SPRING Working Group W. Wang
Internet-Draft A. Wang
Intended status: Standards Track China Telecom
Expires: 24 April 2023 21 October 2022

Segment Encoding and Procedures For Multicast VPN Service in Native IPv6 Network

draft-wang-spring-multicast-vpn-segment-00

Abstract

This draft defines a new segment type for Multicast VPN, which contains the information of VPN customer. This segment type can be used for customer traffic differentiation by destination address on egress PEs, and assures the source and destination address not changed during the transmission.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 24 April 2023.

Copyright Notice

Table of Contents

1. Introduction

Segment Routing([RFC8402]) uses an ordered list of segments to forward packets. Each segment represents a specific function(as described in [RFC8986]), which is usually used as IPv6 destination address and provide the possibility of network programming.

In this draft, we define a new segment type for Multicast VPN---- End.MVPN. This segment type contains Routing Distinguisher (RD) and multicast group information of the VPN customer. The egress PEs can distinguish the traffic of different VPN customers according to this segment, which can be used to perform customer-level traffic statistics, detection and other operations. Egress PEs can obtain VPN customer information from the segment directly without further analysis of data packets.

2. 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 [RFC2119] .

3. Applied scenario

The applied scenario is shown in Figure 1.

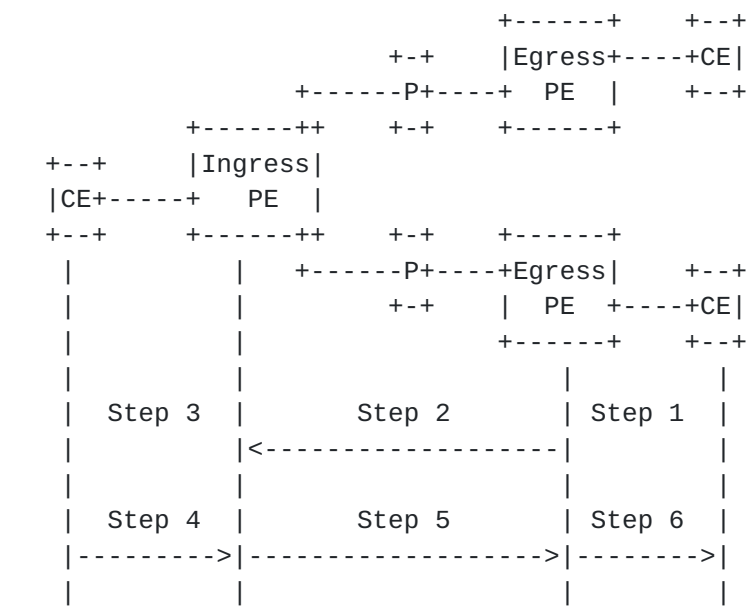

Figure 1: The applied scenario

Where:

Step 1: Egress PE generate an End.MVPN according to the multicast IP address and multicast group information of the VPN customer.

Step 2: Egress PE sends End.MVPN to ingress PE via BGP/PCEP.

Step 3: The ingress PE will maintain a mapping table of End.MVPN and (RD, multicast group address) tuple (called "End.MVPN mapping table").

Step 4: When a packet arrives at ingress PE, it will be encapsulated with a header according to the End.MVPN mapping table, and the destination address will be set to End.MVPN.

Step 5: When the packet arrives at Egress PEs, they will distinguish which VPN customer it belongs to and determine the CEs receiving the packet according to End.MVPN.

Step 6: Egress PEs copy the packet according to the number of CEs receiving the packet, and transmit copies of the packet to the corresponding CEs.

This solution allows the multicast network to distinguish different customers' traffic by destination address, just like the solution in unicast multicast network.

4. Format of End.MVPN

The architecture of IPv6 multicast address is described in [RFC7371]. The encoding format of End.MVPN conforms to the IPv6 multicast address, as shown in Figure 1.

