MPLS-TP Linear Protection
draft-weingarten-mpls-tp-linear-protection-02.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 13, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info).
Please review these documents carefully, as they describe your rights
and restrictions with respect to this document.

Abstract

This document describes mechanisms for linear protection of Multi-Protocol Label Switching Transport Profile (MPLS-TP) Label Switched Paths (LSP) and Pseudowires (PW) on multiple layers. Linear protection provides a fast and simple protection switching mechanism that is especially optimized for a mesh topology. It provides a clear indication of the protection status. The mechanisms are described both at the architectural level as well as providing a protocol that is used to control and coordinate the protection switching.
# Table of Contents

1. Introduction .......................... 4
   1.1. Contributing authors .................. 5
2. Conventions used in this document ............ 5
   2.1. Acronyms .......................... 5
   2.2. Definitions and Terminology .......... 5
3. Network objectives ........................ 6
4. Protection architectures .................... 6
   4.1. 1+1 Protection architecture ............ 7
   4.2. 1:1 Protection architecture ............ 7
   4.3. Protection of P2MP networks ............ 8
   4.4. Extension to 1:n protection ............ 9
   4.5. Revertive and non-revertive switching .... 9
5. Protection switching logic ................... 10
   5.1. Protection switching trigger mechanisms ...... 10
   5.2. Hold-off timer ........................ 11
   5.3. Protection switching control logical architecture .... 11
       5.3.1. PSC Status Module ................. 12
6. Protection switching coordination (PSC) protocol ........ 13
   6.1. Protocol format ........................ 14
       6.1.1. PSC Requests ..................... 15
       6.1.2. Path Fault Identifier ............. 16
       6.1.3. Active path indicator .......... 16
       6.1.4. Current Protection Type ........... 16
   6.2. Addressing of PSC requests ............. 17
   6.3. Principles of Operation ............... 17
       6.3.1. PSC States ...................... 17
       6.3.2. Failure or Degraded condition (Working path) ... 18
       6.3.3. Lockout of Protection ............ 19
       6.3.4. Failure or Degraded condition (Recovery path) ... 20
       6.3.5. Operator Controlled Switching ....... 20
       6.3.6. Recovery from switching .......... 22
7. IANA Considerations ........................ 22
8. Security Considerations ........................ 23
9. Acknowledgements .......................... 23
10. References ............................. 23
    10.1. Normative References ................. 23
    10.2. Informative References ............... 23
Authors’ Addresses .......................... 24
1. Introduction

As noted in the architecture for Multi-Protocol Label Switching Transport Profile (MPLS-TP) [7], the overall architecture framework for MPLS-TP is based on a profile of the MPLS and Pseudowire (PW) procedures as specified for the MPLS and (MS-)PW architectures defined in RFC 3031 [3], RFC 3985 [5] and [6]. One of the basic survivability functions, pointed out by the Survivability Framework document [11], is that of simple and rapid protection switching mechanisms for Label Switched Paths (LSP) and Pseudo-wires (PW).

Protection switching is a fully allocated survivability mechanism. It is fully allocated in the sense that the route and bandwidth of the recovery path is reserved for a selected working path. It provides a fast and simple survivability mechanism, that allows the network operator to easily grasp the active state of the network, compared to other survivability mechanisms.

This draft proposes an architecture and protocol to provide protection for the different types of point-to-point (p2p) paths supported by MPLS-TP. These include LSP, PW, Path Segment Tunnels (PST), and Tandem Connections (TC). For unidirectional protection switching a 1+1 architecture is described. For bidirectional switching both a 1+1 and a 1:1 architecture are described.

In 1+1 unidirectional architecture, a recovery transport path is dedicated to each working transport path. Normal traffic is bridged and fed to both the working and the recovery transport entities by a permanent bridge at the source of the protection domain. The sink of the protection domain selects which of the working or recovery entities to receive the traffic from, based on a predetermined criteria, e.g. server defect indication. When used for bidirectional switching the 1+1 protection architecture must also support a Protection Switching Coordination (PSC) protocol. This protocol is used to help synchronize the decisions of both ends of the protection domain in selecting the proper traffic flow.

