SRv6 Path Midpoint Protection

draft-chen-rtgwg-srv6-midpoint-protection

Huanan Chen, China Telecom
Zhibo Hu, Huawei
Huaimo Chen, Futurewei
Xuesong Geng, Huawei
Yisong Liu, China Mobile
Gyan S. Mishra, Verizon

IETF 116
Overview

Thanks all giving comments/suggestions

We summarized them to the list

- SRv6 Path Midpoint Protection Mechanism: Before IGP Converges (Existing)
- SRv6 Path Midpoint Protection Mechanism: After IGP Converges (New)
SRv6 Path Midpoint Protection Mechanism: Before IGP Converges

- No failure: Packet (Pkt) is sent to C through 1,2,3,4,5,6
- N failed before IGP converges: Packet (Pkt) is sent to C through 1,2,3,4,5,6

SRv6 Path: A->P1->N->Q1->C, represented at A by <B:P1, B:N, B:Q1, B:C>, where B:P1 is end SID of P1, B:N is end SID of N, B:Q1 is end SID of Q1, ...

- P3 as PLR detects failure, reroutes pkt to next end SID B:Q1 without going failed N (i.e., TI-LFA)
SRv6 Path Midpoint Protection Mechanism: After IGP Converges

Endpoint node X: DA of the packet received by node X is a X’s local END SID
E.g., P1, N, Q1, C are endpoint nodes for the SRv6 path

SRv6 Path: A->P1->N->Q1-> C, represented at A by <B:P1, B:N, B:Q1, B:C>,
where B:P1 is end SID of P1, B:N is end SID of N, B:Q1 is end SID of Q1, ...

P1 drops packet since no route to B:N after IGP converges on failed N

IF no FIB entry for DA of packet THEN
   IF NH = SRH && SL != 0 THEN
      SL--; DA = SRH[SL];
      forward packet using FIB entry for DA;
Next Steps

Comments
Summary of Comments

Q1: How does SRv6 Midpoint protection differentiate: link down vs node down, route not present vs IPv6 prefix not advertised?
A1: SRv6 Midpoint Protection does not distinguish between Link Down and Node Down. Assume that the Node is Down to maximize the protection scope.

Q2: In SRv6, some functions may be executed at failed node. SRv6 midpoint protection may miss the execution of some necessary functions like Security.
A2: A mechanism is needed to indicate whether an endpoint can be bypassed or not. [I-D.li-rtgw-enhanced-ti-lfa] provides method to determine whether SRv6 midpoint protection is enabled by defining a “no bypass” flag, which has been updated in the document.

Q3: Here we are handling failure 2 times (One layer-3 adjacency interface and another primary interface), in all other cases we only handle one failure. Better to restrict to handling of one failure.
A3: layer-3 adjacency interface and primary interface may be the same interface. Therefore, It must be processed

Q4: When the repair node is a transit node, it may be against RFC 8200 which does not allow transit node to modify SRH.
A4: Only endpoint node can process SRH, Therefore, only endpoint nodes can perform midpoint protection. This complies with RFC 8200, which has been updated in the document.

Q5: Only endpoint node performs midpoint protection depending on IGP convergence in some case.
A5: Only loose paths depend on IGP convergence. To comply with RFC 8200, we can only prohibit the execution SRv6 Midpoint protection on the transit node.