Fast Reroute for Node Protection in LDP-based LSPs

draft-esale-mpls-ldp-node-frr-02

Raveendra Torvi (rtorvi@juniper.net)
Luay Jalil (luay.jalil@verizon.com)
Luyuan Fang (lufang@microsoft.com)
Santosh Esale (sesale@juniper.net)

IETF-94, November 4
Yokohama

Requirements

- Fast Re-route for LDP-signaled transport LSPs
- Local protection to minimize connectivity disruption
- Protection for both link and node failure
- No restrictions on the network topology – provide topology independent local protection
- Minimize additional provisioning/configuration required

Node Protection Building Blocks

- For a given (multi-point to point) LSP traversing a given protected node:
  - PLR: router one hop upstream from the protected node
    - With respect to the LSP
    - Previous hop with respect to the protected node
  - MP: Any router on the LSP, provided that the path from that router to the egress of the LSP is not affected by failure of the protected node
    - More on this in the next slides…
  - Bypass LSP: LSP created from PLR to MP
    - Bypasses the protected node
    - The same bypass LSP is used to protect all LSPs traversing PLR, protected node, and MP
  - Label mapping: obtained from MPT using Targeted LDP between PLR and MP
    - The label from MP may not be the same as the label from the next hop
    - Only labels for Address Prefix FECs with Prefix Lenght 32 (IPv4) or 128 (IPv6) should be exchanged
    - To acquire label mapping only for the FEC of this LSP PLR may use LDP Downstream on Demand
    - Same applies to every LSPs traversing PLR, protected node, and MPT

Node Protection – Determining MPT (1)

(protected node is **not** ABR)

Consider an LSP that traverses PLR, protected node, and particular neighbor of the protected node - we'll refer to this neighbor as the "*next next-hop*“

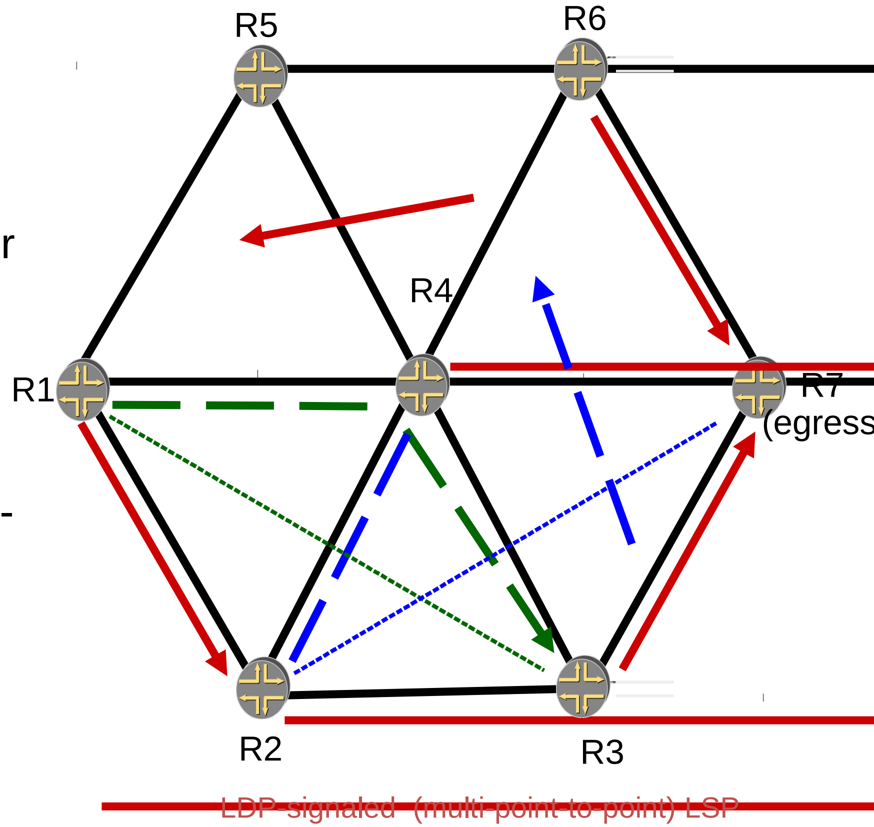
- From PLR’s perspective the protected node is the next hop for the FEC associated with that LSP
- From protected node’s perspective the next next-hop is the next hop for that FEC

When the protected node is not an Area Border Router (ABR), PLR can determine the next next-hop as a by-product of SPF required by ISIS/OSPF

