MPLS Egress Protection Framework

draft-ietf-mpls-egress-protection-framework-01

Yimin Shen  (yshen@juniper.net)
Minto Jeyananth (minto@juniper.net)
Bruno Decraene  (bruno.decraene@orange.com)
Hannes Gredler  (hannes@rtbrick.com)
Carsten Michel  (c.michel@telekom.de)
Huaimo Chen  (huaimo.chen@huawei.com)
Yuanlong Jiang  (jiangyuanlong@huawei.com)

IETF 102, 2018.07
Update

Introduced a new "stub link" mode for IGP context ID advertisement.
Framework

- Fast reroute (local detection + local repair) for egress node and link
- Multi-service and multi-transport
- Common architecture to unify solutions and minimize complexity
- Future compatibility
Applicability

• Services: L2/L3 VPNs, hierarchical LSPs, etc.
• Tunnels: RSVP, LDP, BGP, IGP, segment routing, etc.
• Homogeneous and heterogeneous transport tunnels and bypass tunnels.
• L3VPN egress protection is given as an example.
• PW egress protection is published as RFC 8104.
Architecture and Components

• Protection at service level and transport tunnel level

• Two roles of router:
  • PLR - detects a failure, and fast reroutes at transport tunnel level.
  • Protector - reroutes at service level, by forwarding to service destination based on a service label in the context of the protected egress router’s label space (aka. context-based forwarding).

• Context-based forwarding

• Context ID of {egress router, protector}
  • Enables context-based forwarding on protector.
  • Facilitates bypass tunnel setup.

• Co-located protector and centralized protector
Relationship with Global Repair

- Egress protection can be used in conjunction with global repair to complement end-to-end failure protection.
  - Egress protection – local, fast but temporary repair
  - Global repair - permanent repair
Next Step

• We’d like to ask for consideration for WG last call.