP multicast group addresses. This profile of functionality is the expected best practice for residential access routers, small branch routers, or similar deployments.

Most of the principles outlined in this document do also apply when using protocols other than IGMP, such as Protocol Independent Multicast - Sparse Mode (PIM-SM), or when performing NAT between multiple "inside" interfaces, but explicit consideration for these cases is outside the scope of this document.

This document describes the behavior of a device that functions as a NAT for unicast flows and also forwards IP multicast traffic in either direction (’inside’ to ’outside’, or ’outside’ to ’inside’). This allows a host ’inside’ the NAT to both receive multicast traffic and to source multicast traffic. Hosts on the ’inside’ interface(s) of a NAT indicate their interest in receiving an IP multicast flow by sending an IGMP message to their local interface. An IP multicast-capable NAT will see that IGMP message (IGMPv1 [RFC1112], IGMPv2 [RFC2236], IGMPv3 [RFC3376]), possibly perform some functions on that IGMP message, and forward it to its upstream router. This causes the upstream router to send that IP multicast traffic to the NAT, which forwards it to those ’inside’ segment(s) with host(s) that had previously sent IGMP messages for that IP multicast traffic.

Out of scope of this document are PIM-SM [RFC4601] and IPv6 [RFC2460]. The IGMP Proxy devices that are scoped in this document do not forward PIM-SM. IPv6 is out of scope because NAT is not considered necessary with IPv6.

This document is a companion document to "NAT Behavioral Requirements for Unicast UDP" [RFC4787].

2. Terminology Used in This Document

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 [RFC2119].

In this document, the term "NAT" applies to both Network Address and Port Translator (NAPT) as well as a NAT that does not translate ports.

The term 'inside' refers to the interface(s) on a NAT that contain hosts that wish to source or receive IP multicast traffic. The term 'outside' refers to the interface(s) that the NAT forwards IGMP membership messages to, and where the NAT routes IP multicast traffic that originates from hosts on its 'inside' interface.

3. Background

When a NAT isn't used, a host might be connected to the Internet in a configuration such as this:

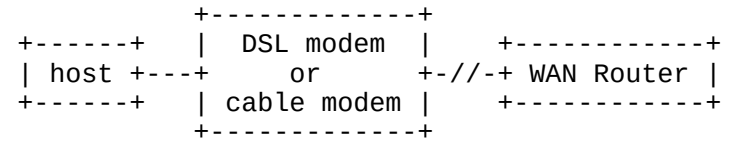

Figure 1: Network without NATing IGMP Proxy

If instead of a single host as shown in Figure 1, one or more LANs with potentially multiple hosts are to be connected, with the same type of service termination on the DSL or cable modem, a NAT device is added as shown in Figure 2. This device, in general, perform routing and NAT functions such that it does look like a single host towards the DSL/cable modem.

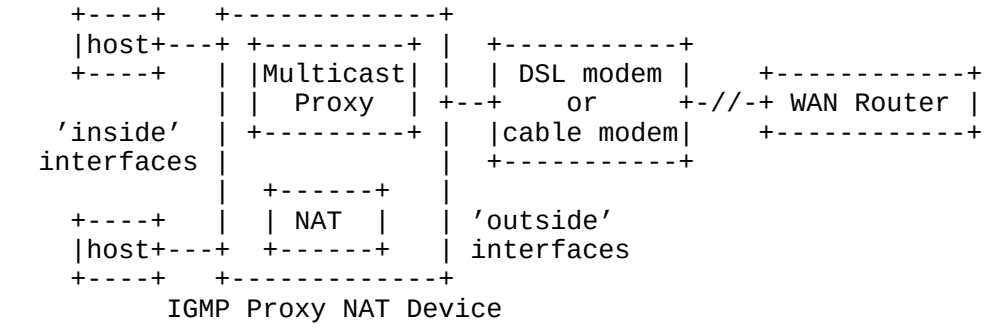

Figure 2: Network with NATing IGMP Proxy

In IP multicast, IGMP is the protocol used by hosts, such as the one shown in Figure 1. For the NAT device in Figure 2 to look like the single host for IP multicast services towards the DSL/cable modem and

to forward IP multicast traffic from and to the multiple hosts in the picture, it needs to perform so called "IGMP Proxying" [RFC4605] -- but within the context of also performing NAT. NAT is not covered by [RFC4605]. Adding NAT to IGMP proxying does not need to change the processing of the IGMP messages as defined in RFC 4605:

> IGMP messages are never logically forwarded by the IGMP proxying device, but rather sourced or received by it. In general, receipt of IGMP messages by the device updates the device's IGMP state. The updated state changes the device's forwarding of multicast messages or triggers the sending of IGMP messages. "Forwarding" of IGMP protocol messages may thus only happen implicitly by implementation optimizations that create shortcuts in this machinery.

