Network Working Group	S. Bryant
Internet-Draft	E. Osborne
Intended status: Standards Track	Cisco
Expires: February 05, 2012	N. Sprecher
	Nokia Siemens Networks
	A. Fulignoli, Ed.
	Ericsson
	Y. Weingarten, Ed.
	Nokia Siemens Networks
	August 04, 2011

MPLS-TP Linear Protection
draft-ietf-mpls-tp-linear-protection-09.txt

Abstract

The Transport Profile for Multiprotocol Label Switching (MPLS-TP) is being specified jointly by IETF and ITU-T. This document addresses the functionality described in the MPLS-TP Survivability Framework document [SurvivFwk] and defines a protocol that may be used to fulfill the function of the Protection State Coordination for linear protection, as described in that document.
This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunications Union Telecommunications Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network as defined by the ITU-T.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The MPLS Transport Profile (MPLS-TP) [TPFwk] is a framework for the construction and operation of packet-switched transport networks based on the architectures for MPLS ([RFC3031] and [RFC3032]) and for Pseudowires (PWs) ([RFC3985] and [RFC5659]) and the requirements of [RFC5654].
Network survivability is the ability of a network to recover traffic delivery following failure, or degradation of network resources. The MPLS-TP Survivability Framework [SurvivFwk] is a framework for survivability in MPLS-TP networks, and describes recovery elements, types, methods, and topological considerations, focusing on mechanisms for recovering MPLS-TP Label Switched Paths (LSPs).
Linear protection in mesh networks – networks with arbitrary interconnectivity between nodes – is described in Section 4.7 of [SurvivFwk]. Linear protection provides rapid and simple protection switching. In a mesh network, linear protection provides a very suitable protection mechanism because it can operate between any pair of points within the network. It can protect against a defect in an intermediate node, a span, a transport path segment, or an end-to-end transport path.

1.1. Protection architectures

Protection switching is a fully allocated survivability mechanism. It is fully allocated in the sense that the route and resources of the protection path are reserved for a selected working path or set of working paths. It provides a fast and simple survivability mechanism, that allows the network operator to easily grasp the active state of the network, that can operate between any pair of points within the network.
As described in the Survivability Framework document [SurvivFwk], protection switching is applied to a protection domain. For the purposes of this document, we define the protection domain of a point-to-point LSP as consisting of two Label Edge Routers (LER) and the transport paths that connect them (see Figure 3 below). For a point-to-multipoint LSP the protection domain includes the root (or source) LER, the destination (or sink) LERs, and the transport paths that connect them.

In 1+1 unidirectional architecture as presented in [SurvivFwk], a protection transport path is dedicated to the working transport path. Normal traffic is bridged (as defined in [RFC4427])and fed to both the working and the protection paths by a permanent bridge at the source of the protection domain. The sink of the protection domain uses a selector to select either the working or protection paths 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 State Coordination (PSC) protocol. This protocol is used to help coordinate between both ends of the protection domain in selecting the proper traffic flow.
In the 1:1 architecture, a protection transport path is dedicated to the working transport path of a single service and the traffic is only transmitted either on the working or the protection path, by using a selector 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 at both ends select the same path, this architecture must support a PSC protocol.
The 1:n protection architecture extends the 1:1 architecture above by sharing the protection path among n services. Again, the protection path is fully allocated and disjoint from any of the n working transport paths that it is being used to protect. The normal data traffic for each service is transmitted either on the normal working path for that service or, in cases that trigger protection switching (as listed in [SurvivFwk]), may be sent on the protection path. The switching action is similar to the 1:1 case where a selector is used at the source. It should be noted that in cases where multiple working path services have triggered protection switching that some services, dependent upon their Service Level Agreement (SLA), may not be transmitted as a result of limited resources on the protection path. In this architecture there may be a need for coordination of the protection switching, and also for resource allocation negotiation. The procedures for this are for further study and may be addressed in future documents.

1.2. Scope of the document

As was pointed out in the Survivability Framework [SurvivFwk] and highlighted above, there is a need for coordination between the end points of the protection domain when employing bidirectional protection schemes. This is especially true when there is a need to verify that the traffic continues to be transported on a bi-directional LSP that is co-routed.
The scope of this draft is to present a protocol for the Protection State Coordination of Linear Protection. The protocol addresses the protection of LSPs in an MPLS-TP network as required by [RFC5654] (in particular requirements 63-65 and 74-79) and described in [SurvivFwk]. The basic protocol is designed for use in conjunction with the 1:1

protection architecture bidirectional protection and for 1+1 protection of a bidirectional path (for both unidirectional and bidirectional protection switching). Applicability of the protocol for 1:1 unidirectional protection and for 1:n protection schemes may be documented in a future document and are out of scope for this document. The applicability of this protocol to additional MPLS-TP constructs and topologies may be documented in future documents.
While the unidirectional 1+1 protection architecture does not require the use of a coordination protocol, the protocol may be used by the ingress node of the path to notify the far-side end point that a switching condition has occurred and verify the consistency of the end point configuration. This use may be especially useful for point-to-multipoint transport paths, that are unidirectional by definition of [RFC5654]. The use of this protocol for point-to-multipoint paths is out of scope for this document and may be addressed in a future applicability document.