- No additional SPF may be needed

When the protected node is not an ABR, PLR uses the next next-hop as MPT

- As path from the next next-hop to the egress is not affected by failure of the protected node



Protected node	PLR	MPT (next next-hop)	Bypass LSP
R2	R1	R3	<R1, R4, R3>
R3	R2	R7	<R2, R4,

Node Protection – Determining MPT (2)

(protected node is ABR)

Consider an LSP that traverses PLR, protected node, and particular neighbor of the protected node - we'll refer to this neighbor as the "*next next-hop*"

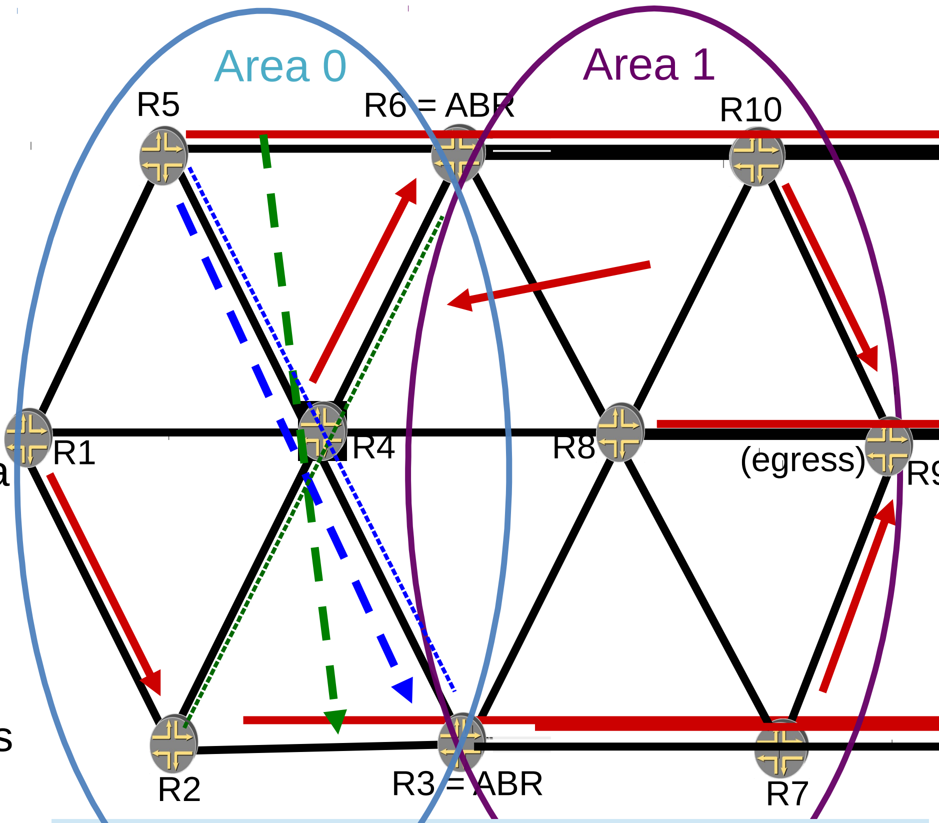
When the protected node is an ABR, PLR may not be able to determine the next next-hop from its SPF

- As PLR and the next next-hop may end up in different IGP areas
- Yet in ISIS/OSPF scope of SPF is the IGP area of PLR

In this scenario PLR uses an "***alternative***" ABR as MPT

- For a given LSP that traverses PLR and protected ABR, an alternative ABR is defined as any ABR that advertises into PLR's own IGP area reachability to the FEC associated with the LSP