This specifically means that IGMP protocol packets sent by the NAT device will always use the IP address of the interface ('inside' or 'outside') from which they are sent, but because those packets are logically "sourced" and not "forwarded", NAT does not have any impact on this.

Unlike unicast flows, packets with a multicast destination IP address do not have their destination IP address or destination port changed by a NAT. However, their source IP address (and source UDP port, in some cases with a NAPT) is changed if the packet goes from an 'inside' interface of a NAT to the 'outside' interface of a NAT -- similar to the behavior of a unicast packet across those same interfaces.

Adding NAT to IGMP proxying changes the processing of IP multicast data packets forwarded across the IGMP proxying device as described in the following sections. These changes actually simplify the ability to deploy IGMP proxying over a device that does *not* perform NAT.

With an IGMP Proxy NAT Device, IP multicast data traffic sourced from hosts on the 'inside' is NATed such that it will look like it is being sourced from a host directly connected to the WAN router, thus eliminating all non-standard PIM-SM concerns/configurations described in Section 3.2 of [RFC4605].

4. Requirements

4.1. NATing IP Multicast Data Packets

4.1.1. Receiving Multicast Data Packets

REQ-1: For IP multicast packets that are forwarded to a host(s) on its 'inside' interface(s), a NAT MUST NOT modify the destination IP address or destination port of the packets.

If a NAT were to modify the destination IP or port addresses, the NAT would also need to modify session announcements (e.g., electronic program guides, Session Announcement Protocol (SAP)) and session establishment and control (e.g., SIP, Real Time Streaming Protocol (RTSP)) messages. Such modifications of application messages are not considered a best practice. Furthermore, a NATed multi-homed network would need to coordinate such rewriting between its NATs.

REQ-2: A NAT MUST forward IP multicast UDP datagrams from its 'outside' interface to multicast receivers on its 'inside' interface(s).

REQ-3: A NAT SHOULD forward IP multicast non-UDP protocols (e.g., Pragmatic General Multicast (PGM) [RFC3208], Resource Reservation Protocol (RSVP) [RFC2205]) from its 'outside' interface to IP multicast receivers on its 'inside' interface(s).

4.1.2. Sending Multicast Data Packets

The following requirement is normal NAT behavior for unicast packets, as described in [RFC4787], and is extended here to provide support for IP multicast senders behind the NAT.

REQ-4: A NAT MUST modify the source IP address of packets that arrive from an 'inside' interface towards the 'outside' interface so that those packets use the NAT's 'outside' IP address(es).

a: If the NAT also performs port translation (that is, it is a NAPT), the NAT MUST also create a mapping to allow responses to that IP multicast packet to be received by the appropriate host. For Any Source Multicast, also see Section 4.3.

b: To allow hosts to learn the NAT's 'outside' interface address, the NAT MUST have "Endpoint-Independent Mapping" behavior (REQ-1 of [RFC4787]), no matter if the destination IP address is a unicast address or an IP multicast address.

c: If the NAT has multiple public IP addresses, the NAT SHOULD have an address pooling behavior of "Paired" (as described in Section 4.1 of [RFC4787]) for its IP multicast mappings as well as for its unicast UDP mappings. This allows a multicast source to discover the NAT's public IP address using a unicast address discovery mechanism (e.g., [ICE]) and communicate that discovered IP address to a multicast receiver.

REQ-5: A NAT MUST forward IP multicast UDP datagrams from its 'inside' interface(s) to its 'outside' interface.

a: NATs that support the above requirement MUST also provide a configuration option to disable this feature. Otherwise, a multihomed network would cause duplicate instances of the multicast data traffic on the public network.

As many NATs are located adjacent to bandwidth-constrained access links, it is important that IP multicast senders communicating with IP multicast receivers behind the NAT not have their flows consume bandwidth on the access link. This is accomplished by applications using administratively scoped IP addresses. Similarly, link-local multicast traffic isn't supposed to be routed off the local network.

REQ-6: The NAT's default configuration MUST NOT forward administratively scoped IP multicast traffic (239.0.0.0/8) [RFC2365] from its 'inside' interface(s) to its 'outside' interface.

