MPLS Egress Protection Framework
draft-shen-mpls-egress-protection-framework-04

Yimin Shen (yshen@juniper.net)
Minto Jeyananth (minto@juniper.net)
Bruno Decraene (bruno.dehraene@orange.com)
Hannes Gredler (hannes@rtbrick.com)
Carsten Michel (c.michel@telekom.de)

IETF 98, 2017.03
Egress Protection

• Egress failures - egress node and egress link (aka. PE-CE link, AC).
• Egress protection – FRR for protecting MPLS tunnels and services against egress failures.
  • Equivalent to FRR for transit link/node failures, e.g. RSVP, LDP, LFA.
  • Driven by local failure detection and local repair.
  • Complements global repair and topology convergence.
Protection at Service and Transport Levels

• Egress link failure is a service-level failure.
  • Service packets are unable to reach the service destination.

• Egress node failure is a two-level failure.
  • Transport tunnel - MPLS packets are unable to reach the egress router.
  • Each service carried by the tunnel - Service packets are unable to reach the service instance.

• Egress protection must be provided at both levels.
  • Transport level – PLR redirects packets to a “protector”.
  • Service level – Protector hosts “protection service instances” to forward service packets towards service destinations.
Goals

• Provide a generic and unified solution for egress protection.
  • Multi-transport and multi-service
  • Minimized complexity
• Provide a framework and guidelines towards services.
  • Service protocol extensions, if needed, should be addressed by separate drafts on a per-service-type basis.
    ✓ PWE3 – RFC 8401
    ✓ Layer-3 VPNs – section 8 of the draft
Goals (cont.)

• Must support P2P tunnels, as well as P2MP and MP2P tunnels by treating sub-LSPs as P2P.
• PLR must be agnostic with services and service labels, and maintain protection state on a per-tunnel basis, rather than per-service-label basis.
• PLR must be able to use local routing/TE info to resolve bypass tunnel.
• Protector must be able to perform context-based IP forwarding or label switching for rerouted service packets.
• Must work seamlessly with transit link/node protection mechanisms.
Building Blocks

• Router at PLR (point of local repair)
  • Penultimate hop router in egress node protection.
  • Egress router in egress link protection.
  • Pre-establishes a bypass tunnel to protector.

• Protector
  • Points bypass tunnel to special label table and IP forwarding table, corresponding to the label space and IP address space of protected egress router, respectively.

• Bypass tunnel
  • PLR reroutes packets to protector via a bypass tunnel, with service label intact.
  • UHP tunnel

• Context ID and context-based forwarding
  • Protector forwards service packets to ultimate service destinations, by using a label table and IP forwarding table indicated by a context ID.
Update 1 - New Co-authors

• Hannes Gredler (hannes@rtbrick.com)
• Carsten Michel (c.michel@telekom.de)
Update 2 – Allow Tunnel Protocol Extensions

• The draft should work with existing tunnel protocols.
• Tunnel protocol extensions are not precluded, if they can facilitate egress protection establishment.
  • Example: draft-ietf-teas-rsvp-egress-protection
Update 3 – Egress Link Protection

CE1 -> PEO -> P1 -> PE1/PLR -> PE2/protector -> CE2

- Transport tunnel
- Bypass tunnel
- Service packets
Update 4 – Centralized Protector Model
Next Steps

• Welcome comments.
• As the draft is mature, we’d like to request for WG adoption.