Internet Engineering Task Force (IETF)
Request for Comments: 6516
Category: Standards Track
ISSN: 2070-1721

Y. Cai
E. Rosen, Ed.
IJ. Wijnands
Cisco Systems
February 2012

IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages

Abstract

The specification for Multicast Virtual Private Networks (MVPNs) contains an option that allows the use of PIM as the control protocol between provider edge routers. It also contains an option that allows UDP-based messages, known as Selective Provider Multicast Service Interface (S-PMSI) Join messages, to be used to bind particular customer multicast flows to particular tunnels through a service provider's network. This document extends the MVPN specification (RFC 6513) so that these options can be used when the customer multicast flows are IPv6 flows.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6516.

Table of Contents

1. Introduction

The Multicast Virtual Private Network (MVPN) specification [RFC6513] defines the notion of a "PMSI" (Provider Multicast Service Interface) and specifies how a PMSI can be instantiated by various kinds of tunnels through a service provider's network ("P-tunnels"). It also specifies the procedures for using PIM (Protocol Independent Multicast [RFC4601]) as the control protocol between Provider Edge (PE) routers. When PIM is used as the control protocol, PIM messages are sent through a P-tunnel from one PE in an MVPN to others in the same MVPN. These PIM messages carry customer multicast routing information. However, [RFC6513] does not cover the case where the customer is using IPv6, but the service provider is using P-tunnels created by PIM over an IPv4 infrastructure.

The MVPN specification [RFC6513] also specifies "S-PMSI (Selective PMSI) Join" messages, which are optionally used to bind particular customer multicast flows to particular P-tunnels. However, the specification does not cover the case where the customer flows are IPv6 flows.

This document extends [RFC6513] by adding the specification for handling customer IPv6 multicast flows when a service provider is using PE-PE PIM and/or S-PMSI Join messages over an IPv4 infrastructure. This document also specifies how to send multiple S-PMSI Join messages in a single UDP datagram.

This document uses terminology defined in [RFC6513]: C-source, C-group, C-flow, P-group, and (C-S,C-G).

2. Specification of Requirements

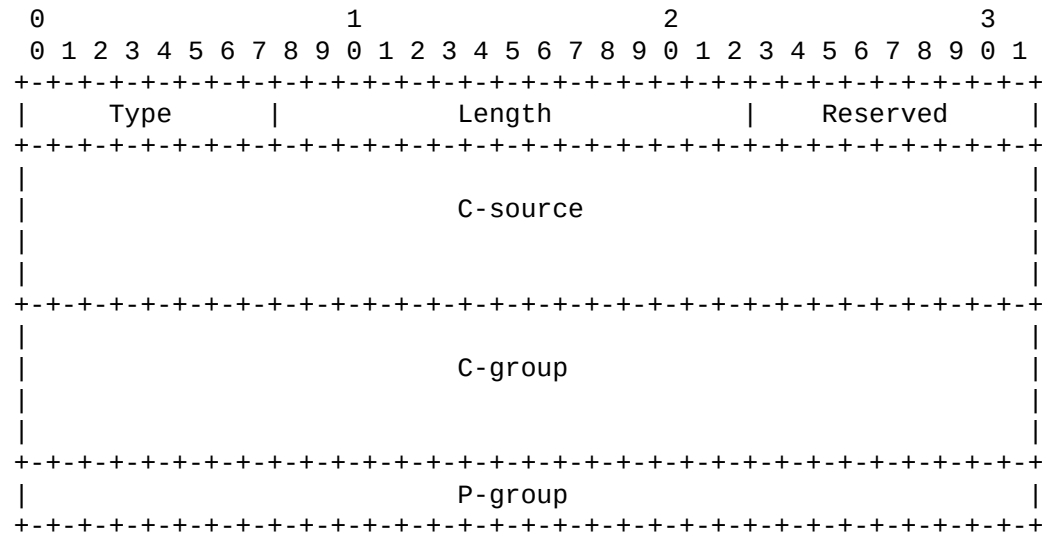
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. S-PMSI Joins Binding IPv6 Flows to GRE/IPv4 P-Tunnels

The S-PMSI Join message is defined in Section 7.4.2.2 of [RFC6513]. These messages contain a type field, and [RFC6513] defines only Type 1 S-PMSI Joins. A Type 1 S-PMSI Join may be used to assign a customer IPv4 (C-S,C-G) flow to a P-tunnel that is created by PIM/IPv4. To transmit data or control packets over such a P-tunnel, the packets are encapsulated in GRE (Generic Routing Encapsulation) within IPv4, as specified in Section 12 of [RFC6513].