1.3. Contributing authors

Hao Long (Huawei), Dan Frost (Cisco), Davide Chiara (Ericsson), Francesco Fondelli (Ericsson),

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 [RFC2119].

2.1. Acronyms

This draft uses the following acronyms:

DNR	Do not revert
FS	Forced Switch
G-ACh	Generic Associated Channel
LER	Label Edge Router
LO	Lockout of protection
MPLS-TP	Transport Profile for MPLS
MS	Manual Switch
NR	No Request
PSC	Protection State Coordination Protocol
SD	Signal Degrade
SF	Signal Fail
SLA	Service Level Agreement

WTR	Wait-to-Restore

2.2. Definitions and Terminology

The terminology used in this document is based on the terminology defined in [RFC4427] and further adapted for MPLS-TP in [SurvivFwk]. In addition, we use the term LER to refer to a MPLS-TP Network Element, whether it is a LSR, LER, T-PE, or S-PE.

3. Protection switching control logic

Protection switching processes the local triggers described in requirements 74-79 of [RFC5654] together with inputs received from the far-end LER. Based on these inputs the LER will take certain protection switching actions, e.g. switching the selector to transmit on the working or protection path for 1:1 protection or switching the selector to receive the traffic for either 1:1 or 1+1 protection, and transmit different protocol messages.
The following figure shows the logical decomposition of the Protection Switching Control Logic into different logical processing units. These processing units are presented in subsequent subsections of this document. This logical decomposition is only intended for descriptive purposes, any implementation that produces the external behavior described in section 4 is acceptable.

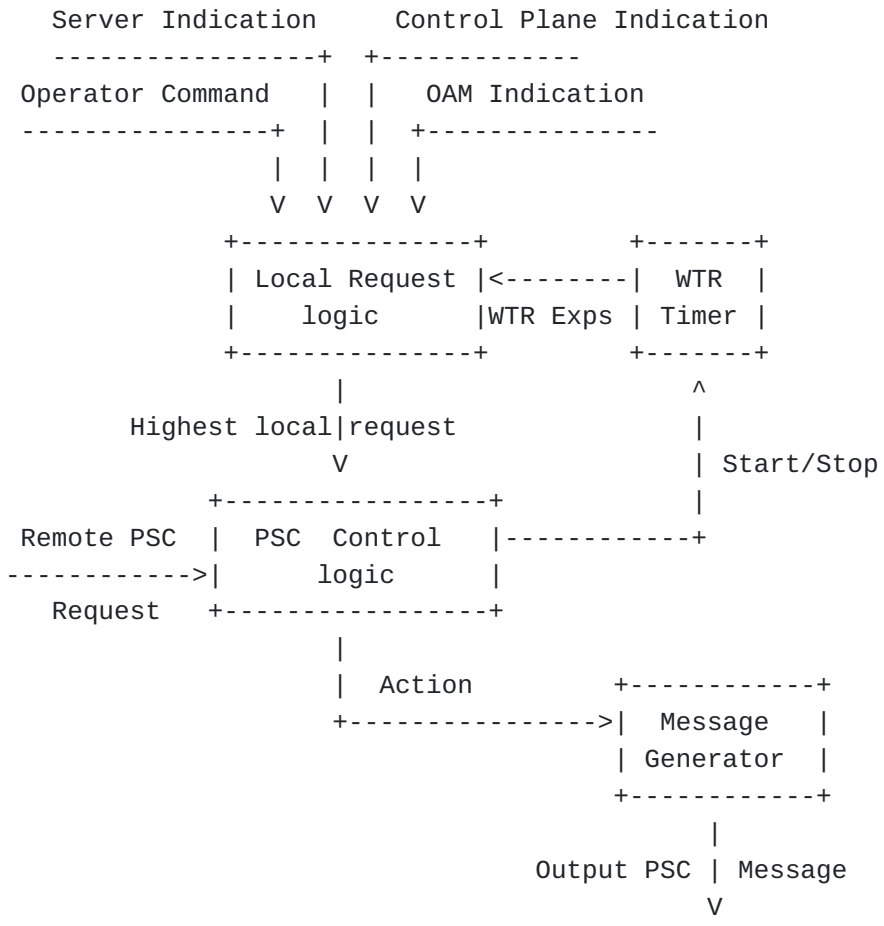


Figure 1 describes the logical architecture of the protection switching control. The Local Request logic unit accepts the triggers from the OAM, external operator commands, from the local control plane (when present), and the Wait-to-Restore timer. By considering all of these local request sources it determines the highest priority local request. This high-priority request is passed to the PSC Control logic, that will cross-check this local request with the information received from the far-end LER. The PSC Control logic uses this input to determine what actions need to be taken, e.g. local actions at the LER, or what message should be sent to the far-end LER, and the current status of the protection domain.

3.1. Local Request Logic

The Local Request logic processes input triggers from five sources:

*Operator command – the network operator may issue local administrative commands on the LER that trigger protection switching. The commands Forced Switch, Manual Switch, Clear, Lockout of Protection (see definitions in [RFC4427]) MUST be supported. An implementation MAY provide additional commands for

operator use; providing that these commands do not introduce incompatable behavior between two arbitrary implementations, they are outside the scope of this document. For example, an implementation could provide a command to manually trigger a "WTR expires" trigger (see below) input without waiting for the duration of the WTR timer; as this merely hastens the transition from one state to another and has no impact on the state machine itself, it would be perfectly valid.

