SRv6 Midpoint Protection

draft-chen-rtgwg-srv6-midpoint-protection-02

Huanan Chen
China Telecom
Zhibo Hu
Huaimo Chen
Xuesong Geng
Huawei Technologies

Motivation

- When SRv6 Policy endpoint node fails, current local repair mechanism can't provide protection:
  - The current repair path also traverses the endpoint.
  - After IGP convergence, the repair path will be deleted along with the route.

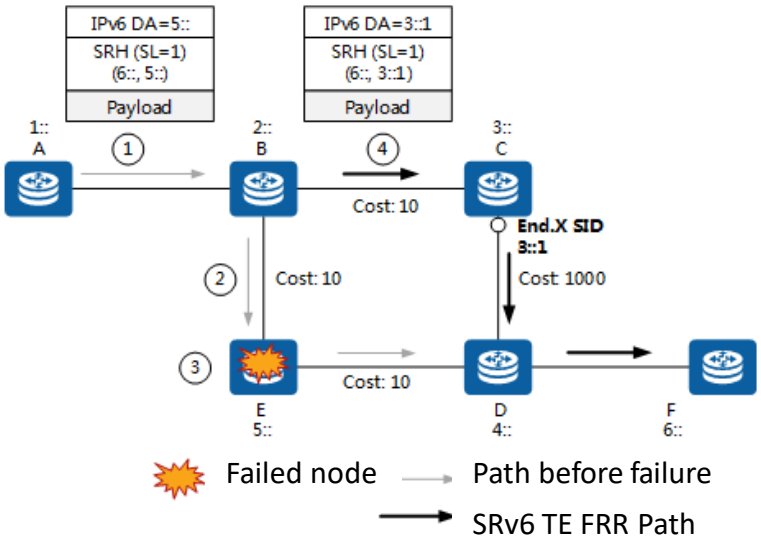
- Therefore, Proxy forwarding mechanism is provided. When an endpoint node fails, other nodes can perform proxy forwarding, bypass the failed node, and continue the forwarding.

- This is a useful supplement to Ti-LFA and provides a local repair mechanism for SRv6 policies.

- This document defines the behavior of the SRv6 midpoint protection, including extensions for transit/end/end.x repair node.

SRv6 Midpoint Protection Mechanism

- When an endpoint node E fails, the packet needs to bypass node E and be forwarded to the next endpoint node of the failed endpoint.
  - Step1: Before IGP convergence, Node B still keeps the fib to Node E, but the out interface is down. The proxy forwarding behavior is executed on Node B. SL--, copy the next sid to the destination address of the IPv6 header. And forwards the packet based on the updated destination address.
  - Step2: After IGP convergence, all the node deletes the fib of Node E. Node A will be fibmiss and triggering proxy forwarding.
  - Step3: After SRv6 Policy convergence, The node forwards the packet along the converged path.



SRv6 Midpoint Protection Behaviors

Take an example when the repair node is transit node:

- IF the primary out interface used to forward the packet failed

  IF NH = SRH && SL != 0, and the failed endpoint is directly connected to the Repair Node

  SL--; 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

  IF NH = SRH && SL != 0

  SL --;

  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 according to the matched entry;

Security Considerations

- The midpoint protection cannot be enabled by default.

- The repair node can modify the SRH only when the failed endpoint is in the same trusted domain node. In the other word, midpoint protection is only enabled when the repair node is trusted by the failed node.

Next Step

- Contributions and comments are welcome
- WG Adoption?

Thanks