Authors: J. Xie   X. Geng
         Huawei Technologies   Huawei Technologies
         Y. Liu
         China Mobile
         Source Segment for Multicast Source Routing over IPv6

Abstract

   This document defines the general concept of source segment which is
   used as the IPv6 source address in an IPv6 packet. Source segment
   for multicast service is introduced in this document.

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 [RFC2119]

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Segment Routing ([RFC8402]) leverages the mechanism of source
routing. An ingress node steers a packet through an ordered list of
instructions, called "segments". Each one of these instructions
represents a function to be implemented at a specific location in
the network. A function is locally defined on the node where it is
executed. Network Programming combines Segment Routing functions to
achieve a networking objective that goes beyond mere packet routing.
[RFC8986] defines the SRv6 Network Programming concept and specifies
the main Segment Routing behaviors and network programming
functions.

Previous segments defined in SRv6 can be used as the destination
address of an IPv6 packet. This document introduces the new
segments, source segments, which can be used as the IPv6 source
address of an IPv6 packet. This document defines the general concept
of source segment and the source segment used for multicast service.
Protocol extensions on the control plane are not in the scope of
this document.

This document defines the general concept of source segment and the source segment used for multicast service. Protocol extensions on the control plane are not in the scope of this document.

2. Terminologies

The following new terms are used throughout this document:

MSR6: Multicast Source Routing over IPv6;

MSR6 Domain: a set of nodes participating in the multicast source routing;

3. Source Segment Definition

Source segment is different from the existing SID defined in RFC8402 from the following aspects:

  *Source segment is unchanged along the SRv6 path

  *Source segment is distributed by the ingress node but indicates functions in other nodes along the path, e.g., egress node. Forwarding table should be maintained in the nodes where the instruction takes place.

  *When the source segment is encapsulated in an SRv6 packet, it is activated by other instructions in the data plane because source address is not parsed in existing forwarding process of a unicast packet

Using source segment for SRv6 Network Programming have several benefits including:

  *Enhance network programming capability for more SRv6 functions and extend the programming space in IPv6 header;

  *Provide sematic for source address with similar IPv6 address allocation and management method as SRv6;

  *Facilitates security management inside the limited domain;

Source segment should be avoided to process hop by hop. Per-hop process of source segment which will degrade forwarding performance and bring compatibility issues.

4. SID Format

Source segment leverages the format of SID defined in SRv6 network programming.

Source segment consists of LOC:FUNCT:ARG, where a locator (LOC) is
encoded in the L most significant bits of the SID, followed by F
bits of function (FUNCT) and A bits of arguments (ARG).

A locator may be represented as B:N where B is the SRv6 SID block
(IPv6 prefix allocated for SRv6 SIDs by the operator) and N is the
identifier of the ingress node .

The FUNCT is an opaque identification of the behavior bound to the
SID. The behavior could be executed in other nodes except ingress
node.

The behavior indicated by FUNCT may require additional information
for its processing. This information may be encoded in the ARG bits
of the SID.

5. Source Segment for MVPN

In the multicast service, packet is replicated along the tree
towards a set of leaf nodes. MVPN routing and the corresponding
information could be encapsulated in the source segment carried in
the IPv6 source address. Source Segment for MVPN is distributed by
the multicast source node and the function is executed by the
multicast leaf nodes.As described in section 3, Source Segment for
MVPN is not changed when the packet is replicated and forwarded
along the P2MP path.

This section defines the source segment for MVPN.

5.1. Behaviors

The following is a set of behaviors that can be associated with a
source segment for MVPN.

```
+------------+-----------------------------------------------------+
|  Src.DT4   |Source address for decapsulation and IPv4 table lookup|
|------------|-----------------------------------------------------+
|  Src.DT6   |Source address for decapsulation and IPv6 table lookup|
|------------|-----------------------------------------------------+
|  Src.DT46  |Source address for decapsulation and IP table lookup  |
|------------|-----------------------------------------------------+
|  Src.DT2   |Source address for decapsulation and L2 table lookup  |
|------------|-----------------------------------------------------+
```

5.2. SRC.DT4

The "Source address for decapsulation and IPv4 table lookup"
behavior ("Src.DT4" for short) is used in MVPNv4 use case where an
MFIB lookup in a specific VRF table T at the egress node is
required. The Src.DT4 SID is an SID associated with an IPv4 MFIB

table T on the egress PE, either through a control-plane message
advertised by the ingress PE, or through a local configuration on
the egress PE. When an IPv6 encapsulated packet with IPv6 source
address being S is received on an egress PE, and S is associated
with an Src.DT4 SID on the egress PE, the egress PE does the
following behavior:

```
S01. If (Upper-Layer header type == 4(IPv4) ) {
S02.    Remove the outer IPv6 header with all its extension headers
S03.    Set the packet's associated MFIB table to T
S04.    Submit the packet to the egress IPv4 MFIB lookup for
            transmission to the new multicast downstreams
S05. } Else {
S06.    Drop the packet;
S07. }
```