In the 1:1 architecture, a recovery transport path is dedicated to the working transport path. However, the normal traffic is transmitted only once, on either the working or the recovery path, by using a selector bridge at the source of the protection domain. A selector at the sink of the protection domain then selects the path that carries the normal traffic. Since the source and sink need to be coordinated to ensure that the selector bridge at both ends select the same path, this architecture must support the PSC protocol.
1.1. Contributing authors

Hao Long (Huawei)

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].

2.1. Acronyms

This draft uses the following acronyms:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNR</td>
<td>Do not revert</td>
</tr>
<tr>
<td>FS</td>
<td>Forced Switch</td>
</tr>
<tr>
<td>GACH</td>
<td>Generic Associated Channel Header</td>
</tr>
<tr>
<td>LSR</td>
<td>Label Switching relay</td>
</tr>
<tr>
<td>MPLS-TP</td>
<td>Transport Profile for MPLS</td>
</tr>
<tr>
<td>MS</td>
<td>Manual Switch</td>
</tr>
<tr>
<td>P2P</td>
<td>Point-to-point</td>
</tr>
<tr>
<td>P2MP</td>
<td>Point-to-multipoint</td>
</tr>
<tr>
<td>PDU</td>
<td>Packet Data Unit</td>
</tr>
<tr>
<td>PSC</td>
<td>Protection Switching Coordination Protocol</td>
</tr>
<tr>
<td>PST</td>
<td>Path Segment Tunnel</td>
</tr>
<tr>
<td>SD</td>
<td>Signal Degrade</td>
</tr>
<tr>
<td>SF</td>
<td>Signal Fail</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>WTR</td>
<td>Wait-to-Restore</td>
</tr>
</tbody>
</table>

2.2. Definitions and Terminology

Protection domain: Transport path (e.g. LSP, PW, PST, TC) that provides protection for its normal traffic. The protection domain consists of the following elements - Two end points (East and West) that in each direction one acts as the source and the other as the sink, a working path, and a recovery path.

Recovery path: A transport path dedicated to transport normal user traffic in case of a failure of the Working path.

Working path: A transport path used for transport of normal user traffic, under normal conditions.

The terminology used in this document is based on the terminology used in other related documents.
defined in [10]. In addition, we use the term LSR to refer to a MPLS-TP Network Element, whether it is a LSR, LER, T-PE, or S-PE.

3. Network objectives

Linear protection for MPLS-TP should comply with the following network objectives:

- **Switch time**: protection switching should operate as quickly as possible. A switching time of less than 50ms has been proposed as a target for certain use cases. The switching time does not include the detection time and the hold-off time.

- **Hold-off times**: to allow protection by the layer that is closest to the detected defect and retain the stability of the network, a hold-off timer should be employed when a defect is detected. At the expiration of the hold-off period, the defect should be rechecked and if still existent the protection mechanism shall be invoked.

- **Extent of protection**: the protection mechanism should restore interrupted traffic due to a facility (link or node) failure, within a protection domain. Traffic terminating at a failed node may be disrupted, however, traffic passing through to other nodes should be protected.

- **Operation modes**: the protection mechanism should provide protection for both unidirectional and bidirectional transport entities. The protection mechanism should support both revertive and non-revertive modes of operation.

- **Manual control**: administrative commands may be provided for manual control of the protection switching operations. The following are examples of possible manual commands: Clear, Forced Switch, Manual Switch (see definitions in [10]).

4. Protection architectures

The protection mechanism defined here supports transport paths (as defined in [2]') within a mesh-based network. This includes support for unidirectional, both point-to-point and point-to-multipoint, and bidirectional point-to-point paths. This protection may be supported by different protection architectures as described in the following subsections.
4.1. 1+1 Protection architecture

The 1+1 protection architecture provides for a fully dedicated recovery path in addition to the configured working path. Both the recovery and working path MUST support the full SLA requirements for the traffic between the two end points of the protection domain.

