

IDMR Working Group
Internet Draft
Document: [draft-tsenevir-pim-sm-snoop-00.txt](#)
Category: Informational

Tissa Senevirathne
Sridhar Vallepali

Force10 Networks
April, 2002

Protocol Independent Multicast-Sparse Mode (PIM-SM) Snooping

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#) [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at

<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at

<http://www.ietf.org/shadow.html>.

For potential updates to the above required-text see:

<http://www.ietf.org/ietf/1id-guidelines.txt>

Abstract

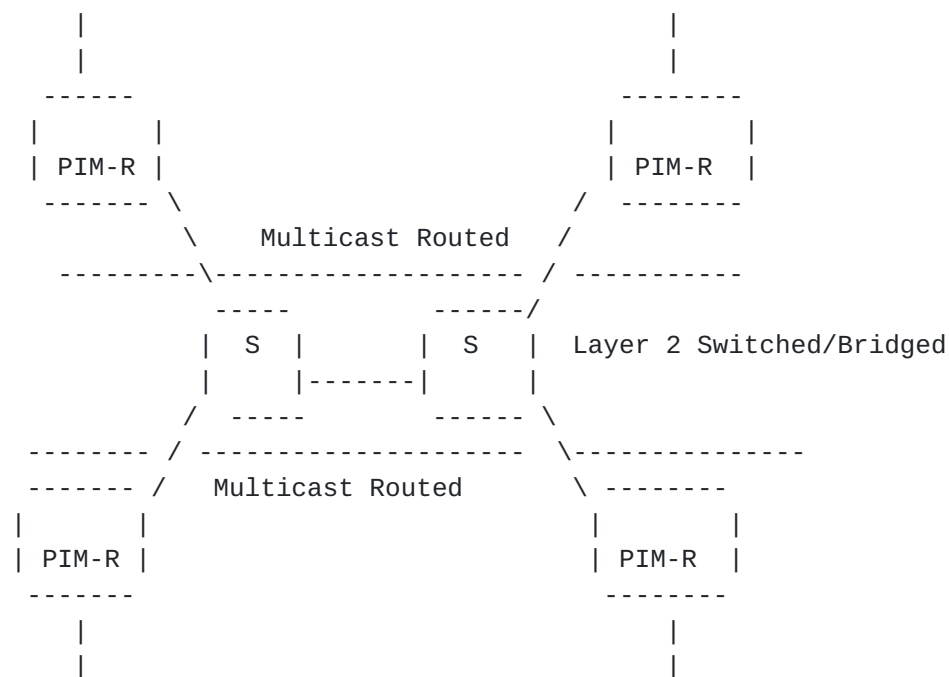
This document provides PIM-SM snooping solution. In the document we present the framework and reference model and required PIM-SM messages for PIM-SM snooping solutions. Also we attempt to discuss related issues to PIM-SM snooping.

Conventions 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](#) [2].

1. Introduction

IGMP snooping is popularly used to limit the scope of IP multicast traffic in enterprise Local Area Networks (LAN). With the recent popularity of Layer 2 Networks in core of the networks, PIM-SM snooping is gaining popularity as a way of constraining IP multicast traffic to the section of network that is interested in receiving such traffic.



PIM-R - PIM-SM Routers

S - PIM-SM Snooping Device

Fig: Reference Model of PIM-SM snooping

2. PIM-SM Snooping Framework

Devices that implement PIM-SM snooping are required have ability to

1. Intercept Join/Prune messages [3]
2. Ability to create IP Multicast scope per VLAN (Virtual LAN) basis.
3. MUST not have impact on other Multicast traffic
4. MUST not modify packet content (such as TTL..) or in other words MUST be forwarded using Layer 2 forwarding rules.

Senevirathne Informational - Expiration October 2002

2

[draft-tsenevir-pim-sm-snooping-00.txt](#)

April 2002

3. Theory of Operation

Let assume that

VLAN V has interfaces $I == \{i1, i2, ..ij...in\}$

Let assume we identified, by snooping PIM-SM join messages, that interface set G need to join (*,G) or (S,G). These interfaces Let call outgoing interfaces.

$G == \{o1, o2, ..oj...om\}$; G subset of I .

Now create a sub-scope S within the VLAN such that

input interfaces == I and

out put interfaces == G

3.1 Maintaining outgoing interfaces

outgoing interface (o) is added to the list when a join message is received from that interface.

When an interface is added to the G a Hold timer is created for each interface. Periodic Join messages update the life.

When there are more than one Join is received from a given interface the largest hold time MUST be used.

When hold time expires the interface SHOULD be removed from that group for that VLAN.

When a Prune message is received the interface SHOULD be removed from that group for that VLAN.

If more than one Join message was received from an interface and a Prune message is received the Hold timer MUST be update according to the other active Joins.

3.2 (*,G) vs (S,G)

Devices that perform PIM-SM snooping is practically operating as a Layer 2 device. When PIM-SM is not implemented entire VLAN is the IP Multicast scope. The scope of PIM-SM snooping is to constrain the IP Multicast data flooding. As such, PIM-SM snooping does not attempt to distinguish between (*,G) and (S,G). In effect PIM-SM snooping implement (V,G). Where V is all interface of the VLAN V. Such generalization, simplify the implementation; serves the purpose and avoid blackholes when IP routing changes the RPF interfaces.

4. Security Considerations

PIM-SM snooping does not affect the security aspects of PIM-SM.

Senevirathne Informational - Expiration October 2002 3

 [draft-tsenevir-pim-sm-snooping-00.txt](#) April 2002

5. References

- 1 Bradner, S., "The Internet Standards Process -- Revision 3", [BCP 9](#), [RFC 2026](#), October 1996.
- 2 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997
- 3 Estrin, D., et.al, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, [RFC 2362](#), June 1998.

10. Acknowledgments

11. Author's Addresses

Tissa Senevirathne
1440 McCarthy Blvd
Milpitas, CA
Phone: 408-965-5103
Email: tsenevir@force10networks.com

Sridhar Vallepali
1440 McCarthy Blvd
Milpitas, CA
Phone: 408-571-3500

Senevirathne Informational - Expiration October 2002 4
[draft-tsenevir-pim-sm-snooping-00.txt](#) April 2002

Full Copyright Statement

"Copyright (C) The Internet Society (2002). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into

