# SRv6 Midpoint Protection

## draft-chen-rtgwg-srv6-midpoint-protection-03

Huanan Chen

**China Telecom**

Zhibo Hu

Huaimo Chen

Xuesong Geng

**Huawei Technologies**

# Outline

- Motivations and Goals
- SRv6 midpoint protection mechanism
- Security Considerations
- Q&A
- Next Steps

# Motivations and Goals

## Motivations

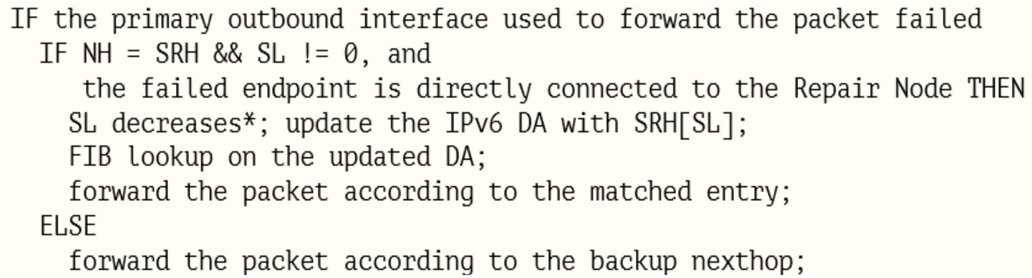
- Scenario: When an SRv6 Policy Endpoint is failed, the existing FRR mechanism cannot be used to restore the reachability;
- Requirement: SRv6 E2E protection could work, but a simpler and faster local repair mechanism is also requested;
- Existing work: The mechanism defined in [draft-ietf-spring-segment-protection-sr-te-paths-00] is able to provide endpoint protection for SR MPLS endpoint protection;

**Goals:** This document introduces a SRv6 proxy forwarding 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

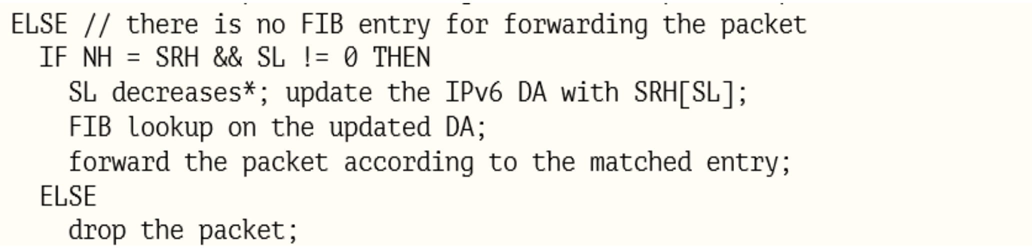
**Mechanism:**

- If the Repair Node is adjacent to the failed Endpoint: the node executes the following proxy forwarding behavior to perform the end function and replace the failed node:



```
IF the primary outbound interface used to forward the packet failed
  IF NH = SRH && SL != 0, and
     the failed endpoint is directly connected to the 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;
```

- If the Repair Node is remote to the failed Endpoint : FIB miss happens in the remote node after IGP convergence, and the node executes the following proxy forwarding behavior to perform the end function and replace the failed node:



```
ELSE // there is no FIB entry for forwarding the packet
  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;
```

# Security Considerations

## Security Considerations

- Scenario #1: The PLR node and the failed node must belong to the same trusted domain.
  - Trusted domain is identified by same SRv6 SID block as defined in RFC 8986
- Scenario #2: A mechanism is requested to ensure that security-related segments (or other important functions) cannot be bypassed. Refer to [draft-li-rtgwg-enhanced-ti-lfa-03]

# Q&A

**Question 1:** How to differentiate the condition the route is node down vs. link down?

- link failure and node failure are both treated as node failure, just as FRR mechanism;

**Question 2:** What about the function supposed to be executed at node E?

- The proxy behavior is for path repair which guarantees the reachability and other functions can't be agented. So only end function is executed;

**Question 3:** Could TE path be changed when doing protection?

- Middle point protection is for temporary reachability repair when failure happens in the TE path; If SLA of the TE path is supposed to be guaranteed during the protection process, E2E protection could be considered;

# Next Steps

- Comments and questions are welcome
- Ready for WG adoption

# Thanks!