*Server layer alarm indication – the underlying server layer of the network detects failure conditions at the underlying layer and may issue an indication to the MPLS-TP layer. The server layer may employ its own protection switching mechanism, and therefore this input MAY be controlled by a holdoff-timer that SHOULD be configurable by the network operator. The holdoff-timer is described in greater detail in [SurvivFwk].

*Control plane – if there is a control plane active in the network (either signaling or routing), it MAY trigger protection switching based on conditions detected by the control plane. If the control plane is based on GMPLS [RFC3945] then the recovery process SHALL comply with the process described in [RFC4872] and [RFC4873].

*OAM indication – OAM fault management or performance measurement tools may detect a failure or degrade condition on either the working or protection transport path and this MUST input an indication to the Local Request Logic.

*WTR expires – The Wait-to-Restore timer is used in conjunction with recovery from failure conditions on the working path in revertive mode. The timer SHALL signal the PSC control process when it expires and the end point SHALL revert to the normal transmission of the user data traffic.

The input from these sources SHOULD be retained persistently for the duration of condition that initiated the trigger. The Local request logic processes these different input sources and, based on the priorities between them (see section 4.3.2), produces a current local request. If more than one local input source generates a trigger, then the Local request logic selects the higher priority indicator and ignores any lower priority indicator. As a result, there is a single current local request that is passed to the PSC Control logic. The different local requests that may be output from the Local Request Logic are:

*Clear – if the operator cancels an active local administrative command, i.e. LO/FS/MS.

*Lockout of Protection (LO) – if the operator requested to prevent switching data traffic to the protection path, for any purpose.

*Signal Fail (SF) – if any of the Server Layer, Control plane, or OAM indications signaled a failure condition on either the protection path or one of the working paths.

*Signal Degrade (SD) – if any of the Server Layer, Control plane, or OAM indications signaled a degraded transmission condition on either the protection path or one of the working paths. The determination and actions for SD are for further study and may appear in a separate document. All references to SD input are place-holders for this extension.

*Clear Signal Fail (SFc) – if all of the Server Layer, Control plane, or OAM indications are no longer indicating a failure condition on a path that was previously indicating a failure condition.

*Forced Switch (FS) – if the operator requested that traffic be switched from one of the working paths to the protection path.

*Manual Switch (MS) – if the operator requested that traffic be switched from the working path to the protection path. This is only relevant if there is no currently active fault condition or Operator command.

*WTR Expires – generated by the WTR timer completing its period.

If none of the input sources have generated any input then the Local request logic should generate a No Request (NR) request as the current local request .

3.2. Remote Requests

In addition to the local requests, generated as a result of the local triggers, indicated in the previous subsection, the PSC Control Logic SHALL accept PSC messages from the far-end LER of the transport path. Remote messages indicate the status of the transport path from the viewpoint of the far-end LER. These messages may drive state changes on the local MEP, as defined later in this document. When using 1+1 unidirectional protection, an LER that receives a remote request SHALL NOT perform any protection switching action, i.e. will continue to select traffic from the working path and transport traffic on both paths.
The following remote requests may be received by the PSC process:

*Remote LO – indicates that the remote end point is in Unavailable state due to a Lockout of Protection operator command.

*Remote SF – indicates that the remote end point has detected a Signal Fail condition on one of the transport paths in the protection domain. This remote message includes an indication of which transport path is affected by the SF condition. In addition, it should be noted that the SF condition may be either a unidirectional or a bidirectional failure, even if the transport path is bidirectional.

*Remote SD – indicates that the remote end point has detected a Signal Degrade condition on one of the transport paths in the protection domain. This remote message includes an indication of which transport path is affected by the SD condition. In addition, it should be noted that the SD condition may be either a unidirectional or a bidirectional failure, even if the transport path is bidirectional.

*Remote FS – indicates that the remote end point is operating under an operator command to switch the traffic to the protection path.

*Remote MS – indicates that the remote end point is operating under an operator command to switch the traffic from the working path to the protection path.

*Remote WTR – indicates that the remote end point has determined that the failure condition has recovered and has started its WTR timer in preparation for reverting to the Normal state.

*Remote DNR – indicates that the remote end point has determined that the failure condition has recovered and will continue transporting traffic on the protection path due to operator configuration that prevents automatic reversion to the Normal state.

*Remote NR – indicates that the remote end point has no abnormal condition to report.

3.3. PSC Control Logic

The PSC Control Logic accepts the following input –

a. the current local request output from the Local Request Logic (see Section 3.1),

b. the remote request message from the remote end point of the transport path (see Section 3.2), and

c. the current state of the PSC Control Logic (maintained internally by the PSC Control Logic).

Based on the priorities between the different inputs, the PSC Control Logic determines the new state of the PSC Control Logic and what actions need to be taken.
The new state information is retained by the PSC Control Logic, while the requested action should be sent to the PSC Message Generator (see Section 3.4) to generate and transmit the proper PSC message to be transmitted to the remote end point of the protection domain.

3.4. PSC Message Generator

Based on the action output from the PSC Control Logic this unit formats the PSC protocol message that is transmitted to the remote end point of the protection domain. This message may either be the same as the previously transmitted message or change when the PSC control state (see section 3.6) has changed. The messages are transmitted as described in section 4.1 of this document.

