1. Problem:

LDP is a widely used label distribution protocol used for building end-to-end IP/MPLS LSPs across provider network. Many times critical IP applications need faster restoration on a network failure. Currently the fast reroute is provided by installing RSVP bypass tunnel. But, there is a greater need from customers where they want to provide fast restoration with single protocol solution, instead of managing multiple protocols.

2. Summary:

The LDP DOD FRR approach works similar to RSVP-TE Bypass tunnel or facility backup solution, but uses "LDP Downstream-On-Demand" instead of RSVP protocol. Point of Local Repair (PLR) sets up source routed LDP Bypass Tunnel towards the merge point (MP) that avoids the primary links or node of the PLR. PLR calculates an alternate path for protected link and then establishes bypass LDP by using LDP downstream on demand.

After setting up the LDP Bypass tunnel, PLR builds an alternate next-hop with top-label as LDP Bypass and bottom-label as regular LDP label. PLR installs such alternate next-hops into forwarding plane with primary next-hops. Upon protected link or node failure, forwarding plane of the PLR tunnels the primary traffic through the bypass, which guarantees a loop-free path until it merges with primary path. This approach can also be used for mLDP link and node protection.

3. Description:

To provide LDP FRR, it requires LDP protocol extensions. The new TLVs LDP FRR Capability TLV, FRR Address List TLV, "Protection" Fec element and Exclude TLV will be introduced. The protocol extensions are specified in the section 4.

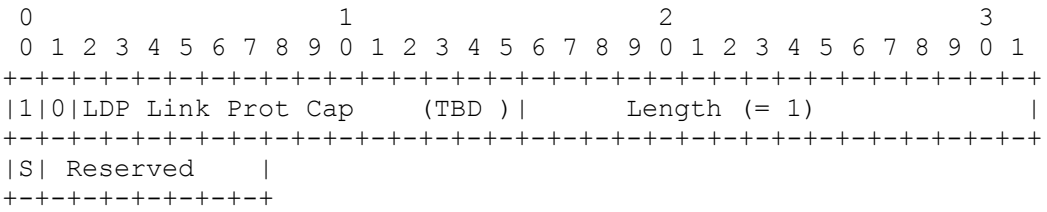
Procedure:

1. LDP will exchange the LDP FRR capability information in the LDP Initialization message by adding new Capability Parameter TLV, LDP FRR Capability TLV, which is used to indicate support of LDP FRR procedures mentioned in this document to provide link and node protection.
2. Once LDP session becomes operational, each LSR sends its remote LDP session addresses by adding new FRR Address List TLV in the Address Message. This is used to notify protection Fec addresses.
3. Each LSR creates targeted LDP sessions to all neighbor nodes as well as to next next hop nodes.
4. The PLR requests the label for the "Protection Fec" by sending label request message to downstream node as well as to "Next Next hop node".
5. The Exclude TLV will be added in the label request message and will be sent on other interface based on the next best link excluding the protected link.
6. After getting label for the protection fec, LDP install this label as backup label as the top label and primary label as the bottom label in the forwarding path.
7. If the primary link or node fails, the forwarding path will use backup label as the top label and packets will sent to backup path.

4. LDP Protocol Extensions

4.1 The LDP FRR Link Protection Capability TLV

A new Capability Parameter TLV is defined, the LDP FRR Link protection Capability. Following is the format of the LDP FRR Link protection Capability Parameter.

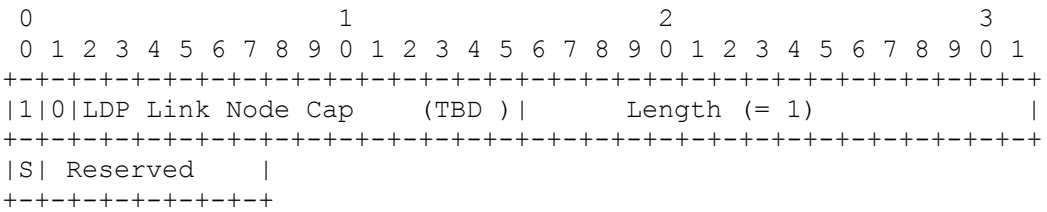


S: As specified in [RFC5561]

The LDP link protection Capability TLV MUST be supported in the LDP Initialization Message. Advertisement of the LDP Link protection Capability indicates support of the procedures for Link protection procedures detailed in this document. If the peer has not advertised the corresponding capability, then label request messages using the PROT FEC Element SHOULD NOT be sent to the peer.