In this document, we define the Type 4 S-PMSI Join. A Type 4 S-PMSI Join may be used to assign a customer IPv6 (C-S,C-G) flow to a P-tunnel that is created by PIM/IPv4. GRE/IPv4 encapsulation is used to send data or control packets on the P-tunnel.

3.1. Encoding



Type (8 bits): 4

Length (16 bits): 40, the length in octets of the entire S-PMSI Join message, including the Type, Length, Reserved, C-source, C-group, and P-group fields.

Reserved (8 bits): this field SHOULD be zero when transmitted and MUST be ignored when received.

C-source (128 bits): the IPv6 address of the traffic source in the VPN.

C-group (128 bits): the IPv6 group address of the multicast traffic.

P-group (32 bits): the IPv4 group address identifying the P-tunnel. Data packets sent on this tunnel are encapsulated in IPv4 GRE packets with this group address in the IP destination address field of the outer header.

3.2. Encapsulation of S-PMSI Joins in UDP Datagrams

All S-PMSI Joins are encapsulated in UDP datagrams [RFC768]. A Type 4 S-PMSI Join MUST be encapsulated in an IPv6 UDP datagram. The IPv6 source address field of these datagrams SHOULD be the IPv4-mapped IPv6 address [RFC4291] corresponding to the IPv4 address that the originating PE router uses as its source address in the instance of PIM that is used to create the specified P-tunnel.

A single UDP datagram MAY carry multiple S-PMSI Join messages, as many as can fit entirely within it. If there are multiple S-PMSI Joins in a UDP datagram, they MUST be of the same S-PMSI Join type. The end of the last S-PMSI Join (as determined by the S-PMSI Join length field) MUST coincide with the end of the UDP datagram, as determined by the UDP length field. When processing a received UDP datagram that contains one or more S-PMSI Joins, a router MUST process all the S-PMSI Joins that fit into the datagram.

4. PE-PE PIM/IPv6 over an IPv4 P-Tunnel

If a VPN customer is using PIM over IPv6, but the SP (service provider) is using an IPv4 infrastructure (i.e., is using an IPv4-based control protocol to construct its P-tunnels), then the PE routers will need to originate IPv6 PIM control messages. The IPv6 Source Address field of any such IPv6 PIM control message SHOULD be the IPv4-mapped IPv6 address [RFC4291] corresponding to the IPv4 address that the originating PE router uses as its source address in the instance of PIM that is used to create the specified P-tunnel. If the IPv6 Destination Address field is the multicast address ALL-PIM-ROUTERS, the IPv6 form of the address (ff02::d) is used. These IPv6 PIM control messages are, of course, not transmitted natively over the service provider’s network but rather are encapsulated in GRE/IPv4.

5. IANA Considerations

[RFC6513] created an IANA registry for the "S-PMSI Join Message Type Field". This document registers a new value in that registry:

Value: 4
Description: GRE S-PMSI for IPv6 traffic (unaggregated)

6. Security Considerations

There are no additional security considerations beyond those of [RFC6513].

7. Acknowledgments

The authors wish to thank DP Ayyadevara, Arjen Boers, Rayen Mohanty, Rajesh Sharma, and Karthik Subramanian.

8. Normative References

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 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.

[RFC6513] Rosen, E., Ed., and R. Aggarwal, Ed., "Multicast in MPLS/BGP IP VPNs", RFC 6513, February 2012.

Authors' Addresses

Yiqun Cai
Cisco Systems, Inc.
170 Tasman Drive
San Jose, CA 95134
EMail: ycai@cisco.com

Eric C. Rosen (editor)
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
EMail: erosen@cisco.com

IJsbrand Wijnands
Cisco Systems, Inc.
De kleetlaan 6a Diegem 1831
Belgium
EMail: ice@cisco.com