SRv6 Midpoint Protection
draft-chen-rtgwg-srv6-midpoint-protection-08

Abstract

The current local repair mechanism, e.g., TI-LFA, allows local repair actions on the direct neighbors of the failed node or link to temporarily route traffic to the destination. This mechanism could not work properly when the failure happens in the destination point. In SRv6 TE, the IPv6 destination address in the outer IPv6 header could be the segment endpoint of the TE path rather than the destination of the TE path. When the SRv6 endpoint fails, local repair couldn't work on the direct neighbor of the failed endpoint either. This document defines midpoint protection for SRv6 TE path, which enables other nodes on the network to perform endpoint behaviors instead of the faulty node, Update the IPv6 destination address to the other endpoint, and choose the next hop based on the new destination address.

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 12 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.  Introduction ................................. 3
2.  SRv6 Midpoint Protection Mechanism ............ 3
3.  SRv6 Midpoint Protection Example ............... 3
4.  SRv6 Midpoint Protection Behavior .............. 5
   4.1. Endpoint Node as Repair Node ............... 5
   4.2. Endpoint x Node as Repair Node ............. 6
5.  Determining whether the Endpoint could Be Bypassed ........ 6
6.  Security Considerations ........................ 6
7.  IANA Considerations ........................... 7
8.  Acknowledgements ................................ 7
9.  References ................................... 7
   9.1. Normative References ....................... 7
   9.2. Informative References ..................... 8
Authors' Addresses ................................. 8
1. Introduction

The current mechanism, e.g., TI-LFA ([I-D.ietf-rtgwg-segment-routing-ti-lfa]), allows local repair actions on the direct neighbors of the failed node or link to temporarily route traffic to the destination. This mechanism could not work properly when the failure happens in the destination point. In SRv6 TE, the IPv6 destination address in the outer IPv6 header could be the segment endpoint of the TE path rather than the destination of the TE path ([RFC8986]). When the endpoint fails, local repair couldn't work on the direct neighbor of the failed endpoint either. This document defines midpoint protection for SRv6 TE path, which enables other nodes on the network to perform endpoint behaviors instead of the faulty node, Update the IPv6 destination address to the other endpoint, and choose the next hop based on the new destination address.

2. SRv6 Midpoint Protection Mechanism

When an endpoint node fails, the packet needs to bypass the failed endpoint node and be forwarded to the next endpoint node of the failed endpoint. Only endpoint node can process SRH. Therefore, only endpoint nodes can perform midpoint protection. There are two stages or time periods after an endpoint node fails. The first is the time period from the failure until the IGP converges on the failure. The second is the time period after the IGP converges on the failure.

During the first time period, the packet will be sent to the direct neighbor of the failed endpoint node. After detecting the failure of its interface to the failed endpoint node, the neighbor forwards the packets around the failed endpoint node. It changes the IPv6 destination address with the IPv6 address of the next endpoint node (or the last or other reasonable endpoint node) which could avoid going through the failed endpoint.

During the second time period. There is no route to the failed
endpoint node after the IGP converges. When a previous hop node of the failed endpoint node finds out that there is no route to the IPv6 destination address (of the failed endpoint node), it changes the IPv6 destination address with the IPv6 address of the next endpoint node. Note that the previous hop node may not be the direct neighbor of the failed endpoint node.

3. SRv6 Midpoint Protection Example

The topology in Figure 1 illustrates an example of network topology with SRv6 enabled on each node.

In this document, an end SID at node n with locator block B is represented as B:n. An end.x SID at node n towards node k with locator block B is represented as B:n:k. A SID list is represented as <S1, S2, S3> where S1 is the first SID to visit, S2 is the second SID to visit and S3 is the last SID to visit along the SRv6 TE path.

In the reference topology, suppose that Node N1 is an ingress node of SRv6 TE path going through N3 and N4. Node N1 steers a packet into a segment list < B:2, B:3, B:4 >.

When node N3 fails, the packet needs to bypass the failed endpoint node and be forwarded to the next endpoint node after the failed endpoint in the TE path. When outbound interface failure happens in the Repair Node (which is not limited to the previous hop node of the failed endpoint node), it performs the proxy forwarding as follows:

During the first time period (i.e., before the IGP converges), node
N2 (direct neighbor of N3) as a Repair Node forwards the packets around the failed endpoint N3 after detecting the failure of the outbound interface to the endpoint B:3. It changes the IPv6 destination address with the next sid B:4. N2 detects the failure of outbound interface to B:4 in the current route, it could use the normal Ti-LFA repair path to forward the packet, because it is not directly connected to the node N4. N2 encapsulates the packet with the segment list < B:5:6> as a repair path.

