Application-aware Targeted LDP

draft-ietf-mpls-app-aware-tldp-01

Raveendra Torvi (rtorvi@juniper.net)
Luay Jalil (luay.jalil@verizon.com)
Kamran Raza (skraza@cisco.com)
Zhenbin Li (lizhenbin@huawei.com)
Uma Chunduri (uma.chunduri@ericsson.com)
Chris Bowers (cbowers@juniper.net)
Santosh Esale (sesale@juniper.net)

IETF-94 (Yokohama)

Speaker: Santosh Esale

Central Idea

- Initiating and responding LSR are made aware of targeted LDP application that needs a tLDP session

- Benefits
  - Establishment of automatic tLDP session based on negotiated targeted LDP applications
  - Establishment of limited number of tLDP sessions for certain automatic applications
  - Targeted application mapped to LDP FEC elements to advertise only necessary FEC label bindings over the session

Protocol changes

- Advertise and negotiate targeted applications capability (TAC) during tLDP session initialization

- The TAC TLVs capability data consists of one or more targeted application element (TAE) each pertaining to unique targeted application

- On the receipt of a valid TAC TLV, an LSR must generate its own TAC TLV with TAEs

- If there is at least one TAE common between the TAC TLV it has received and its own, the tLDP session proceed to establishment as per RFC 5036. If not, a LSR sends a 'Session Rejected/Targeted Application Capability Mis-Match' message to the peer and close the session

New since last update

Targeted application FEC advertisement procedures

Targeted Application	Description	FEC type mappings
LDPv4 Remote LFA	LDPv4 over LDPv4 or other MPLS tunnel	IPv4 prefix
LDPv6 Remote LFA	LDPv6 over LDPv6 or other MPLS tunnel	IPv6 prefix
LDP FEC 129 PW	LDP FEC 129 Pseudowire	Generalized Pwid FEC Element
mLDP Node Protection Or mLDP Tunneling	mLDP nodeprotection	P2MP, MP2MP-up MP2MP-down HSMPdownstream HSMP-upstream
LDP FEC 128 PW	LDP FEC 128P seudowire	PWid FEC Element
etc	..	..

New since last update

- Interaction of targeted application capabilities and state advertisement control capabilities
    - TAC
        - Facilitates the awareness of targeted applications to both the peers
        - The set of applications negotiated by the TAC mechanism is symmetric between the two LDP peers
    - SAC
        - Responding LSR is not aware of targeted applications
        - Creates asymmetric advertisement of state information between the two peers.
    - Thus the TAC mechanism enables two LDP peers to symmetrically advertise state information for negotiated targeted applications while SAC mechanism enables both of them to asymmetrically disable receipt of state information for some of the already negotiated applications

Use cases

- Remote LFA

- FEC 129

- LDP over RSVP tunneling

- mLDP node protection

Next steps

- Summary
    - Latest version addresses all the comments that
    - that we have received so far
        - Of course, more comments are always welcome
    - Draft addresses real deployment use-cases

- The authors believe that the draft is ready for WGLC