PLR discovers an alternative ABR from the IGP database



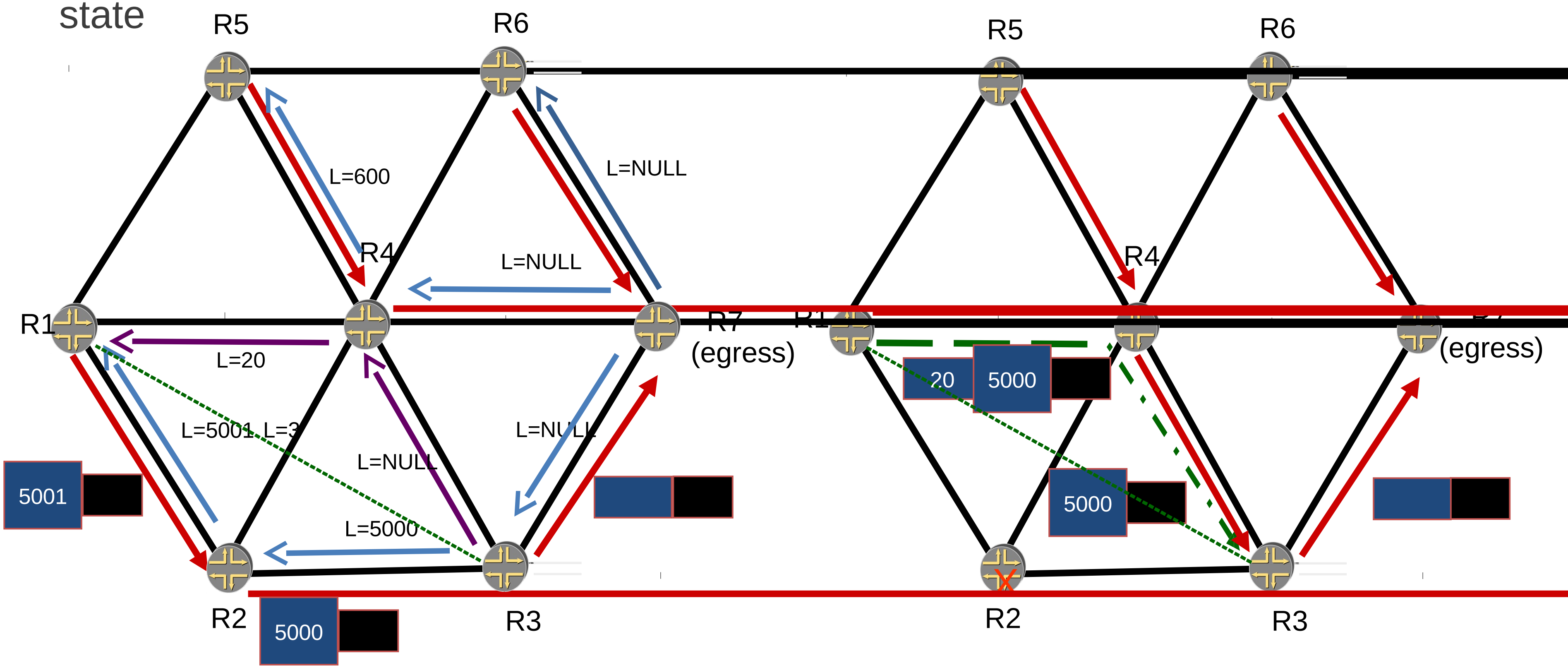
Protected node	PLR	MPT (Alternative ABR)	Bypass LSP
R7	R3	R10	<R3, R8, R10>
R10	R6	R7	<R6, R8

Node Protection - Example

(protected node is **not** ABR)

Label handling and data flow during steady state

Data flow after node failure



LDP-signaled (multi-point-to-point) LSP

LDP-signaling for signaled (multi-point-to-point) LSP

Label Distribution for RSVP-TE bypass 1

tLDP session

New in version 01 and 02

- More clarifications on the next next-hop calculations
- Added algorithm to select alternative BR among the set of BRs
- Added the requirement for platform-wide label space
- Added text to describe how to discover all possible MPs of a PLR
- Terminology changed
  - Area - routing subdomain
  - ABR – Border Router
  - Alternative ABR – Alternative BR
  - MPT – MP

In conclusion

- Local link/node protection for LDP based transport LSPs using RSVP-TE bypasses
- No restrictions on the network topology – provides **topology independent local protection**
- Additional provisioning/configuration required could be fairly small
  - Depends on implementation
  - bypass LSPs from PLR to MPT and Targeted LDP between PLR and MPT can be established automatically
- Relies on the existing IETF standards
  - RSVP-TE for establishing bypass LSPs
  - Targeted LDP to obtain label mapping from MPT
    - Needed only for node protection
- Synergy with link/node protection for mLDP-signaled LSPs

Next Steps

- Summary
  - Version 01 and 02 addresses all the comments that we have received so far
  - Link protection with manual RSVP-TE bypass LSPs is already deployed in many networks
  - TI FRR makes the link protection automatic with RSVP-TE auto bypasses
  - TI FRR adds node protection with automatic RSVP-TE auto bypasses
- Implementation
  - Link protection – many
  - Node protection – one so far
- The authors would also like to request a working group adoption