In this architecture (see Figure 1), all traffic from LSR A to LSR Z is bridged, using the permanent bridge at LSR A, to both transport entities, and LSR Z employs a selector bridge to receive the data from the working path, discarding the packets from the recovery path.

In case of a condition, e.g. a failure condition or an operator command, where protection switching is indicated, LSR Z SHOULD select the data packets from the recovery path and discard any data packets from the working path.

It should be further noted that OAM packets for monitoring the protection domain, or control plane packets, may be transmitted on the "non-active" transport path. These packets SHALL NOT be discarded.

```
|-------------Protection Domain--------------|
|**********Working path************              |
+--------+                                      +--------+
    LSR /                                      LSR \
   A (<  
    PB \                                      >) Z
    +--------+                                      +--------+
    |---------|                                      |---------|
|PB: Permanent Bridge                       | SB: Selector Bridge|
\***********Recovery path**********/         \***********Recovery path**********/
```

Figure 1: 1+1 Unidirectional protection architecture

When using the 1+1 architecture for bidirectional switching, each of the end-points would have both a permanent bridge and a selector bridge one for each direction.

4.2. 1:1 Protection architecture

Another option to protect a bidirectional connection is a 1:1 architecture. This architecture provides for a fully allocated recovery transport path in addition to the working transport path used for normal user data. In principle, this recovery path MUST support the full capacity and bandwidth of the SLA but may be
degraded from the normal working path.

In this architecture both ends of the protection domain employ a Selector bridge (SB) that selects the transport path to transmit the data packets over. Under normal conditions the SB selects the working path for transmission of the data packets. When a condition that triggers protection switching is active, the SB at either end need to select the recovery path for data transmission.

```
|-------------Protection Domain--------------|
/**********Working path**********\
+--------+   ==============================   +--------+
| LSR    /|                                    |
| A [<   |                                    | >} Z |
| SB     |
+--------+   ==============================   +--------+
Recovery path
```

SB: Selector Bridge

Figure 2: 1:1 Bidirectional protection architecture using working path

In principle, the recovery path could be used for "extra traffic", i.e. preemptible traffic. However, if protection switching is in force then this traffic SHALL be pre-empted by the protected data that is being transmitted on this path. In any case, the recovery path MUST support OAM and protection coordination traffic (see section 6).

This architecture requires communication between the end-points of the protection domain to coordinate the protection state. In general bidirectional protection switching requires coordination between the end-points and verification that both transmission directions remain on a co-routed bidirectional path.

4.3. Protection of P2MP networks

[2] specifies that all P2MP MPLS-TP connections are unidirectional by nature. It further requires that these connections should be supported by both 1+1 and 1:1 protection architectures.

When protecting a P2MP network using a 1+1 protection architecture, the basic protection mechanism is still relevant. The root LSR will bridge the user traffic (using a permanent bridge) to both the
working and recovery transport entities. Each leaf LSR will select the traffic from one transport path according to its own local triggers. This may lead to a situation where, due to a failure condition on one branch of the network, that some leaf LSRs may select the working transport path, while other leaf LSRs may select traffic from the recovery transport path.

When protecting a P2MP network using 1:1 protection architecture, there is a need for the root LSR to identify the existence of a failure condition on any of the branches of the network.

Editor’s note: This requires the use of tools from the OAM toolset [9], and also a return path that can pass the indication back to the root LSR. This protection architecture, in the P2MP case, also requires that each leaf LSR selects the traffic from the same incoming transport entity that was selected by the root LSR. When protection switching is triggered, the root LSR selects the recovery transport path to transfer the traffic and each leaf LSR needs to select this same transmission. End of Editor’s note!!