REQ-7: The NAT MUST NOT forward Local Network Control Block (224.0.0/24) [RFC3171] (also known as "link-local multicast") traffic from its 'inside' interface(s) to its 'outside' interface.

4.2. IGMP Version Support

REQ-8: A NAT MAY support IGMPv1 (although IGMPv1 is considered obsolete).

REQ-9: A NAT MUST support IGMPv2.

REQ-10: A NAT SHOULD support IGMPv3.

4.2.1. IGMPv1 or IGMPv2

For IGMPv1 and IGMPv2, a NAT can successfully operate by merely forwarding IGMP membership reports and queries between the interested hosts (on its internal interface) towards its external interface.

REQ-11: If a NAT supports IGMPv1 and/or IGMPv2 (but not IGMPv3), the NAT MAY simply receive IGMP membership reports on the 'inside' interface, NAT them, and relay the IGMP membership report, and do the same function in the opposite direction to the IGMP listeners. That is, the NAT does not need to do any aggregation of IGMP messages.

- a: If a NAT relays IGMPv1 or IGMPv2 messages in this manner, it MUST NOT decrement the TTL of the IGMP messages, as they are already sent with TTL=1.

- b: However, it is RECOMMENDED that such a NAT implement IGMP/MLD Proxying [RFC4605], because IGMP aggregation provides a useful optimization.

4.2.2. IGMPv3

When an IGMPv3 proxying device receives an IGMP membership on an 'inside' interface, it creates its own IGMP proxying membership state and its own IGMP forwarding table. It then creates an independent IGMP membership report on its 'outside' interface reporting the IP multicast groups/channels -- but there is no direct relationship or "forwarding" of IGMP membership reports or queries across the interfaces. The NAT device will subsequently receive an IP multicast data packet on the 'outside' interface and forward the IP multicast packet to the 'inside' interface(s) based on its IGMP forwarding table.

By performing NAT on IGMPv3 membership reports, the membership reports appear to originate from a single IGMPv3 reporter instead of different reporters. Because IGMPv3 has different types of membership reports differentiating between status (IS_INCLUDE, IS_EXCLUDE) and change indication (e.g., TO_INCLUDE, TO_EXCLUDE), if a NAT were to interleave reports from two or more reporters (joining and leaving the same groups), the NAT would create a sequence of packets that are not compliant with an IGMPv3 reporter [RFC3376]. For this reason, the following requirements are specified:

REQ-12: If a NAT supports IGMPv3, the NAT MUST implement IGMP/MLD Proxying [RFC4605]. Such compliance causes the NAT to aggregate the IGMPv3 membership reports and report only the aggregated information upstream.

REQ-13: If a NAT supports IGMPv3, the NAT MUST implement Source-Specific Multicast (SSM) for IP [RFC4607] and IGMPv3/MLDv2 for SSM [RFC4604].

Failure to implement IGMP aggregation [RFC4605] will cause undesired temporary black holing of IP multicast traffic. For example, consider two hosts behind the same NAT. If one host is joining a session at the same time another is leaving the session, and the NAT were to merely relay the join and leave upstream, the session will be terminated, and the join and leave announcements would not comply with Section 5 of [RFC3376].

4.3. Any Source Multicast Transmitters

Any Source Multicast (ASM) uses the IP addresses in the 224/8 through 231/8, and 233/8 through 239/8 range [IANA-ALLOC].

When a host both receives an ASM stream and sends traffic into it, using RTP [RFC3550], there is a potential problem if a NAT merely followed the requirements of [RFC4787]. The problem is that RTP uses the source transport address (source IP address and source UDP port) and the Real-time Transport Protocol / RTP Control Protocol (RTP/RTCP) SSRC value to identify session members. If a session member sees the same SSRC arrive from a different transport address, that session member will perform RTP collision detection (Section 8.2 of [RFC3550]). If a NAT merely followed the requirements of [RFC4787] and timed out a UDP session after 2 minutes of inactivity and RTCP receiver reports are sent less often than every 2 minutes, RTP collision detection would be performed by other session members sharing the same SSRC, complicating diagnostic tools and potentially interfering with jitter buffer algorithms. This situation can occur, for example, with an IP multicast group of approximately 300 members with a normal 50 Kbps audio RTP stream.

Source-Specific Multicast does not need this long timer because application feedback reports are unicast (rather than IP multicast) and identifiers, rather than IP addresses and UDP ports, are used to identify a specific IP multicast receiver (e.g., [RTCPSSM].

