IGMP Proxy Behavior
draft-wing-behave-multicast-00

Status of this Memo

Copyright Notice

Abstract

   This document describes the behavior of an IGMP Proxy, as implemented
   in NAT devices, and places requirements on such devices.

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 RFC 2119 [1].

Table of Contents

1. **Problem Statement**

    For users to accept and enjoy multicast, multicast UDP must work as
    seamlessly as unicast UDP. However, today's equipment has little
    consistency in multicast operation which results in inconsistant user
    experiences and failed multicast operation.

2. **Document Scope**

    This document describes the behavior of a device which:

    o   functions as an IGMP proxy on behalf of hosts,
    o   receives multicast traffic from one interface (typically its WAN
        interface) and sends that multicast traffic to other interface(s),
    o   uses IGMPv2 or IGMPv3, and
    o   uses IPv4.

    Specifically out of scope are:

    o   sending multicast traffic,
    o   PIM-SM [13],
    o   IPv6, and,
    o   IGMPv1.

    Sending multicast traffic is out of scope because it requires NATting
    the source IP address of such transmitted multicast traffic.
    Similarly, PIM is used only between routers and the IGMP Proxy
    devices that are scoped in this document do not function as routers.
    IPv6 is out of scope because NAT is not considered necessary with
    IPv6. IGMPv1 is not significantly deployed on the Internet.

    This document does not describe how to implement multicast, IGMPv2,
    or IGMPv3 in an IGMP Proxy device. Rather, it provides requirements
    for an IGMP Proxy device so that hosts behind the NAT can receive
    multicast traffic without any knowledge of the IGMP Proxy.

3. **Introduction**

    As detailed in the Document Scope section, the primary functions of
    an IGMP proxy device are to collect IGMP traffic from one interface
    and relay it to another interface, and accept multicast traffic from

thatinterface and route -- or replicate it -- to other interface(s).

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

```
              +-------------+
  +------+    |  DSL modem  |         +------------+
  | host +---+     or       +---//---+ WAN Router |
  +------+    | cable modem |         +------------+
              +-------------+
```
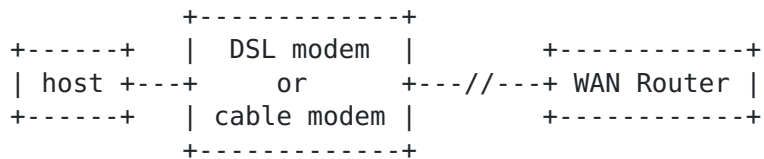
When an IGMP Proxy (NAT) device is added to such a network, its
behavior is identical towards the upstream (WAN) router.
Specifically, when dealing with multicast, the IGMP Proxy has the
same behavior towards the WAN as if it was a host.

```
  +------+  +------------+   +-------------+
  | host +--+            |   |  DSL modem  |         +------------+
  +------+  | IGMP Proxy +---+     or       +---//---+ WAN Router |
  +------+  |    (NAT)   |   | cable modem |         +------------+
  | host +--+            |   +-------------+
  +------+  +------------+
```
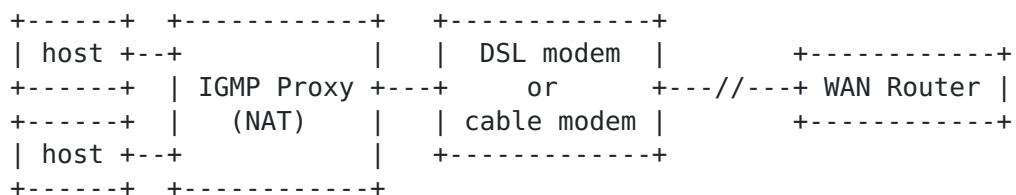
This document specifies how an IGMP Proxy provides multicast
functionality to the hosts on its local LAN.

At the time of this writing, IGMPv2 [2] is still a common multicast
signaling protocol, although new applications are now using IGMPv3
[3]. This document describes NAT requirements for both IGMPv2 and
IGMPv3.

This document is a companion document to "NAT/Firewall Behavioral
Requirements" [6], and uses the terminology defined in that document.

3.1 Host Multicast Overview

A host interested in receiving multicast traffic indicates its
interest by sending an IGMP message to its local LAN. The contents
of the IGMP message and the IP destination address is different for
IGMPv2 and IGMPv3; see IGMPv2 [2] section 9 and IGMPv3 [3] section
4.2.14 for details.

The basic host operation is:

o the IGMP Proxy listens on the for an IGMP message from hosts on
      its local network,
   o an application learns of a multicast address it's interested in
      receiving. This usually occurs via some sort of signaling (such
      as SIP [10] or SAP [8]), or by a user entering a multicast address
      directly into an application,

o the application sends an IGMP membership report to the local
   network,
o The NAT performs specific aggregation functions (detailed in
   RFC2236 and RFC3376), creates a NAT binding, and informs the
   upstream WAN router of its interest in receiving the multicast
   traffic by sending an IGMP membership report to the upstream
   router,
o To indicate continued interest in recieving the multicast traffic,
   the application periodically re-transmits IGMP membership report
   messages, and these are aggregated by the NAT and periodically
   transmitted to the upstream router,
o when all multicast listeners are no longer interested in multicast
   traffic (either due to not sending membership reports, or due to
   the NAT querying the hosts using IGMP), the NAT closes its NAT
   binding and informs the upstream WAN router to cease sending
   multicast traffic.

An IGMP Proxy would perform these operations, and would also route --
or replicate -- incoming multicast traffic to the interface(s) where
a host is interested in that multicast traffic.