3.5. Wait-to-Restore (WTR) timer

The WTR timer is used to delay reversion to Normal state when recovering from a failure condition on the working path and the protection domain is configured for revertive behavior. The length of the timer may be provisioned by the operator. The WTR may be in one of two states – either Running or Stopped. The control of the WTR timer is managed by the PSC Control Logic, by use of internal signals to start and stop, i.e. reset, the WTR timer.
If the WTR timer expires prior to being stopped it SHALL generate a WTR Expires local signal that is processed by the Local Request Logic. If the WTR timer is running, sending a Stop command SHALL reset the timer, and put the WTR timer into Stopped state, but SHALL NOT generate a WTR Expires local signal. If the WTR timer is stopped, a Stop command SHALL be ignored.

3.6. PSC Control States

The PSC Control Logic should maintain information on the current state of the protection domain. Information on the state of the domain is maintained by each LER within the protection domain. The state information would include information of the current state of the protection domain, an indication of the cause for the current state (e.g. unavailable due to local LO command, protecting due to remote FS), and, for each LER, should include an indication if the state is related to a remote or local condition.
It should be noted that when referring to the "transport" of the data traffic, in the following descriptions and later in the document that the data will be transmitted on both the working and the protection paths when using 1+1 protection, and on either the working or the protection path exclusively when using 1:1 protection. When using 1+1

protection, the receiving LER should select the proper transmission, according to the state of the protection domain.
The protection domain states that are supported by the PSC Control Logic are:

- Normal state – Both the protection and working paths are fully allocated and active, data traffic is being transported over (or selected from) the working path, and no trigger events are reported within the domain.

- Unavailable state – The protection path is unavailable – either as a result of an operator Lockout command or a failure condition detected on the protection path.

- Protecting failure state – The working path has reported a failure/degrade condition and the user traffic is being transported (or selected) on the protection path.

- Protecting administrative state – The operator has issued a command switching the user traffic to the protection path.

- Wait-to-restore state – The protection domain is recovering from a SF/SD condition on the working path that is being controlled by the Wait-to-Restore (WTR) timer.

- Do-not-revert state – The protection domain has recovered from a Protecting state, but the operator has configured the protection domain to not automatically revert to the Normal state upon recovery. The protection domain SHALL remain in this state until the operator issues a command to revert to the Normal state or there is a new trigger to switch to a different state.

See section 4.3.3 for details on what actions are taken by the PSC Process Logic for each state and the relevant input.

3.6.1. Local and Remote state

An end-point may be in a given state as a result of either a local input indicator, e.g. OAM, WTR timer, or as a result of receiving a PSC message from the far-end LER. If the state is entered as a result of a local input indicator, then the state is considered a local state. If the state is entered as a result of a PSC message, in the absence of a local input, then the state is considered a remote state. This differentiation affects how the LER reacts to different inputs, as described in Section 4.3.3. The PSC Control logic should maintain, together with the current protection domain state, an indication of whether this is a local or remote state, for this LER.
In any instance where the LER has both a local and remote indicators that cause the protection domain to enter a particular state, then the state is considered a local state, regardless of the order in which the

indicators were processed. If, however, the LER has local and remote indicators that would cause the protection domain to enter different states, e.g. a Local SF on working and a Remote Lockout message, then the input with the higher priority (see section 4.3.2) will be the deciding factor and the source of that indicator will determine whether it is local or remote. In the given example the result would be a Remote Unavailable state transmitting PSC messages that indicate a SF condition on the working path and that the protection path is not being used to transport protected traffic (as described in the next section).

4. Protection state coordination (PSC) protocol

Bidirectional protection switching, as well as unidirectional 1:1 protection, requires coordination between the two end points in determining which of the two possible paths, the working or protection path, is transmitting the data traffic in any given situation. When protection switching is triggered as described in section 3, 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 LER 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 LER. The other possibility is a single-phased coordination, in which the initiating LER performs the protection switchover to the alternate path and informs the far-end LER of the switch, and the far-end LER will complete the switchover.
This protocol is a single-phased protocol, as described above. In the following subsections we describe the protocol messages that are used between the two end points of the protection domain.

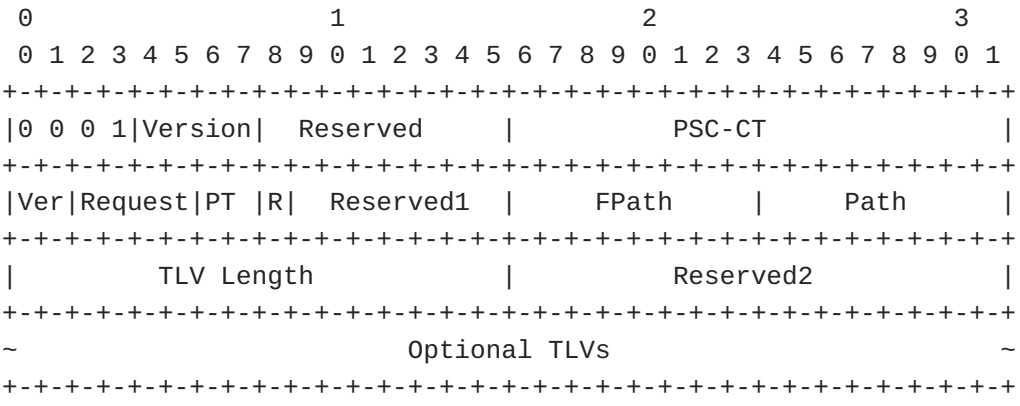
4.1. Transmission and acceptance of PSC control packets