REQ-14: If a host on the 'inside' interface of a NAT belongs to an Any Source Multicast host group and the host sends a UDP packet to the same group, the NAT SHOULD have a UDP mapping timer of 60 minutes for that mapping.

a: This UDP mapping SHOULD be destroyed when the host leaves that host group. The NAT is aware of this through receipt of an IGMP message from the host.

b: If a NAT has exhausted its resources, the NAT MAY time out that mapping before 60 minutes have elapsed, but this is discouraged. Note that even in a situation with resource exhaustion, a NAT is still required to follow the minimum mapping duration of 2 minutes (REQ-5 of [RFC4787]).

5. Requirements Summary

This section summarizes the requirements.

REQ-1: For IP multicast packets that are forwarded to a host(s) on its 'inside' interface(s), a NAT MUST NOT modify the destination IP address or destination port of the packets.

REQ-2: A NAT MUST forward IP multicast UDP datagrams from its 'outside' interface to multicast receivers on its 'inside' interface(s).

REQ-3: A NAT SHOULD forward IP multicast non-UDP protocols (e.g., PGM [RFC3208], RSVP [RFC2205]) from its 'outside' interface to IP multicast receivers on its 'inside' interface(s).

REQ-4: A NAT MUST modify the source IP address of packets that arrive from an 'inside' interface towards the 'outside' interface so that those packets use the NAT's 'outside' IP address(es).

a: If the NAT also performs port translation (that is, it is a NAPT), the NAT MUST also create a mapping to allow responses to that IP multicast packet to be received by the appropriate host. For Any Source Multicast, also see Section 4.3.

b: To allow hosts to learn the NAT's 'outside' interface address, the NAT MUST have "Endpoint-Independent Mapping" behavior (REQ-1 of [RFC4787]), no matter if the destination IP address is a unicast address or an IP multicast address.

c: If the NAT has multiple public IP addresses, the NAT SHOULD have an address pooling behavior of "Paired" (as described in Section 4.1 of [RFC4787]) for its IP multicast mappings as well as for its unicast UDP mappings. This allows a multicast source to discover the NAT's public IP address using a unicast address discovery mechanism (e.g., [ICE]) and communicate that discovered IP address to a multicast receiver.

REQ-5: A NAT MUST forward IP multicast UDP datagrams from its 'inside' interface(s) to its 'outside' interface.

a: NATs that support the above requirement MUST also provide a configuration option to disable this feature. Otherwise, a multihomed network would cause duplicate instances of the multicast data traffic on the public network.

REQ-6: The NAT's default configuration MUST NOT forward administratively scoped IP multicast traffic (239.0.0.0/8) [RFC2365] from its 'inside' interface(s) to its 'outside' interface.

REQ-7: The NAT MUST NOT forward Local Network Control Block (224.0.0/24) [RFC3171] (also known as "link-local multicast") traffic from its 'inside' interface(s) to its 'outside' interface.

REQ-8: A NAT MAY support IGMPv1 (although IGMPv1 is considered obsolete).

REQ-9: A NAT MUST support IGMPv2.

REQ-10: A NAT SHOULD support IGMPv3.

REQ-11: If a NAT supports IGMPv1 and/or IGMPv2 (but not IGMPv3), the NAT MAY simply receive IGMP membership reports on the 'inside' interface, NAT them, and relay the IGMP membership report, and do the same function in the opposite direction to the IGMP listeners. That is, the NAT does not need to do any aggregation of IGMP messages.

a: If a NAT relays IGMPv1 or IGMPv2 messages in this manner, it MUST NOT decrement the TTL of the IGMP messages, as they are already sent with TTL=1.

b: However, it is RECOMMENDED that such a NAT implement IGMP/MLD Proxying [RFC4605], because IGMP aggregation provides a useful optimization.

REQ-12: If a NAT supports IGMPv3, the NAT MUST implement IGMP/MLD Proxying [RFC4605]. Such compliance causes the NAT to aggregate the IGMPv3 membership reports and report only the aggregated information upstream.

REQ-13: If a NAT supports IGMPv3, the NAT MUST implement Source-Specific Multicast (SSM) for IP [RFC4607] and IGMPv3/MLDv2 for SSM [RFC4604].

REQ-14: If a host on the 'inside' interface of a NAT belongs to an Any Source Multicast host group and the host sends a UDP packet to the same group, the NAT SHOULD have a UDP mapping timer of 60 minutes for that mapping.

a: This UDP mapping SHOULD be destroyed when the host leaves that host group. The NAT is aware of this through receipt of an IGMP message from the host.

b: If a NAT has exhausted its resources, the NAT MAY time out that mapping before 60 minutes have elapsed, but this is discouraged. Note that even in a situation with resource exhaustion, a NAT is still required to follow the minimum mapping duration of 2 minutes (REQ-5 of [RFC4787]).

