Abstract

To deliver reliable service, multi-protocol label switching (MPLS) requires a set of procedures to enable protection of the traffic carried on label switched paths (LSPs). Thus existing signaling mechanisms must be extended appropriately to support such functionality. Recently, CR-LDP [ ] has introduced extensions to LDP to support the establishment of LSP tunnels. This draft extends CR-LDP to support path protection [ ] in MPLS. Specifically, we provide signaling support for establishing working and backup LSPs.
1. Motivation

Recently, there has been considerable standards activity within the IETF towards establishing a recovery framework for MPLS [3], and towards devising recovery mechanisms for MPLS-based networks [2], [4], [5], [7], [8], [9] and, lately, also for intelligent optical networks [6]. A number of these proposals have considered path-based recovery. There is, therefore, a need to appropriately extend existing signaling protocols to facilitate the operation of these path-based recovery mechanisms.

2. Purpose of this Document

The purpose of this document is to extend CR-LDP to support path protection in MPLS networks. Although we focus here on the path protection mechanism proposed in [2], several of the extensions that we introduce are general, and are applicable to any path-based recovery scheme; for example, optical lightpath recovery.

3. Background

CR-LDP [1] extends the LDP protocol to support the establishment of constraint based routed LSP. New TLVs that have been added for this purpose include LSPID, Explicit Route, Explicit Route Hop, Route Pinning, Preemption, Traffic Parameters, Resource Class, and CR-LSP FEC. To create a constraint routed LSP, the sender node creates an CR-LDP Label Request message. If the sender wishes the Label Request message to follow a pre-determined route, it uses an Explicit Route TLV to identify the route. The destination node of a label-switched
path responds to a Label Request by allocating a label and including a LABEL object in the CR-LDP Label Mapping message that it sends in response to the Label Request message. The Label Mapping message is sent back upstream by following, in reverse order, the path state that was created by the Label Request message on its way downstream.

Although CR-LDP offers some support for reliability, such as a Hello message for detecting link failures and an Initialization Message, it still does not provide adequate support to allow for the operation of a path protection mechanism [2]. In this draft, we introduce extensions to CR-LDP to enable support of MPLS path protection. Specifically, we propose the following:

-- Adding an Explicit Route Protection ER-Hop type to allow for the identification of the endpoints (the path switch LSR (PSL) and the path merge LSR (PML)) of a protected path or path segment (protection domain).

-- Adding Path Protection TLV to the Label Request message to help configure a protection domain.

-- Adding Path Protection Error Codes

4. Terminology

The terminology used in our draft follows that defined in [1], [2] and [3]. We will repeat some of the important terms here for the convenience of the reader.

PSL: Path Switch LSR. A PSL is defined as an LSR that originates both the working and the recovery paths of a protected LSP. The PSL is the source of the recovery path.

PML: Path Merge LSR. A PML is defined as an LSR that receives both the working and the recovery paths of a protected LSP. The PML is the destination of the recovery path.

RNT: Reverse Notification Tree. An RNT is used to notify all upstream neighbors of a node that has detected a fault.

Virtually Merged LSPs: A collection of LSPs that belong to the same CR-LDP session, and all of which terminate at the same destination, and share a common route from some point towards that destination.
5. Extensions to Support Protection Domain Configuration

One of the first requirements for a path-based protection scheme is the configuration of a protection domain [3], namely the identification and configuration of the set of LSRs (or OXCs in an agile optical network) that are the end-points of the protected LSP or LSP segment (or optical trail). In addition, for a path-based protection mechanism [2] it is also necessary to identify the node(s) that will serve as the root(s) of the reverse notification tree(s) (RNT), and to identify the node(s) (PMLs) that will merge traffic from the working and protection paths [2]. The configuration of the protection domain ideally occurs in conjunction with the establishment of the working path. (Note that in a path-based scheme, the protection path may be pre-configured or may be configured after the fault is detected and a notification communicated to the path switch LSR (PSL), which is responsible for switching traffic from the failed working path to the protection/backup path.)