4.4. Extension to 1:n protection

This is for further study

Editor’s note: Definition of 1:n protection should be that there is one recovery path that is given a different label relative to each working path that is being protected. When any one of the working paths indicates a failure, then the traffic is redirected to the recovery path, using the dedicated recovery label. When more than one working path reports a failure, then the path with the highest priority will have its traffic redirected to the recovery path and traffic from other paths will not be protected. It should be noted further that 1:n protection cannot be supported using a single phase protocol, since the coordination of which is the highest priority path and notification to other paths needs acknowledgement, i.e. at least a second phase.

There is a suggestion to have a separate draft for the extension to 1:n protection, that would include a definition to the two phased protocol. This draft should only prepare the groundwork of the protocol so as not to preclude the 1:n protection.

This is still under discussion. End of Editor’s note

4.5. Revertive and non-revertive switching

In revertive operation, the normal traffic signal is restored to the working transport path after the condition that triggered the
switching has cleared. When a manual operator command (e.g. Forced Switch) has cleared, then the reversion happens immediately. When a failure or degradation of service has cleared, the reversion may be delayed until the expiry of a Wait-to-restore timer, used to neutralize the effect of intermittent defects.

In non-revertive mode of operation, the normal traffic continues to use the recovery transport path, even after the condition that triggered has cleared. Eventually, the network may be reverted to use the working transport path, by using an explicit operator command (see section 6.3.5).

The 1+1 protection architecture is often provisioned to operate as non-revertive, since the recovery transport path is fully dedicated in any case and continuing to select it on the sink avoids a second disturbance to the traffic. There may, however, be certain operator policies that dictate provisioning revertive operation for 1+1 protection.

The 1:1 protection architecture is often provisioned to operate in revertive mode. This takes advantage of the (typically) more optimized working transport path, even at the cost of the additional disturbance to traffic from the additional switch.

The configuration of revertive or non-revertive operation SHOULD be the same at both ends of the protection domain.

5. Protection switching logic

5.1. Protection switching trigger mechanisms

The protection switching should be initiated in reaction to any of the following triggers:

- Server layer indication - if any of the lower layers (e.g. the physical layer) raises an interrupt indicating that a failure has been detected.

- OAM signalling - if the OAM continuity and connectivity verification tools detect that there is a loss of continuity or mis-connectivity or the performance monitoring indicates a degradation of the utility of the working path for the current transport path. In cases of signal degradation, switching to the recovery path SHOULD only be activated if the recovery path can guarantee better conditions than the degraded working path.
o Control plane - if there is a control plane active in the network (either signalling or routing), it may send an indication of problems on the working path. Protection switching should be initiated as a result, until the problems are signalled to have cleared. If the control-plane is based on GMPLS [13] then the recovery process should comply with the process described in [12].

o Operator command - the network operator may issue commands that trigger protection switching. The commands that are supported include - Forced Switch, Manual Switch, Clear, Lockout of Protection, (see definitions in [10]).

5.2. Hold-off timer

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer.

Each protection group should have a provisionable holdoff timer. The suggested range of the holdoff timer is 0 to 10 seconds in steps of 100 ms with an accuracy within 5 ms. The default duration for the holdoff timer is 0 seconds.

When a failure condition is detected, this will not immediately activate protection switching if the provisioned hold-off timer value is non-zero. Rather, the hold-off timer will be started. When the hold-off timer expires, we check if a failure condition is still present. If there is still a failure condition, then the protection switching is activated, regardless if it is the same failure condition that caused the activation the hold-off timer.

5.3. Protection switching control logical architecture

Protection switching processes the triggers described above together with the inputs received from the far-end LSR. These inputs cause the LSR to take certain actions, e.g. switching the Selector Bridge to select the working or recovery path, and to transmit different protocol messages.
Figure 3: Protection switching control logic

Figure 3 describes the logical architecture of the protection switching control. The Local Request logic unit accepts the triggers from the OAM, external operator commands, and from the local control plane (when present) and determines the highest priority request. This high-priority request is passed to both the PSC Message generator, that will generate the appropriate protocol message to be sent to the far-end LSR, and the Global Request logic, that will cross-check this local request with the information received from the far-LSR. The Global Request logic then processes these two PSC requests that determines the highest priority request that is passed to the PSC Process logic. The PSC Process logic uses this input to determine what actions need to be taken, e.g. switching the Selector Bridge, and the current status of the protection domain.