6. Security Considerations

The Security Considerations sections of IGMPv3 [RFC3376] and IGMP Proxying [RFC4605] apply to a device complying with this document.

When a host is using RTP and participating in an Any Source Multicast session, the host's periodic RTCP receiver reports cause the NAT to create a mapping. When the group size is less than approximately 300, the RTCP reports are sent frequently enough that a NAT's mapping will always be kept open. When the group size is larger than approximately 300, the RTCP reports are sent less frequently. The recommendation in Section 4.3 causes the NAT mapping to be kept open for the duration of the host's participation in that IP multicast session no matter the size of the multicast host or periodicity of the host's RTCP transmissions.

7. Acknowledgments

Thanks to Jari Arkko, Yiqun Cai, Stephen Casner, Remi Denis-Courmont, Lars Eggert, Gorry Fairhurst, Alfred Hines, Prashant Jhingran, Bharat Joshi, Francois Le Faucheur, Albert Manfredi, Marcus Maranhao, Bryan McLaughlin, Chris Newman, Tim Polk, Pekka Savola, Mark Townsley, Magnus Westerlund, and Stig Venaas for their assistance in writing this document.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC2365] Meyer, D., "Administratively Scoped IP Multicast", BCP 23, RFC 2365, July 1998.

[RFC3171] Albanna, Z., Almeroth, K., Meyer, D., and M. Schipper, "IANA Guidelines for IPv4 Multicast Address Assignments", BCP 51, RFC 3171, August 2001.

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

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[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, 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.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

8.2. Informative References

[IANA-ALLOC] Internet Assigned Numbers Authority, "Internet Multicast Addresses", <http://www.iana.org/assignments/multicast-addresses>.

[ICE] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", Work in Progress, October 2007.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3208] Speakman, T., Crowcroft, J., Gemmell, J., Farinacci, D., Lin, S., Leshchiner, D., Luby, M., Montgomery, T., Rizzo, L., Tweedly, A., Bhaskar, N., Edmonstone, R., Sumanasekera, R., and L. Vicisano, "PGM Reliable Transport Protocol Specification", RFC 3208, December 2001.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

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

[RTCPSSM] Ott, J., Chesterfield, J., and E. Schooler, "RTCP Extensions for Single-Source Multicast Sessions with Unicast Feedback", Work in Progress, January 2008.

Appendix A. Application Considerations

SSM requires listeners to know the SSM channel (S,G), which is comprised of the IP source address (S) and the IP multicast group (G). An SSM source needs to communicate its IP address in its SSM session establishment message (e.g., in its Session Description Protocol (SDP) [RFC4566]). When the SSM sender is behind a NAT and the SSM receiver(s) are on the other side of that NAT, the SSM sender will need to determine its IP source address relevant to the SSM receivers; generally, this will be the 'outside' IP address of the NAT. This 'outside' address needs to be included in the SSM session establishment message (e.g., SDP) so that listeners on the 'outside' of the NAT can receive the SSM channel.

If there are SSM listeners on both the 'outside' and 'inside' of the NAT, it may be valuable to consider using ICE [ICE] in the session advertisement; the full scope of the interaction between SSM and ICE is beyond the scope of this document.

If multiple SSM sources on the 'inside' of a NAT choose the same multicast group address, those sources are uniquely identifiable because their IP addresses are unique. However, if their multicast traffic is NATed and sent on the NAT's public interface, the traffic from those individual sources is no longer uniquely identifiable. This will cause problems for multicast receivers, which will see an intermixing of traffic from those sources. Resolution of this issue is left for future study. In the meantime, applications that source SSM multicast traffic are encouraged to allow the user to modify the multicast SSM address so that users can avoid this problem if that application is placed behind a NAT.

A multicast source that wants its traffic to not traverse a router (e.g., leave a home network) may find it useful to send traffic with IP TTL=1. Both ASM and SSM sources may find this useful.

As many NATs use the same private address space (e.g., 192.168.0.0/16, [RFC1918]), RTP stacks are encouraged to generate CNAMEs properly (see end of Section 6.5.1 of [RFC3550].)

Authors' Addresses

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

EMail: dwing@cisco.com

Toerless Eckert
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

EMail: eckert@cisco.com

Full Copyright Statement

Intellectual Property