The PSC control packets SHALL be transmitted over the protection path only. This allows the transmission of the messages without affecting the normal data 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.
When the protection domain state is changed due to a local input, three PSC messages SHALL be transmitted as quickly as possible, to allow for rapid protection switching. This set of three rapid messages allows for fast protection switching even if one or two of these packets are lost or corrupted. When the protection domain state changes due to a remote message the LER SHOULD send the three rapid messages. However, when the LER tranfers from WTR state to Normal state as a result of a remote NR message, the three rapid messages SHALL be transmitted. After the transmission of the three rapid messages, the LER MUST retransmit the most recently transmitted PSC message on a continual basis.

Both the default frequency of the three rapid messages as well as the default frequency of the continual message transmission SHALL be configurable by the operator. The actual frequencies used MAY be configurable, at the time of establishment, for each individual protected LSP. For management purposes, the operator SHOULD be able to retrieve the current default frequency values as well as the actual values for any specific LSP. For protection switching within 50ms, it is RECOMMENDED that the default interval of the first three rapid PSC messages SHOULD be no larger than 3.3ms. Using this frequency would allow the far-end to be guaranteed of receiving the trigger indication within 10ms and completion of the switching operation within 50ms. Subsequent messages SHOULD be continuously transmitted with a default interval of 5 seconds. The purpose of the continual messages is to verify that the PSC session is still alive.
If no valid PSC message is received, over a period of several continual messages intervals, the last valid received message remains applicable.

4.2. Protocol format

The protocol messages SHALL be sent over the G-ACh as described in [RFC5586]. There is a single channel type for the set of PSC messages. The actual message function SHALL be identified by the Request field of the ACH payload as described below.
The channel type for the PSC messages SHALL be PSC-CT=0xHH (to be assigned by IANA)
The following figure shows the format for the complete PSC message:



Where:

- *Both Reserved1 and Reserved2 fields MUST be set to 0 and ignored upon receipt.

- *The following subsections describe the remaining fields of the PSC payload.

4.2.1. PSC Ver field

The Ver field identifies the version of the protocol. For this version of the document the value SHALL be 1.

4.2.2. PSC Request field

The PSC protocol SHALL support transmission of the following requests between the two end points of the protection domain:

*(14) Lockout of protection – indicates that the end point has disabled the protection path as a result of an administrative command. Both the FPath and Path fields SHALL be set to 0.

*(12) Forced switch – indicates that the transmitting end point has switched traffic to the protection path as a result of an administrative command. The Fpath field SHALL indicate that the working path is being blocked (i.e. Fpath set to 1), and the Path field SHALL indicate that user data traffic is being transported on the protection path (i.e. Path set to 1).

*(10) Signal Fail – indicates that the transmitting end point has identified a signal fail condition on either the working or protection path. The Fpath field SHALL identify the path that is reporting the failure condition (i.e. if protection path then Fpath is set to 0 and if working path then Fpath is set to 1), and the Path field SHALL indicate where the data traffic is being transported (i.e. if protection path is blocked then Path is set to 0 and if working path is blocked then Path is set to 1).

*(7) Signal Degrade – indicates that that the transmitting end point has identified a degradation of the signal, or integrity of the packet transmission on either the working or protection path. This request is presented here only as a place-holder. The specifics for the method of identifying this degradation is out-of-scope for this document. The details of the actions to be taken for this situation is left for future specification.

*(5) Manual switch – indicates that the transmitting end point has switched traffic to the protection path as a result of an administrative Manual Switch command. The Fpath field SHALL indicate that the working path is being blocked (i.e. Fpath set to 1), and the Path field SHALL indicate that user data traffic is being transported on the protection path (i.e. Path set to 1).

*(4) Wait to restore – indicates that the transmitting end point is recovering from a failure condition of the working path and has started the Wait-to-Restore timer. Fpath SHALL be set to 0 and ignored upon receipt. Path SHALL indicate the working path that is currently being protected (i.e. Path set to 1).

*(1) Do not revert – indicates that the transmitting end point has recovered from a failure/blocked condition, but due to the local settings is is requesting that the protection domain continues to transport the data as if it is in a protecting state, rather than revert to the Normal state. Fpath SHALL be set to 0 and ignored upon receipt. Path SHALL indicate the working path that is currently being protected (i.e. Path set to 1).

*(0) No request – indicates that the transmitting end point has nothing to report, Fpath and Path fields SHALL be set to according to the state of the end point, see section 4.3.3 for detailed scenarios.

All other values are for future extensions (to be administered by IANA) and SHALL be ignored upon receipt.

4.2.3. Protection Type (PT)

The PT field indicates the currently configured protection architecture type, this SHOULD be validated to be consistent for both ends of the protection domain. If an inconsistency is detected then an alarm SHALL be sent to the management system. The following are the possible values:

*3: bidirectional switching using a permanent bridge

*2: bidirectional switching using a selector bridge

*1: unidirectional switching using a permanent bridge

*0: for future extensions

As described in the introduction (section 1.1) a 1+1 protection architecture is characterized by the use of a permanent bridge at the source node, whereas the 1:1 and 1:n protection architectures are characterized by the use of a selector bridge at the source node.