5.3.1. PSC Status Module

The PSC Control Logic must retain the status of the protection domain. The possible different states indicate the current status of the protection environment, and can be in one of three states:
o Normal (Idle) state - When both the recovery and the working paths are fully allocated and active, data traffic is being transmitted over the working path, and there are no events being reported within the domain.

o Protecting state - When the working path has reported a signal failure or degradation of signal and the data traffic has been redirected to the recovery path.

o Unavailable state - When the recovery path is unavailable, either as a result of reporting a SF or SD condition, or as a result of an administrative Lockout command.

This state may affect the actions taken by the control logic, and therefore, the PSC Status Module transfers the current status to the Local Request Logic.

See section 6.3.1 for details on what actions are affected by the PSC state.

6. Protection switching coordination (PSC) protocol

Bidirectional protection switching requires coordination between the two end-points in determining which of the two possible paths, the working or recovery path, is operational in any given situation. When protection switching is triggered as described in section 5.1, the end-points must inform each other of the switch-over from one path to the other in a coordinated fashion.

There are different possibilities for the type of coordinating protocol. One possibility is a two-phased coordination in which the MEP that is initiating the protection switching sends a protocol message indicating the switch but the actual switch-over is performed only after receiving an ‘Ack’ from the far-end MEP. The other possibility is a single-phased coordination, in which the initiating MEP switches over to the alternate path and informs the far-end of the switch, and the far-end must complete the switch-over.

In the following sub-sections we describe the protocol messages that should be used between the two end-points of the protection domain.

For the sake of simplicity of the protocol, this protocol is based on the single-phase approach described above.

The protocol messages SHOULD be transmitted over the recovery path only. This allows the transmission of the messages without affecting the normal traffic in the most prevalent case, i.e. the normal state.

In addition, limiting the transmission to a single path avoids possible conflicts and race conditions that could develop if the PSC messages were sent on both paths.

6.1. Protocol format

The protocol messages SHALL be sent over the GACH as described in [8]. There is a single channel type for the set of PSC messages, each message will be identified by the first field of the ACH payload as described below. PSC messages SHOULD support addressing by use of the method described in [8]. The following figure shows the format for the full PSC message.

```
+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 1|0 0 0 0|0 0 0 0 0 0 0 0|   MPLS-TP PSC Channel Code    |
+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    ACH TLV Header                             |
+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                    Addressing TLV                             +
|                                                               |
+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                    PSC Control Packet                         +
+----------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Figure 4: Format of PSC packet with a GACH header
```

Where:

- **MPLS-TP PSC Channel Code** is the GACH channel number assigned to the PSC = TBD
- **The ACH TLV Header** is described in [8]
- **The use of the Addressing TLV** are described in section 6.2
- **The following figure shows the format of the PSC Control message** that is the payload for the PSC packet.

Editor’s note: There is a suggestion that this format should be aligned with the format used by G.8031/G.8131/Y.1731 in ITU. The argument being that this would make it easier to pass review from ITU and allow easier transfer of technology.

The counter-argument is that the ITU format is based upon an attempt
to find a common format for different functionality and therefore involves different fields that are not necessary for the protection switching. Defining a new dedicated format would make for a simpler and more intuitive protocol. End of editor’s note.

```
+---------------+---------------+---------------+---------------+
| Ver | Request | Typ |   FPath     |     Path        |    Reserved   |
+---------------+---------------+---------------+---------------+
```

Figure 5: Format of the PSC control packet

Where:

- **Ver**: is the version of the protocol, for this version the value SHOULD be 0.
- **Request**: this field indicates the specific PSC request that is being transmitted, the details are described in section 6.1.1
- **Typ**: indicates the type of protection scheme currently supported, more details are given in section 6.1.4
- **FPath**: used to indicate the path that is reporting a failure condition, the possible values are described in section 6.1.2
- **Path**: used to indicate the currently active path, possible values are described in section 6.1.3
- **Rsv, Reserved**: these fields are reserved for possible future use.