4. NAT IGMP Proxy Requirements

This section lists the specific requirements for NATs that implement
IGMP Proxies.

4.1 Perform Host and IGMP Proxy Functions

The IGMP Proxy MUST perform functions as if it were a host, as
outlined in Section 3.1. Additionally, the IGMP Proxy MUST also
route incoming multicast packets to the interface that contained the
host(s) interested in that multicast traffic. If hosts on multiple
interfaces are interested in the same multicast traffic, the IGMP
Proxy MUST replicate the traffic so that it is sent to all interfaces
with interested hosts.

4.2 IGMP Packets Sent Towards WAN Interface

The IGMP packets sent by the NAT MUST follow the requirements in
RFC3376 section 4 [3], specificially the TTL MUST be 1, IP precedence
MUST be Internetwork Control (Type of Service 0xc0), and it MUST
carry the IP Router Alert option.

The IGMP packets sent by the NAT towards the WAN MUST use the NAT's
public IP address as the source IP address.

4.3 Keep NAT Binding Open

The BEHAVE [6] document only requires that a NAT binding be kept open
for inside-to-outside UDP flows. However, with multicast traffic,
UDP traffic will only arrive outside-to-inside.

Hosts will periodically send IGMP Report messages to indicate
continued interest in receiving the multicast traffic. As long as
the IGMP Proxy sees a host is interested in receiving the flow, the
NAT MUST continue to receive multicast traffic from the WAN and send
it to the interfaces with interested hosts.

Per IGMPv3, the default transmission interval for the periodic
Membership Report is one second. Per IGMPv2, the default
transmission interval for the periodic Unsolicited Report Interval is
10 seconds. If a host no longer sends its periodic messages within
those timeframes, the NAT MAY consider the host no longer wants to
receive the multicast traffic and can inform the upstream WAN router
and close the NAT binding. However, it is suggested that the NAT
wait until 3 missing unsolicited reports (to account for packet loss
on the LAN, especially wireless LANs), or that the NAT first query
the host using IGMPv2 or IGMPv3.

4.4 Support Non-UDP Traffic

Although multicast traffic is usually UDP, multicast traffic is not
required to be UDP. Thus, a NAT MUST support multicast traffic of
any IP protocol. This behavior will allows for seamless support of
emerging protocols. This behavior MAY be configurable by the user.

4.5 Inform Upstream Router of Multicast Interest

As long as a host is interested in receiving a multicast stream, the
IGMP Proxy -- because it is acting like a host -- MUST also send
periodic IGMP Report messages to the upstream WAN router to indicate
continued interest in receiving the multicast traffic.

When all listeners behind the IGMP Proxy are no longer interested in
the multicast traffic, the NAT MUST inform the upstream (WAN) router
by sending an updated IGMP Membership Report, and the NAT MUST also
delete its NAT binding. Informing the upstream router quickly is
necessary to avoid wasting the bandwidth of the access link.

5. RTP Considerations

A signficant use of multicast is RFC3550 [4] (RTP), which runs over
UDP. A multicast listener would receive RTP over multicast UDP on
port X, and would send unicast RTCP to the multicast RTP transmitter

over port Y. Although RFC3550 implies that X+1=Y, the NAT MUST NOT
make this assumption because signaling can specify an alternate port
for RTCP[5].

6. Security Considerations

Compliance with this specification does not increase security risks
beyond those already discussed in the Security Considerations section
of IGMPv3 [3].

7. IANA Considerations

This document does not require any IANA registrations.

8. Acknowledgments

Thanks to Bryan McLaughlin and Yiqun Cai for their assistance in
writing this document.

9. References

9.1 Normative References

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

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

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

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

[5]   Huitema, C., "Real Time Control Protocol (RTCP) attribute in

Session Description Protocol (SDP)", RFC 3605, October 2003.

[6]   Jennings, C., "NAT/Firewall Behavioral Requirements",
      draft-audet-nat-behave-00 (work in progress), July 2004.

9.2 Informational References

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

[8]   Handley, M., Perkins, C. and E. Whelan, "Session Announcement
        Protocol", RFC 2974, October 2000.

[9]   Srisuresh, P. and K. Egevang, "Traditional IP Network Address
        Translator (Traditional NAT)", RFC 3022, January 2001.

[10]   Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A.,
        Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP:
        Session Initiation Protocol", RFC 3261, June 2002.

[11]   Droms, R., "Dynamic Host Configuration Protocol", RFC 2131,
        March 1997.

[12]   Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D. and
        R. Wheeler, "A Method for Transmitting PPP Over Ethernet
        (PPPoE)", RFC 2516, February 1999.

[13]   Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S.,
        Handley, M. and V. Jacobson, "Protocol Independent
        Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC
        2362, June 1998.

Author's Address

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

    EMail: dwing@cisco.com

Intellectual Property Statement

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights 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; nor does it represent that it has
   made any independent effort to identify any such rights. Information
   on the procedures with respect to rights in RFC documents can be
   found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this
   specification can be obtained from the IETF on-line IPR repository at
   http://www.ietf.org/ipr.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights that may cover technology that may be required to implement
   this standard. Please address the information to the IETF at
   ietf-ipr@ietf.org.

Disclaimer of Validity

   This document and the information contained herein are provided on an
   "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS
   OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET
   ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,
   INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE
   INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED
   WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

   Copyright (C) The Internet Society (2004). This document is subject
   to the rights, licenses and restrictions contained in BCP 78, and
   except as set forth therein, the authors retain all their rights.

Acknowledgment

Wing   Expires April 17, 2005   [Page 9]