5.3. SRC.DT6

SRC.DT6 behavior could be used in MVPNv6 use case where a MFIB
lookup in a specific VRF table at the egress node is required.

```
S01. If (Upper-Layer header type == 41(IPv6) ) {
S02.    Remove the outer IPv6 header with all its extension headers
S03.    Set the packet's associated IPv6 MFIB table to T
S04.    Submit the packet to the egress IPv6 MFIB lookup for
            transmission to the new multicast downstreams
S05. } Else {
S06.    Drop the packet;
S07. }
```

5.4. SRC.DT46

SRC.DT46 behavior could be used in MVPN use case where a MFIB lookup
in a specific VRF table at the egress node is required.

```
S01. If (Upper-Layer header type == 4(IPv4) ) {
S02.    Remove the outer IPv6 header with all its extension headers
S03.    Set the packet's associated MFIB table to T
S04.    Submit the packet to the egress IPv4 MFIB lookup for
            transmission to the new destination
S05. } Else if (Upper-Layer header type == 41(IPv6) ) {
S06.    Remove the outer IPv6 header with all its extension headers
S07.    Set the packet's associated MFIB table to T
S08.    Submit the packet to the egress IPv6 MFIB lookup for
            transmission to the new destination
S09. } Else {
S10.    Drop the packet;
S11. }
```

5.5. Src.DT2

SRC.DT2 behavior could be used in MVPN use case where a L2 table
lookup in a specific Layer-2 Multicast forwarding table at the
egress node is required.

```
S01. If (Upper-Layer header type == 143(Ethernet) ) {
S02.    Remove the outer IPv6 header with all its extension headers
S03.    Set the packet's associated Layer-2 Multicast forwarding tabl
S04.    Submit the packet to the egress Layer-2 Multicast forwarding
            lookup for transmission to the new multicast downstreams
S05. } Else {
S06.    Send an ICMP Parameter Problem to the Source Address
            with Code 4 (SR Upper-layer Header Error)
            and Pointer set to the offset of the Upper-Layer header,
            interrupt packet processing, and discard the packet
S07. }
```

6. Exception Handling

Once a source segment is used in an MSR6 data packet as source
address, it is expected to receive an ICMPv6 error message with the
source segment being the Destination address, and such a packet is
expected to be processed by Ingress PE.

Additionally, there are cases where a source segment may appear as
destination address of an packet that is not an ICMPv6 message. This
could be a packet without SRH, or a packet with SRH and the active
segment is the source segment. Such a packet is expected to be
dropped.

The following pseudo-code describes how a packet with a source
segment as destination address is handled:

```
 1. IF Upper Layer Protocol = ICMPv6   ;;Ref1: ICMPv6 packet
 2.    Send to CPU in limited rate.
 3. ELSE
 4.    Drop the packet.
```

7. Use Case

The source segment could be applied in the following case:

  1. MSR6: The MSR6 MVPN uses the source segment in the IPv6 source
     address for identifying a VRF in IPv6 multicast source routing.

  2. Tree SID over SRv6: MVPN service can use Tree SID over SRv6 [I-
     D.ietf-bess-mvpn-evpn-sr-p2mp] for point-to-multipoint
     transport of a packet. When a Tree SID over SRv6 P-tunnel is

shared across different MVPNs, an IPv6 address in IPv6 source
address for identifying a VRF is possible.

3. MVPN service can use Ingress Replication(IR) [RFC6513] to
   simulate a point-to-multipoint P-tunnel. In an IPv6
   environment, Ingress Replication can use IPv6 encapsulation for
   each branch. When the egress PE of an Ingress Replication P-
   tunnel branch receives a packet, it gets to know the VRF of the
   packet through the Destination address in the IPv6 header. This
   means that, every egress PE of the IR P-tunnel branch need to
   allocate an IPv6 address to identify a VRF. If the source
   segment is used for the IPv6 source address, only one IPv6
   address of the Ingress PE is needed for identifying a VRF, and
   thus save the IPv6 addresses and their operation costs.

8. IANA Considerations

TBD

9. Security Considerations

TBD

10. References

10.1. Normative References

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet
           Control Message Protocol (ICMPv6) for the Internet
           Protocol Version 6 (IPv6) Specification", STD 89, RFC
           4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-
           editor.org/info/rfc4443>.

[RFC6513] Rosen, E., Ed. and R. Aggarwal, Ed., "Multicast in MPLS/
           BGP IP VPNs", RFC 6513, DOI 10.17487/RFC6513, February
           2012, <https://www.rfc-editor.org/info/rfc6513>.

[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>.

10.2. Informative References

[I-D.ietf-bess-mvpn-evpn-sr-p2mp]
          Parekh, R., Filsfils, C., Venkateswaran, A., Bidgoli, H.,
          Voyer, D., and Z. Zhang, "Multicast and Ethernet VPN with
          Segment Routing P2MP and Ingress Replication", Work in
          Progress, Internet-Draft, draft-ietf-bess-mvpn-evpn-sr-
          p2mp-06, 2 July 2022, <https://www.ietf.org/archive/id/
          draft-ietf-bess-mvpn-evpn-sr-p2mp-06.txt>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
          2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
          May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Jingrong Xie
Huawei Technologies

Email: xiejingrong@huawei.com

Xuesong Geng
Huawei Technologies

Email: gengxuesong@huawei.com

Yisong Liu
China Mobile

Email: liuyisong@chinamobile.com