**6.1.1. PSC Requests**

The Protection Switching Coordination (PSC) protocol SHALL support the following request types, in order of priority from highest to lowest:

- **(1111) Clear**
- **(1110) Lockout protection**
- **(1101) Forced switch**
- **(0110) Signal fault**
- **(0101) Signal degrade**
See section 6.3 for a description of the operation of the different requests.

### 6.1.2. Path Fault Identifier

The Fpath field of the PSC control SHALL be used only in a Signal fault (0101) or Signal degrade (0100) control packet. Its value indicates on which path the signal anomaly was detected. The following are the possible values:

- 0: indicates that the fault condition is on the Recovery path
- 1: indicates that the fault condition is on the Working path
- 2-255: for future extensions

### 6.1.3. Active path indicator

The Path field of the PSC control SHALL be used to indicate which path the source MEP is currently using for data transmission. The MEP should compare the value of this bit with the path that is locally selected for data transmission to verify that there is no inconsistency between the two end-points of the protected domain. If an inconsistency is detected then an alarm should be raised. The following are the possible values:

- 0: indicates that normal traffic is being transmitted on the Working path.
- 1: indicates the Recovery path is being used to transmit the normal traffic from the Working path.
- 2-255: for future extensions

### 6.1.4. Current Protection Type

The Typ field indicates the currently configured protection architecture type, this should be validated to be consistent for both ends of the protected domain. If an inconsistency is detected then an alarm should be raised. The following are the possible values:
o 11: 1+1 bidirectional switching
o 10: 1:1 bidirectional switching
o 01: 1+1 unidirectional switching
o 00: 1:1 unidirectional switching

6.2. Addressing of PSC requests

The PSC request should include the following addressing information, in ACH-TLV fields (as described in [8]):

- Source address: the address of the LSR that initiated this message. There MUST be only one Source address TLV present in the message.

- Destination address: the address of the LSR of the far-end MEP that this message is intended for. There MUST be at least one Destination address TLV present in the message.

- Fault location: the address of the LSR reporting a SF condition, if known. This TLV is present only in SF or SD messages and only if the information was provided by the switching trigger.

The format for the TLV fields are as specified in [8].

6.3. Principles of Operation

In all of the following sub-sections, assume a protected domain between LSR-A and LSR-Z, using paths W (working) and R (recovery).

6.3.1. PSC States

6.3.1.1. Normal State

When the protected domain has no special condition in effect, the ingress LSR SHOULD forward the user data along the working path, and, in the case of 1+1 protection, the Permanent Bridge will bridge the data to the recovery path as well. The receiving LSR SHOULD read the data from the working path.

The ingress LSR MAY transmit a No Request PSC packet with the Path field set to 0 for the recovery path.
6.3.1.2. Protecting State

When the protection mechanism has been triggered and the protected domain has performed a protection switch, the domain is in the protecting state. In this state the normal traffic is transmitted and received on the recovery path.

If the protection domain is currently in a protecting state, then the LSRs SHOULD NOT accept a Manual Switch request.

If the protection domain is currently in a protecting state, and a Forced Switch is requested then the normal traffic SHALL continue to be transmitted on the recovery path even if the original protection trigger is cleared.

6.3.1.3. Unavailable State

When the recovery path is unavailable - either as a result of a Lockout operator command (see section 6.3.3), or as a result of a SF or SD detected on the recovery path (see section 6.3.4) - then the protection domain is in the unavailable state. In this state, the normal traffic is transmitted and received on the working path.

While in unavailable state any event that would trigger a protection switching SHOULD be ignored with the following exception - If a Signal Degrade request is received, then protection switching will be activated only if the recovery path can guarantee a better signal than the working path.

The protection domain will exit the unavailable state and revert to the normal state when, either the operator clears the Lockout command or the recovery path recovers from the signal fault or degraded situation. Both ends will resume sending the PCS packets over the recovery path, as a result of this recovery.

