SRv6 Midpoint Protection

draft-chen-rtgwg-srv6-midpoint-protection-05

Huanan Chen (China Telecom)
Zhibo Hu (Huawei Technologies)
Huaimo Chen (Futurewei)
Xuesong Geng (Huawei Technologies)
Yisong Liu (China Mobile)

Motivations and Goals

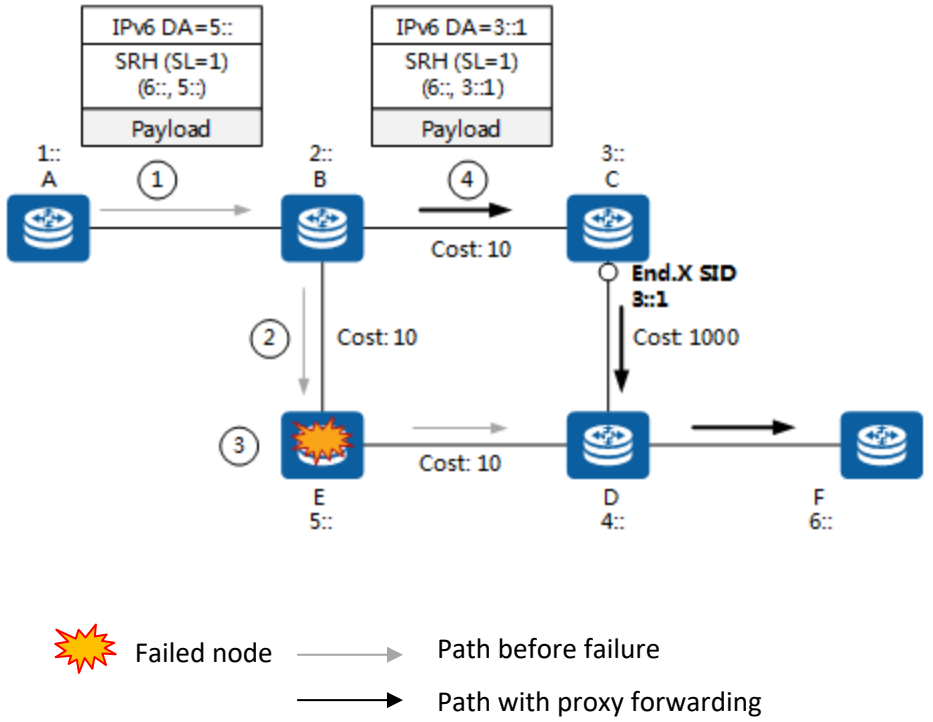
Motivations

- **Scenario**: When an SRv6 Endpoint failed, the existing FRR mechanism cannot be used to restore the reachability;
- **Requirement:** SRv6 E2E protection could work, but a simpler and faster local repair mechanism is also requested;
- **Existing work:** The mechanism defined in [draft-ietf-spring-segment-protection-sr-te-paths] is able to provide endpoint protection for SR MPLS network;

Goals: This document introduces a SRv6 midpoint protection mechanism: when an SRv6 endpoint fails, an SRv6 proxy forwarding node can replace the failed endpoint to perform SRv6 end function.

SRv6 Midpoint Protection Mechanism

- If a loose SR TE path fails, The convergence could be divided into 2 periods:
  - 1st Period : Before IGP convergence, the faulty adjacent node is a PLR node, perform proxy forwarding and send packet to the next end point in the segment list.
  - 2nd Period: After IGP convergence, any upstream node, that has been converged and deleted the FIB to E, will be the PLR node and perform the proxy forwarding action.
- After SRv6 Policy convergence, The node forwards the packet along the converged path



SRv6 Midpoint Protection Behavior

When the Repair Node is a transit node or an endpoint node, the protection behavior is defined as:

```
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;
```

When the Repair Node is an endpoint x node, the protection behavior is defined as:

```
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;
```

Draft History

- v00/v01: mechanism description
- V02: Update section 6 of corresponding the discussion of security
  - SRv6 midpoint protection can be executed only in the SRH header encapsulated in the SRv6 domain to which the PLR belongs.
- V03: Update section 5 according to the discussion in spring mailing list thread of “Spring protection - determining applicability”
  - In some use cases, the endpoint cannot be bypassed, for example, the firewall. To solve this problem, this draft refers to “draft-li-rtgwg-enhanced-ti-lfa-03”
- V04/V05: Modify the test and add a new co-author;

Plan

The document is stable and has been fully discussed, so the authors plan to:

- Collect feedback in SPRING
  - How to deal with the case that when the segment of the next endpoint is also failed
    - There will be another repair node does the proxy forwarding to skip the second failed node. This process can be iterated until a reachable endpoint is selected or the segment is the last one in the segment list;
  - Why a local repair solution is requested when the E2E protection could also solve the problem
    - Local repair solution could be provide faster protection than the E2E solution, which is requested in some scenario.
  - When the repair node is a transit node, it may be against RFC 8200 which won't allow transit node to modify SRH
    - Section 6 "Security Considerations" is added and proposes to check that the skipped segment belongs to the same block as the repair node first to guarantee that they are in the same trusted domain, before doing the proxy forwarding defined in the document. (as mentioned in the history overview)
- Ask WG Adoption in RTGWG

Thanks