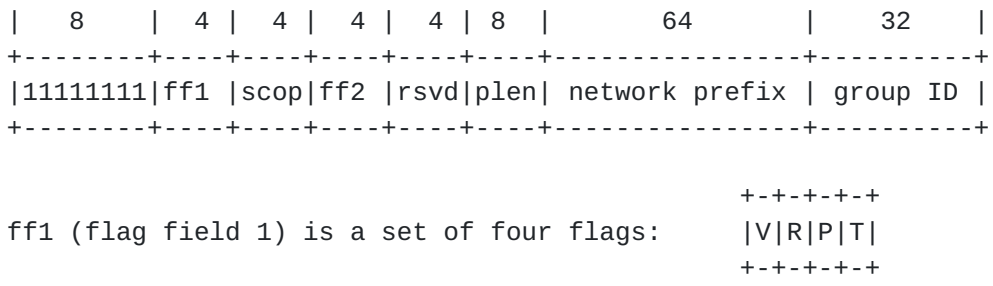

Figure 1: The format of End.MVPN

The highest bit in ff1 is set to "VPN Muticast Bit", which can be abbreviated as "V" bit.

* V bit (1 bit): When it is set, it means the multicast group address is an End.MVPN SID. Otherwise, it is a common multicast address.

* network prefix (64 bits): When "V" is set, this field carries the customer's RD. Otherwise, the information carried in this field should be determined by the other bits in ff1.

* group ID (32 bits): This field carries the information of customer group, the determination rules of values in described in Section 6.

The meanings and values of other fields follow the rules in [RFC7371].

5. End.MVPN mapping table

During the transimission of multicast VPN packet, the destination address in header is End.MVPN SID, which is generated by egress PE. Due to the header is encapsulated by ingress PE, it needs a method to determine which End.MVPN should be assigned to the packet.

On ingress PE, a "End.MVPN mapping table" should be maintain to save the mapping between End.MVPN SID and (RD, multicast group address). Its structure is illustrated as follow:

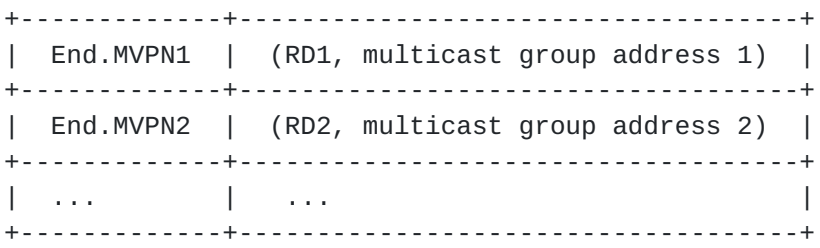

Figure 2: The mapping table between End.MVPN and (RD, multicast group address)

6. The generation of End.MVPN

The format of End.MVPN is defined in Section 4. End.MVPN is generated by egress PE and transmitted to ingress PE. The generation of End.MVPN is shown as follows:

1. egress PE extract the RD and multicast group address of a customer.

2. egress PE set the value of "V" bit to 1, and set the value of "network prefix" to the customer's RD.

3. egress PE set the value of "group ID" field according to the customer's multicast group address obtained in step 1:

   * If the multicast group address of customer is an IPv4 address, the value of "group ID" field should be set to the IPv4 multicast group address.

   * If the multicast group address of customer is an IPv6 address, the information carried in "group ID" field depends on the "P" bit in the multicast group address of customer:

     - If the "P" bit is 1, egress PE set the value of "group ID" to the group ID in the customer's multicast group address.

     - If the "P" bit is 0, egress PE set the value of "group ID" to a 32-bit value that is hashed from the customer's multicast group address.

Note that when a End.MVPN is being generated, if "V" bit is set to 1, the "P" bit must be set to 1 as well.