6.3.2. Failure or Degraded condition (Working path)

If one of the LSRs (for example, LSR-A) detects a failure condition or a serious degradation condition on the working path that warrants invoking protection switching, then it SHOULD take the following actions:

- Switch all traffic for LSR-Z to the recovery path only.
- Transmit a PCS control packet, using GACH, with the appropriate Request code (either Signal fault or Signal degrade), the Fpath set to 1, to indicate that the fault/degrade was detected on the working path, and the Path set to 0, indicating that normal
traffic is now being transmitted on the recovery path. This transmission should be repeated every xx ms for the duration of the failure/degrade condition.

- Verify that LSR-Z replies with a PCS control packet indicating that it has switched to the recovery path. If this is not received after xxx then send an alarm to the management system.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has switched, it SHOULD perform the following actions:

- Check priority of the request
- Switch all traffic addressed to LSR-A to the recovery path only.
- Begin transmission of a PCS control packet, using GACH, with the appropriate Request code (either Signal fault or Signal degrade), the Fpath set to 1, to indicate that the fault/degrade was detected on the working path, and the Path set to 1, indicating that traffic is now being transmitted on the recovery path. This transmission should be repeated every xx ms for the duration of the failure/degrade condition.

### 6.3.3. Lockout of Protection

If one of the LSRs (for example, LSR-A) receives a management command indicating that the protection is disabled, then it SHOULD indicate this to the far-end LSR (for example, LSR-Z) that it is not possible to use the recovery path. The following actions MUST be taken:

- Transmit a PCS control packet, using GACH, with the Request code set to Lockout of protection (1010), the Fpath set to 0, and the Path set to 0.
- All normal traffic packets should be transmitted on the working path only.
- Verify that the far-end LSR (for example LSR-Z) is forwarding the data packets on the working path. Raise alarm in case of mismatch.
- The PSC control logic should go into Unavailable state.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has switched, it SHOULD perform the following actions:
o Check priority of request

o Switch all normal traffic addressed to LSR-A to the working path only.

o The PSC control logic should go into Unavailable status.

o Begin transmission of a PCS control packet, using GACH, with the appropriate Request code (Lockout of protection), the Fpath set to 0, and the Path set to 0, indicating that traffic is now being transmitted on the working path only. This transmission should be repeated every xx ms for the duration of the lockout condition.

6.3.4. Failure or Degraded condition (Recovery path)

If one of the LSRs (for example, LSR-A) detects a failure condition or a serious degradation condition on the recovery path, then it SHOULD take the following actions:

o Begin transmission of a PCS control packet with the appropriate Request code (either Signal fault or Signal degrade), the Fpath set to 0, to indicate that the fault/degrade was detected on the recovery path, and the Path set to 1, indicating that traffic is now being forwarded on the working path. This transmission should be repeated every xx ms for the duration of the failure/degrade condition. Note that this will actually reach the far-end if this is a unidirectional fault or recovery path is possibly in a degraded situation.

o The PSC control logic should go into Unavailable state.

o All traffic MUST be transmitted on the working path for the duration of the SF/SD condition.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has become Unavailable, it SHOULD perform the following actions:

o Transmit all traffic on the working path for the duration of the SF/SD condition

o The PSC Control logic should go into Unavailable state.

6.3.5. Operator Controlled Switching

If the management system indicated to one of the LSRs (for example LSR-A) that a switch is necessary, e.g. either a Forced Switch or a Manual Switch, then the LSR SHOULD switch the traffic to the recovery
path and perform the following actions:

- Switch all data traffic to the recovery path only.

- Transmit a PCS control packet, using GACH, with the appropriate Request code (either Manual switch or Forced switch), the Fpath set to 0, to indicate that the fault/degrade was detected on the working path, and the Path set to 1, indicating that traffic is now being forwarded on the recovery path. This transmission should be repeated every xx ms for the duration of the switch condition.