4.2 The LDP FRR Node Protection Capability TLV

A new Capability Parameter TLV is defined, the LDP FRR Node protection Capability. Following is the format of the LDP FRR Node protection Capability Parameter.

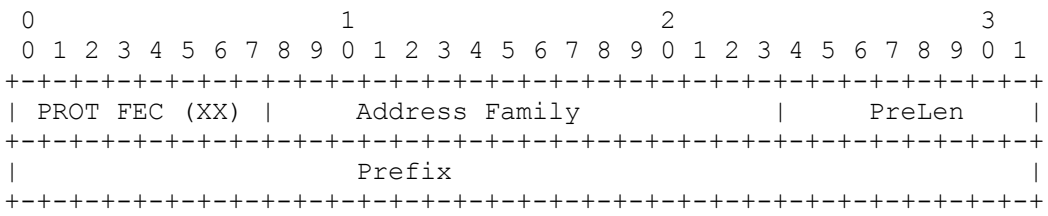


S: As specified in [RFC5561]

The LDP node protection Capability TLV MUST be supported in the LDP Initialization Message. Advertisement of the LDP node protection Capability indicates support of the procedures for Node protection procedures detailed in this document. If the peer has not advertised the corresponding capability, then FRR address messages using the FRR address TLV SHOULD NOT be sent to the peer.

4.3 Protection Fec Element

Protection (PROT) FEC Element value encoding:



Address Family:

Two octet quantity containing a value from ADDRESS FAMILY NUMBERS in [ASSIGNED_AF] that encodes the address family for the address prefix in the Prefix field.

PreLen:

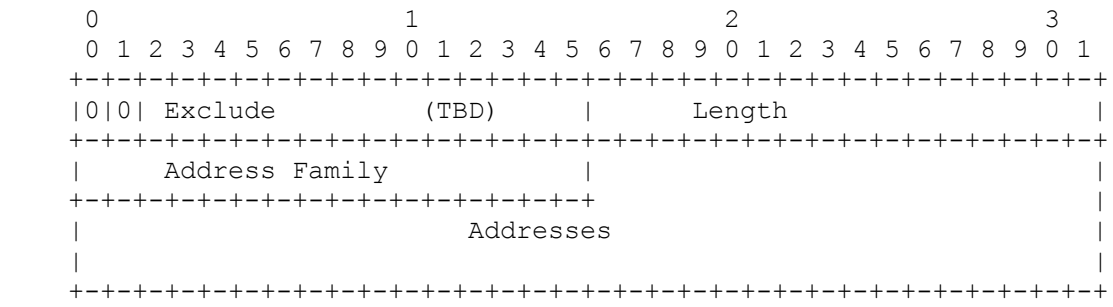
One octet unsigned integer containing the length in bits of the address prefix that follows. A length of zero indicates a prefix that matches all addresses (the default destination); in this case, the Prefix itself is zero octets).

Prefix:

An address prefix encoded according to the Address Family field, whose length, in bits, was specified in the PreLen field, padded to a byte boundary.

4.4 Exclude/Avoid TLV

The Exclude TLV appears in the label request. Its encoding is:



Address Family:
Two octet quantity containing a value from ADDRESS FAMILY NUMBERS in [ASSIGNED_AF] that encodes the addresses contained in the Addresses field.