4.2.4. Revertive (R) field

This field indicates that the transmitting end point is configured to work in revertive mode. If there is an inconsistency between the two end points, i.e. one end point is configured for revertive action and the second end point is in non-revertive mode, then the management system SHOULD be notified. Possible values are:

*0 – non-revertive mode

*1 – revertive mode

4.2.5. Fault path (FPath) field

The Fpath field indicates which path (i.e. working or protection) is identified to be in a fault condition or affected by an administrative command, when a fault or command is indicated by the Request field to be in effect. The following are the possible values:

- *0: indicates that the anomaly condition is on the protection path
- *1: indicates that the anomaly condition is on the working path
- *2-255: for future extensions and SHALL be ignored by this version of the protocol.

4.2.6. Data path (Path) field

The Path field indicates which data is being transported on the protection path. Under normal conditions, the protection path (especially in 1:1 or 1:n architecture) does not need to carry any user data traffic. If there is a failure/degrade condition on one of the working paths, then that working path's data traffic will be transported over the protection path. The following are the possible values:

- *0: indicates that the protection path is not transporting user data traffic (in 1:n architecture) or transporting redundant user data traffic (in 1+1 architecture).
- *1: indicates that the protection path is transmitting user traffic replacing the use of the working path.
- *2-255: for future extensions and SHALL be ignored by this version of the protocol.

4.2.7. Additional TLV information

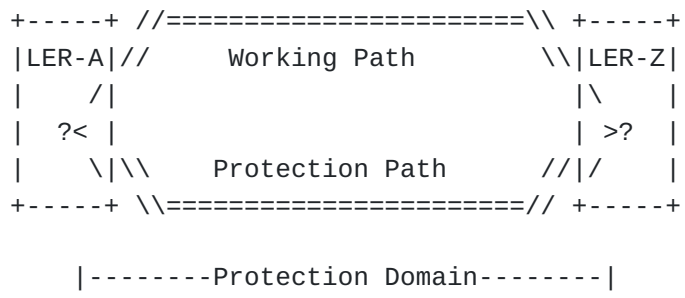
It may be necessary for future applications of the protocol to include additional information for the proper processing of the requests. For this purpose, we provide for optional additional information to be included in the PSC payload. This information MUST include a header that indicates the total length (in bytes) of the additional information.
This information includes the following fields:

- *TLV Length – indicates the number of bytes included in the optional TLV information. For the basic PSC protocol operation described in this document this value MUST be 0.

*Optional TLVs — this includes any additional information formatted as TLV units. There are no TLV units defined for the basic PSC operation.

4.3. Principles of Operation

In all of the following subsections, assume a protection domain between LER-A and LER-Z, using paths W (working) and P (protection) as shown in figure 3.



4.3.1. Basic operation

The purpose of the PSC protocol is to allow an end point of the protection domain to notify its peer of the status of the domain that is known at the end point and coordinate the transmission of the data traffic. The current state of the end point is expressed in the values of the Request field [reflecting the local requests at that end point] and the Fpath field [reflecting knowledge of a blocked path]. The coordination between the end points is expressed by the value of the Path field [indicating where the user data traffic is being transmitted]. Except during a protection switch, the value of the Path field should be identical for both end points at any particular time. The values of the Request and Fpath fields may not be identical between the two end points. In particular it should be noted that a remote message may not cause the end point to change the Request field that is being transmitted while it does affect the Path field (see details in the following subsections).
The protocol is a single-phased protocol. Single-phased implies that each end point notifies its peer of a change in the operation (switching to or from the protection path) and makes the switch without waiting for acknowledgement. As a side-effect of using a single-phased protocol, there will be a short period during state transitions of one-sided triggers (e.g. operator commands, or unidirectional SF) when one LER may be transporting/selecting the data from one transport path while the other end point is transporting/selecting from the other transport path. This should become coordinated once the remote message is received and the far-end LER performs the protection switching operation.

The following subsections will identify the messages that will be transmitted by the end point in different scenarios. The messages are described as REQ(FP, P) – where REQ is the value of the Request field, FP is the value of the Fpath field, and P is the value of the Path field. All examples assume a protection domain between LER-A and LER-Z with a single working path and single protection path (as shown in figure 3). Again it should be noted that when using 1:1 protection the data traffic will be transmitted exclusively on either the protection or working path, while when using 1+1 protection the traffic will be transmitted on both paths and the receiving LER should select the appropriate signal based on the state. The text will refer to this transmission/selection as "transport" of the data traffic. For 1+1 unidirectional protection, the state of the selector will only be switched in reaction to a local message. When receiving a remote message, a LER that is configured for 1+1 unidirectional protection, will transfer to the new remote state, however it will continue to select data according to the latest known local state. When the LER transitions into the Normal state, the PSC Control Process SHALL check the persistent state of the local triggers to decide if it should further transition into a new state.