- Verify that LSR-Z replies with a PCS control packet indicating that it has switched to the recovery path. If this is not received after xxx then send an alarm to the management system.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has switched, it SHOULD perform the following actions:

- Check priority of the request

- Switch all normal traffic addressed to LSR-A to the recovery path only.

- Begin transmission of a PCS control packet, using GACH, with the appropriate Request code (either Manual switch or Forced switch), the Fpath set to 1, to indicate that the fault/degrade was detected on the working path, and the Path set to 1, indicating that traffic is now being forwarded on the recovery path. This transmission should be repeated every xx ms for the duration of the switch condition.

6.3.5.1. Clearing operator commands

The operator may clear the switching condition by issuing a Clear request. This command will cause immediate recovery from the switch that was initiated by any of the previous operator commands, i.e. Forced Switch or Manual Switch. In addition, a Clear command after a Lockout Protection command should clear the Unavailable state and return the protection domain to the normal state.

If the Clear request is issued in the absence of a Manual Switch, Forced Switch, or Lockout protection, then it SHALL be ignored. In the presence of any of these commands, the Clear request SHALL clear the state affected by the operator command.
6.3.6. Recovery from switching

When the condition that triggered the protection switching clears, e.g. the cause of the failure condition has been corrected, the operator clears a Manual Switch, then the protection domain SHOULD follow the following procedures:

- If the network is configured for non-revertive behaviour, then the two LSRs SHOULD transmit DNR (Request code 0010) messages. When the operator clears the non-revertive condition, the two LSRs SHOULD return to use of the working transport path and transmit No request (Request code 0000) messages.

- If the network is recovering from an operator switching command (in revertive mode), then both LSRs SHOULD return to using the working transport path and transmit No request (Request code 0000) messages.

- If the network is recovering from a failure or degraded condition (in revertive mode), then the LSR that detects this recovery SHALL activate a local Wait-to-restore (WTR) timer (see section 6.3.6.1) to verify that there is not an intermittent failure. After the WTR expires, the LSR SHOULD return to using the working transport path and transmit No request (Request code 0000) messages.

6.3.6.1. Wait-to-restore timer

In revertive mode, in order to prevent frequent activation of protection switching due to an intermittent defect, the working transport path must become stable and fault-free before reverting to the normal condition. In order to verify that this is the case a fixed period of time must elapse before the normal traffic uses the working transport path. This period, called the WTR period, should be configurable by the operator in 1-minute intervals within the range 1-12 minutes. The default value is 5 minutes.

During this period, if a failure condition is detected on the working transport path, then the WTR timer is stopped and the normal traffic SHALL continue to be transported over the recovery transport path. If the WTR timer expires without being pre-empted by a failure, then the traffic SHOULD be returned to use the working transport path (as above).

7. IANA Considerations

This document makes no request of IANA.
8. Security Considerations

This document does not by itself raise any particular security considerations.

9. Acknowledgements

The authors would like to thank all members of the teams (the Joint Working Team, the MPLS Interoperability Design Team in IETF and the T-MPLS Ad Hoc Group in ITU-T) involved in the definition and specification of MPLS Transport Profile.

10. References

10.1. Normative References


10.2. Informative References


Authors’ Addresses

Stewart Bryant (editor)
Cisco
United Kingdom

Email: stbryant@cisco.com

Nurit Sprecher (editor)
Nokia Siemens Networks
3 Hanagar St. Neve Ne’eman B
Hod Hasharon, 45241
Israel

Email: nurit.sprecher@nsn.com
Huub van Helvoort (editor)
Huawei
Kolkgriend 38, 1356 BC Almere
Netherlands

Phone: +31 36 5316076
Email: hhelvoort@huawei.com

Annamaria Fulignoli
Ericsson
Italy

Phone:
Email: annamaria.fulignoli@ericsson.com

Yaacov Weingarten
Nokia Siemens Networks
3 Hanagar St. Neve Ne’eman B
Hod Hasharon, 45241
Israel

Phone: +972-9-775 1827
Email: yaacov.weingarten@nsn.com