CR-LDP allows the path to be specified loosely (each node determines it’s next hop) or explicitly (each node has been given it’s next hop). In either case, the ER TLV is used. An Explicit Route Protection ER-Hop TLV is being defined as an extension to the existing CR-LDP ER message fields. The origination or PSL node in the MPLS network participates in setting up the working and protection paths. The destination or PML point node in the MPLS network participates in setting up a recovery path as a merging network switch element. The PSL learns the working and protection paths that are merged to the same outgoing network switch element during signaling or working/protection path configuration process.

5.1 ER PROTECTION ER-HOP TLV

A new ER-Hop TLV is used to identify the PSL and PML. ER Protection has the following format:

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|0|       Type = 0X0805         |           Length = 12       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|P|  Prot. Type |               Reserved                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Router ID (4 bytes)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Path Protection TLV                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The ER-Hop Type is 0x08ff (TBD), the L bit could be strict or loose (i.e., the L bit could be 0 or 1), and the Length is 12.
Whether this element is the PSL or PML. 0 denotes PSL.

**Protection Type**

The protection type this particular working and protection path pair supports. The current values) are (future values are for FFS):

- 0000000 1+1
- 0000001 1:1

**Router ID**

The element’s Router ID. The ER Protection ER-Hop must follow the appropriate ER-Hop to identify the PSL/PML[2].

**Path Protection TLV**

The PSL, after processing the ER Protection ER-Hop, will add the Path Protection TLV to the Label Request Message. The PML, after processing the ER Protection ER-Hop, will remove the Path Protection TLV from the Label Request Message.

### 5.2 Path Protection TLV

A Label Request message travels from a sender to receiver(s) along the same path(s) used by the data packets. The IP source address of a Label Request message must be an address of the sender it describes, while the destination address must be the DestAddress for the session. These addresses assure that the message will be correctly routed through a non-LDP cloud.

The nodes that the Label Request message travels from a sender to receiver(s) may not need path protection for the entire path. The PSL, after processing the ER Protection ER-Hop, will insert the Path Protection object into the Label Request message. Therefore, only the nodes that are part of the protection domain receive informational elements in regard to protection. The PML, after processing the ER Protection ER-Hop, will remove the Path Protection object from the Label Request message.
The format of an CR-LDP Label Request message with the Path Protection TLV extension is:

<table>
<thead>
<tr>
<th>0</th>
<th>Label Request (0x0401)</th>
<th>Message Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FEC TLV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LSPID TLV (CR-LDP, mandatory)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ER-TLV (CR-LDP, optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Path Protection TLV (CR-LDP, optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic TLV (CR-LDP, optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pinning TLV (CR-LDP, optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resource Class TLV (CR-LDP, optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pre-emption TLV (CR-LDP, optional)</td>
<td></td>
</tr>
</tbody>
</table>

The presence of this TLV specifies that protection is supported. The following table illustrates the structure of the Path Protection TLV.

| 0 | 1 | 2 | 3 |
|---------|-----------------------|-------|
| RNTT    | Holdoff Option       | WTR Option |
|         | R Flags              | RESVD   |

Where the attributes are equal to:

U=0, F=0, type is 0x08FF (TBD), and Length is 8.

RNTT

Specifies how the notification is implemented.

Hold-off Timer Option

Specifies the hold-off time requirements.
Wait-to-Restore Timer Option

Specifies the wait-to-restore time requirements.

Revertive Option

Specifies whether the recovery action is revertive.

Flags

Specifies whether the Label Request message is for the working path or protection path.