7. The behaviors of End.MVPN

End.MVPN is used in MVPN usecase where a MFIB lookup in a specific VRF table T at the egress PE is required. This SID is generated by egress PE and transmitted to ingress PE via BGP/PCEP. When an IPv6 packet with IPv6 destination address being D is received on an egress PE, and D is associated with an End.MVPN SID on the egress PE, the egress PE does the following behavior:

* S01. If (V bit in End.MVPN = 1) {
* S02. Look up the End.MVPN mapping table according to End.MVPN, find out the associated RD and the related MFIB(VRF) table T.
* S03. Remove the outer IPv6 header with all its extension headers.
* S04. Set the packet's associated MFIB table to T.
* S05. Submit the packet to the egress MFIB lookup for transmission to the new multicast downstream.
* S06. } Else {
* S07.Set the packet's associated MFIB table to global MFIB.
* S08. Submit the packet to the egress MFIB lookup for transmission to the new multicast downstream.
* S09. }

8. The advertisement of End.MVPN

8.1. BGP

[I-D.ietf-bess-srv6-services]defines SRv6 Services TLV and SRv6 SID Information Sub-TLV to advertise SIDs and associated functions via BGP. [RFC6514] defines BGP-MVPN Source Tree Join Route (Type 7) specific MCAST-VPN NLRI, which consists of the following:

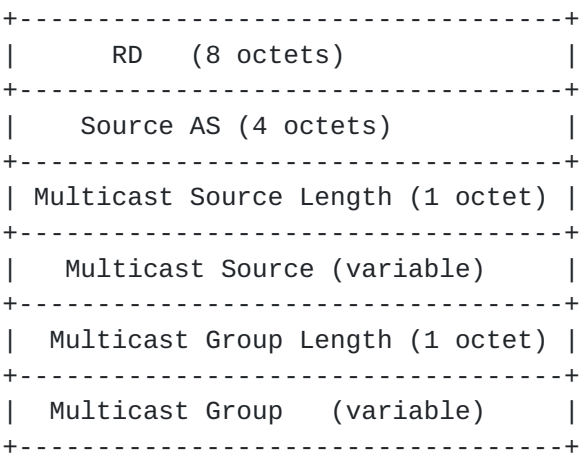

Figure 3: The format of BGP-MVPN Source Tree Join Route specific MCAST-VPN NLRI

To advertise End.MVPN SID and the related (RD, multicast group address), the egress PE can put the SID code point and SRv6 Endpoint Behavior in SRv6 SID Information Sub-TLV, and put RD, source AS number, multicast group address in the Source Tree Join Route. This advertisement will be captured by ingress PE, and provide the useful information to generate the entries of End.MVPN mapping table.

8.2. PCEP

The advertisement of End.MVPN via PCEP is described in TBD.

9. Security Considerations

TBD

10. IANA Considerations

This document defines a new segment type: End.MVPN.

End.MVPN	Destination address for decapsulation and VRF table lookup

The code point is assigned by IANA from the "SRv6 Endpoint Behaviors".

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6514] Aggarwal, R., Rosen, E., Morin, T., and Y. Rekhter, "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", RFC 6514, DOI 10.17487/RFC6514, February 2012, <https://www.rfc-editor.org/info/rfc6514>.

[RFC7371] Boucadair, M. and S. Venaas, "Updates to the IPv6 Multicast Addressing Architecture", RFC 7371, DOI 10.17487/RFC7371, September 2014, <https://www.rfc-editor.org/info/rfc7371>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

11.2. Informative References

[I-D.ietf-bess-srv6-services] Dawra, G., Talaulikar, K., Raszuk, R., Decraene, B., Zhuang, S., and J. Rabadan, "SRv6 BGP based Overlay Services", Work in Progress, Internet-Draft, draft-ietf-bess-srv6-services-15, 22 March 2022, <https://www.ietf.org/archive/id/draft-ietf-bess-srv6-services-15.txt>.

Authors' Addresses

Wei Wang
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: weiwang94@foxmail.com

Aijun Wang
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: wangaj3@chinatelecom.cn