4.3.2. Priority of inputs

As noted above (in section 3.1) the PSC Control Process accepts input from five local input sources. There is a definition of priority between the different inputs that may be triggered locally. The list of local requests in order of priority are (from highest to lowest priority):

1. Clear (Operator command)
2. Lockout of protection (Operator command)
3. Forced switch (Operator command)
4. Signal Fail on protection (OAM/Control Plane/Server Indication)
5. Signal Fail on working (OAM/Control Plane/Server Indication)
6. Signal Degrade on working (OAM/Control Plane/Server Indication)
7. Clear Signal Fail/Degrade (OAM/Control Plane/Server Indication)
8. Manual switch (Operator command)
9. WTR expires (WTR Timer)
10. No request (default)

As was noted above, the Local request logic SHALL always select the local input indicator with the highest priority as the current local request, i.e. only the highest priority local input will be used to affect the control logic. All local inputs with lower priority than this current local request will be ignored.
The remote message from the far-end LER is assigned a priority just below the similar local input. For example, a remote Signal Fail on protection would have a priority just below a local Signal Fail on protection but above a local Forced Switch input. As mentioned in section 3.6.1, the state transition is determined by the higher priority input between the highest priority local input and the remote message. This also determines the classification of the state as local or remote. The following subsections detail the transition based on the current state and the higher priority of these two inputs.

4.3.3. Operation of PSC States

The following sub-sections present the operation of the different states defined in section 3.6. For each state we define the reaction, i.e. the new state and the message to transmit, to each possible input – either the highest priority local input or the PSC message from the remote LER. It should be noted that the new state of the protection domain is described from the point of view of the LER that is reporting the state, therefore, the language of "the LER goes into a state" is referring to the LER reporting that the protection domain is now in this new state. If the definition states to "ignore" the message, the intention is that the protection domain SHALL remain in its current state and the LER SHALL continue transmitting (as presented in section 4.1) the current PSC message.
When a LER is in a remote state, i.e. state transition in reaction to a PSC message recieved from the far-end LER, and receives a new PSC message from the far-end LER that indicates a contradictory state, e.g. in remote Unavailable state receiving a remote FS(1,1) message, then the PSC Control Logic SHALL reevaluate all inputs (both the local input and the remote message) as if the LER is in the Normal state.

4.3.3.1. Normal State

When the protection domain has no special condition in effect, the ingress LER SHALL 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 protection path as well. The receiving LER SHALL read the data from the working path.
When the LER transitions into the Normal state, the PSC Control Process SHALL check the persistent state of the local triggers to decide if it should further transition into a new state. If the result of this check is a transition into a new state, the LER SHALL transmit the corresponding message described in this section and SHALL use the data path corresponding to the new state. When the protection domain remains

in Normal State, the end-point SHALL transmit a NR(0,0) message, indicating – Nothing to report and data traffic is being transported on the working path.
When the protection domain is in Normal State the following transitions are relevant in reaction to a local input to the LER:

*A local Lockout of protection input SHALL cause the LER to go into local Unavailable State and begin transmission of a LO(0,0) message.

*A local Forced switch input SHALL cause the LER to go into local Protecting administrative state and begin transmission of a FS(1,1) message.

*A local Signal Fail indication on the protection path SHALL cause the LER to go into local Unavailable state and begin transmission of a SF(0,0) message.

*A local Signal Fail indication on the working path SHALL cause the LER to go into local Protecting failure state and begin transmission of a SF(1,1) message.

*A local Manual switch input SHALL cause the LER to go into local Protecting administrative state and begin transmission of a MS(1,1) message.

*All other local inputs SHALL be ignored.

In Normal state, remote messages would cause the following reaction from the LER:

*A remote Lockout of protection message SHALL cause the LER to go into remote Unavailable state, while continuing to transmit the NR(0,0) message.

*A remote Forced switch message SHALL cause the LER to go into remote Protecting administrative state, and begin transmitting a NR(0,1) message.

*A remote Signal Fail message that indicates that the failure is on the protection path SHALL cause the LER (LER-A) to go into remote Unavailable state, while continuing to transmit the NR(0,0) message.

*A remote Signal Fail message that indicates that the failure is on the working path SHALL cause the LER to go into remote Protecting failure state, and transmit a NR(0,1) message.

*A remote Manual switch message SHALL cause the LER to go into remote Protecting administrative state, and transmit a NR(0,1) message.

*All other remote messages SHALL be ignored.

4.3.3.2. Unavailable State

When the protection path is unavailable – either as a result of a Lockout operator command, or as a result of a SF detected on the protection path – then the protection domain is in the unavailable state. In this state, the data traffic SHALL be transported on the working path and is not protected. When the domain is in unavailable state the PSC messages may not get through and therefore the protection is more dependent on the local inputs rather than the remote messages (that may not be received).
The protection domain will exit the unavailable state and revert to the Normal state when either the operator clears the Lockout command or the protection path recovers from the signal fail or degraded situation. Both ends will continue to send the PSC messages over the protection path, as a result of this recovery.
When the LER (assume LER-A) is in Unavailable State the following transitions are relevant in reaction to a local input:

*A local Clear input SHALL be ignored if the LER is in remote Unavailable state. If in local Unavailable state due to a Lockout command, then the input SHALL cause the LER to go to Normal state.

*A local Lockout of protection input SHALL cause the LER to remain in local Unavailable State and transmit a LO(0,0) message to the far-end LER (LER-Z).