RESVD

Reserved for Future Use

5.2.1 RNT Type

Specifies whether the RNT is implemented as a Hop-by-hop (Layer 3) LSP, as an MPLS (Layer 2) LSP, or over SONET K1/K2 bytes. The default is Hop-by-hop, 000. Other valid values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>MPLS LSP</td>
</tr>
<tr>
<td>010</td>
<td>SONET K1/K2</td>
</tr>
</tbody>
</table>

5.2.2 Hold-off and Wait-to-restore Timer Options

In order to give lower layers (i.e. SONET) time to perform restoration, the timer options specify the hold-off and wait-to-restore time requirements. Since each element along the path must be able to support the timer options when specified, the options must be specified in the Label Request message. The defaults (although could be operator defined) for the timer options are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>No timer requirements</td>
</tr>
<tr>
<td>00000001</td>
<td>50ms timer requirements</td>
</tr>
<tr>
<td>00000010</td>
<td>100ms timer requirements</td>
</tr>
<tr>
<td>00000101</td>
<td>1s timer requirements</td>
</tr>
<tr>
<td>00001100</td>
<td>2s timer requirements</td>
</tr>
<tr>
<td>00010100</td>
<td>10s timer requirements</td>
</tr>
<tr>
<td>01000110</td>
<td>1m timer requirements</td>
</tr>
<tr>
<td>01001111</td>
<td>10m timer requirements</td>
</tr>
<tr>
<td>11111111</td>
<td>Policy Derived Timer Requirements</td>
</tr>
</tbody>
</table>

5.2.3 Flags

The following flags are defined:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>Working Path Enabled</td>
</tr>
</tbody>
</table>
This flag permits the ingress node or the PSL to identify that the Label Request Message is for the working path.

0x02  Protection Path Enabled

This flag permits the ingress node or the PSL to identify that the Label Request Message is for the protection/recovery path.

0x04  Extra Traffic

This flag permits the protection links to carry extra traffic. This flag is an indication that any resources allocated to this protection path are available to be used by other traffic, however it does not necessarily mean that the extra traffic will use the same labels as the protection path.

5.3 Status Codes for Protection
In the processing described above, certain errors must be reported as due to failure of established paths specified in the CR-TLVs.

The following defines status code types:

<table>
<thead>
<tr>
<th>Type</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x440000FF</td>
<td>Bad EXPLICIT_ROUTE Protection sub-object</td>
</tr>
<tr>
<td>0x440000FF</td>
<td>Bad PSL node</td>
</tr>
<tr>
<td>0x440000FF</td>
<td>Bad PML node</td>
</tr>
<tr>
<td>0x440000FF</td>
<td>Protection Mechanism not supported</td>
</tr>
</tbody>
</table>

6. Open Issues

1. Extensions to support using SONET or WDM layer for notification need further study.

2. Establishment of a layer 2 path for propagating fault related notification(s) is needed because CR-LDP does not currently provide a mechanism to implement a reverse notification tree (RNT) [2] via the establishment of point-to-multi-point LSPs.

3. Adding a Notification message to carry the fault information signal (FIS) and the fault recovery signal (FRS).

7. Security Concerns

Owens, et al
This Internet Draft does not introduce additional security concerns to signaling in MPLS networks other than those identified in [1].

8. Acknowledgements

We would like to thank Neil Harrison, Dave Allan, and J. Noel Chiappa, and Ben Mack-Crane for useful discussions on MPLS protection, which were helpful in articulating some of the ideas in this draft.

9. Authors’ Addresses

Changcheng Huang
Department of Systems and Computer Engineering
Carleton University
1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
Phone: (613) 520-2600 ext. 2477

Vishal Sharma
Tellabs Research Center
One Kendall Square
Bldg. 100, Ste. 121
Cambridge, MA 02139-1562
Vishal.Sharma@tellabs.com
Phone: 617-577-8760

Srinivas Makam
Tellabs Operations, Inc.
4951 Indiana Avenue
Lisle, IL 60532
Srinivas.Makam@tellabs.com
Ph: 630-512-7217

Ken Owens
Tellabs Operations, Inc.
1106 Fourth Street
St. Louis, MO 63126
Ken.Owens@tellabs.com
Phone: 314-918-1579

Bora Akyol
Pluris, Inc.
10455 Bandley Drive
Cupertino, CA 95014
Akyol@pluris.com
Ph: 408-861-3302

10. References


Owens, et al