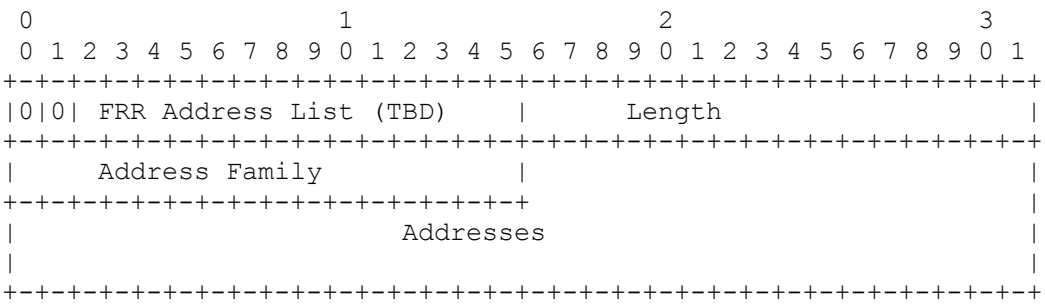
Addresses:
A list of addresses from the specified Address Family. The encoding of the individual addresses depends on the Address Family.

The following address encodings are defined by this version of the protocol:

Address Family	Address Encoding
IPv4	4 octet full IPv4 address
IPv6	16 octet full IPv6 address

4.5 FRR Address List TLV

The FRR Address List TLV appears in the address and address withdraw message. Its encoding is:



Address Family:

Two octet quantity containing a value from ADDRESS FAMILY NUMBERS in [ASSIGNED_AF] that encodes the addresses contained in the Addresses field.

Addresses:

A list of addresses from the specified Address Family. The encoding of the individual addresses depends on the Address Family.

The following address encodings are defined by this version of the protocol:

Address Family	Address Encoding
IPv4	4 octet full IPv4 address
IPv6	16 octet full IPv6 address

5. Link Protection Procedures

Each LSR sends label request message by using the PROT fec which will be sent on the alternate path (secondary path) and optional “Exclude TLV” included in the label request message. The exclude TLV specifies the link address which will be protected. If the Protection Fec address is same as the remote interface address of the link shared between protected node and MP, then there is no need of including the Exclude TLV.

The downstream LSR will exclude this address during CSPF calculations and will calculate a shortest path nexthop with PLR as source and MP as destination and exclude address as the other end of the link. Then it will then send a label request to the nexthop, and the process will continues till the request reaches the MP.

The MP then will send the label mapping message along the path the label request was received. After getting the label mapping message, the LDP will install LDP bypass LSP in the forwarding path and will be used when primary link fails.

6. Node Protection Procedures

Each LSR gets neighbors remote session addresses during session establishment by using FRR address List TLV. By using this address, the LSR established the targeted LDP session to next next node. The targeted session is used only for getting next next hop labels for all fecs.

Once targeted LDP session established, the LSR sends label request with PROT fec to next next node by avoiding the node address. In case of link protection, the exclude address is the remote end link address. In case of node protection, the exclude address is the next node address and Exclude TLV is needed as the exlude address and PROT fec address are different. All other procedure are similar to link protection.

After getting the label mapping message, LDP will install LDP bypass LSP to next next node. All fecs received over targeted session will use this bypass LSP for node failures.

7. Prior Solutions:

There are various methods available for fast restoration:

1. Loop Free Alternative (LFA)
2. Not-via Loop Free Alternative
3. LDP protection using RSVP-TE

LFA has the following issues:

1. LFA does not provide 100% coverage.
2. Micro-forwarding loop issue can potentially nullify the fast restoration benefits.

Not-via Approach:

1. Not-via can provide 100% coverage, it adds complexity.
2. Micro-forwarding –loop issue is another issue.

LDP FRR using RSVP-TE or RSVP-TE Bypass

1. Conceptually this method works similar to the disclosed method with additional complexity, but this method requires RSVP-TE protocol-suite. OSPF-TE, and RSVP protocols.
2. This method is less scalable compared to the invention disclosed. A transit router on a bypass path holds N control state even though they are protecting against failure of same node.

8. Advantages of LDP DOD FRR approach

- Single protocol FRR Solution.
- 100% coverage, independent of topology.
- Easy to manage and understand (As it works similarly to RSVP-TE facility backup)
- More scalable and simpler compared to RSVP-TE Bypass solution
- Implementation overhead is far less compared to RSVP-TE bypass for LDP.