During the second time period (i.e., after the IGP converges), node N2 does not have any route to the failed endpoint N3 in its FIB. Node N2, as a Repair Node, forwards the packets around the failed endpoint N3 to the next endpoint node (e.g., N4) directly. There is no need to check whether the failed endpoint node is directly connected to N2. N2 changes the IPv6 destination address with the next sid B:4. Since IGP has completed convergence, it forwards packets directly based on the IGP SPF path.

4. SRv6 Midpoint Protection Behavior

A node N protecting the failure of an endpoint node on a SRv6 path may be one of the following types:

* a transit node: The transit node cannot process SRH. Therefore, Only Ti-LFA can be executed on the transit node, but not midpoint protection.

* an endpoint node: the destination address (DA) of the packet received by N is a N's local END SID.

* an endpoint x node (i.e., an endpoint with cross-connect node): the destination address (DA) of the packet received by N is a N's local End.X SID with an array of layer 3 adjacencies.

This section describes the behavior of each of these nodes as a repair node for the two time periods after the endpoint node fails.

4.1. Endpoint Node as Repair Node

When the Repair Node is an endpoint node, it provides fast
protections for the failure through executing the following procedure after looking up the FIB for the updated DA.

IF the primary outbound interface used to forward the packet failed
   IF NH = SRH && SL != 0 and
       the failed endpoint is directly connected to Repair Node THEN
       SL decreases; update the IPv6 DA with SRH[SL];
       FIB lookup on the updated DA;
       forward the packet according to the matched entry;
   ELSE
       forward the packet according to the backup nexthop;
   ELSE IF there is no FIB entry for forwarding the packet THEN
       IF NH = SRH && SL != 0 THEN
           SL decreases; update the IPv6 DA with SRH[SL];
           FIB lookup on the updated DA;
           forward the packet according to the matched entry;
       ELSE
           drop the packet;
   ELSE
       forward accordingly to the matched entry;

4.2. Endpoint x Node as Repair Node

When the Repair Node is an endpoint x node, it provides fast protections for the failure through executing the following procedure after updating DA.

IF the layer-3 adjacency interface is down THEN
   FIB lookup on the updated DA;
IF the primary interface used to forward the packet failed THEN
   IF NH = SRH && SL != 0 and
       the failed endpoint directly connected to Repair Node THEN
       SL decreases; update the IPv6 DA with SRH[SL];
       FIB lookup on the updated DA;
       forward the packet according to the matched entry;
   ELSE
forward the packet according to the backup nexthop;
ELSE IF there is no FIB entry for forwarding the packet THEN
  IF NH = SRH && SL != 0 THEN
    SL decreases; update the IPv6 DA with SRH[SL];
    FIB lookup on the updated DA;
    forward the packet according to the matched entry;
  ELSE
    drop the packet;
ELSE
  forward accordingly to the matched entry;

5. Determining whether the Endpoint could Be Bypassed

SRv6 Midpoint Protection provides a mechanism to bypass a failed endpoint. But in some scenarios, some important functions may be implemented in the bypassed failed endpoints that should not be bypassed, such as firewall functionality or In-situ Flow Information Telemetry of a specified path. Therefore, a mechanism is needed to indicate whether an endpoint can be bypassed or not. [I-D.li-rtgwg-enhanced-ti-lfa] provides method to determine whether enable SRv6 midpoint protection or not by defining a "no bypass" flag for the SIDs in IGP.

6. Security Considerations

This section reviews security considerations related to SRv6 Midpoint protection processing discussed in this document. To ensure that the Repair node does not modify the SRH header Encapsulated by nodes outside the SRv6 Domain. Only the segment within the SRH is same domain as the repair node. So it is necessary to check the skipped segment have same block as repair node.
9. References

9.1. Normative References

[I-D.ietf-lsr-isis-srv6-extensions]

[I-D.ietf-lsr-ospfv3-srv6-extensions]


9.2. Informative References
[I-D.hu-spring-segment-routing-proxy-forwarding]

[I-D.ietf-rtgwg-segment-routing-ti-lfa]

[I-D.ietf-spring-segment-routing-policy]

[I-D.li-rtgwg-enhanced-ti-lfa]

[I-D.sivabalan-pce-binding-label-sid]


Authors' Addresses

Chen, et al. Expires 12 January 2023