*A local Clear SF of the protection path in local Unavailable state that is due to a SF on the protection path SHALL cause the LER to go to Normal state. If the LER is in remote Unavailable state but has an active local SF condition, then the local Clear SF SHALL clear the SF local condition and the LER SHALL remain in remote Unavailable state and begin transmitting NR(0,0) messages. In all other cases the local Clear SF SHALL be ignored.

*A local Forced switch SHALL be ignored by the PSC Control Logic when in Unavailable state as a result of a (local or remote) Lockout of protection. If in Unavailable state due to a SF on protection, then the FS SHALL cause the LER to go into local Protecting administrative state and begin transmitting a FS(1,1) message. It should be noted that due to the unavailability of the protection path (i.e., due to the SF condition) that this FS may not be received by the far-end until the SF condition is cleared.

*A local Signal Fail on the protection path input when in local Unavailable state [by implication this is due to a local SF on protection] SHALL cause the LER to remain in local Unavailable state and transmit a SF(0,0) message.

*A local Signal Fail on the working path input when in remote Unavailable state SHALL cause the LER to remain in remote Unavailable state and transmit a SF(1,0) message.

*All other local inputs SHALL be ignored.

If remote messages are being received over the protection path then they would have the following affect:

*A remote Lockout of protection message SHALL cause the LER to remain in Unavailable state, (note that if the LER was previously in local Unavailable state due to a Signal Fail on the protection path, then it will now be in remote Unavailable state) and continue transmission of the current message (either NR(0,0) or LO(0,0) or SF(0,0))

*A remote Forced switch message SHALL be ignored by the PSC Control Logic when in Unavailable state as a result of a (local or remote) Lockout of protection. If in Unavailable state due to a SF on protection, then the FS SHALL cause the LER to go into remote Protecting administrative state and begin transmitting a SF(0,1) message.

*A remote Signal Fail message that indicates that the failure is on the protection path SHALL cause the LER to remain in Unavailable state and continue transmission of the current message (either NR(0,0) or SF(0,0) or LO(0,0)).

*A remote No Request, when the LER is in remote Unavailable state and there is no active local Signal Fail SHALL cause the LER to go into Normal state and continue transmission of the current message. If there is a local Signal Fail on the protection path, the LER SHALL remain in local Unavailable state and transmit a SF(0,0) message. If there is a local Signal Fail on the working path, the LER SHALL go into local Protecting Failure state and transmit a SF(1,1) message. When in local Unavailable state, the remote message SHALL be ignored.

*All other remote messages SHALL be ignored.

4.3.3.3. Protecting administrative state

In the protecting state the user data traffic SHALL be transported on the protection path, while the working path is blocked due to an operator command, i.e. Forced Switch or Manual Switch. The difference

between a local FS and local MS affects what local indicators may be received - the Local request logic will block any local SF when under the influence of a local FS, whereas the SF would override a local MS. In general, a MS will be canceled in case of either a local or remote SF or LO condition.
The following describe the reaction to local input:

*A local Clear SHALL be ignored if in remote Protecting administrative state. If in local Protecting administrative state then this input SHALL cause the LER to go into Normal state.

*A local Lockout of protection input SHALL cause the LER to go into local Unavailable state and begin transmission of a LO(0,0) message.

*A local Forced switch input SHALL cause the LER to remain in local Protecting administrative state and transmit a FS(1,1) message.

*A local Signal Fail indication on the protection path SHALL cause the LER to go into local Unavailable state and begin transmission of a SF(0,0) message, if the current state is due to a (local or remote) Manual switch operator command. If the LER is in (local or remote) Protecting administrative state due to a FS situation, then the SF on protection SHALL be ignored.

*A local Signal Fail indication on the working path SHALL cause the LER to go into local Protecting failure state and begin transmitting a SF(1,1) message, if the current state is due to a (local or remote) Manual switch operator command. If the LER is in remote Protecting administrative state due to a remote Forced Switch command, then this local indication SHALL cause the LER to remain in remote Protecting administrative state and transmit a SF(1,1) message. If the LER is in local Protecting administrative state due to a local Forced Switch command then this indication SHALL be ignored (i.e. the indication should have been blocked by the Local request logic).

*A local Clear SF SHALL clear any local SF condition that may exist. If in remote Protecting administrative state, the LER SHALL stop transmitting the SF(x,1) message and begin transmitting an NR(0,1) message.

*A local Manual switch input SHALL be ignored if in remote Protecting administrative state is due to a remote Forced switch command. If the current state is due to a (local or remote) Manual switch operator command, it SHALL cause the LER to remain in local Protecting administrative state and transmit a MS(1,1) message.

*All other local inputs SHALL be ignored.

While in Protecting administrative state the LER may receive and react as follows to remote PSC messages:

*A remote Lockout of protection message SHALL cause the LER to go into remote Unavailable state and begin transmitting a NR(0,0) message. It should be noted that this automatically cancels the current Forced switch or Manual switch command and data traffic is reverted to the working path.

*A remote Forced switch message SHALL be ignored by the PSC Process Logic if there is an active local Forced switch operator command. If the Protecting administrative state is due to a remote Forced switch message then the LER SHALL remain in remote Protecting administrative state and continue transmitting the last message. If the Protecting administrative state is due to either a local or remote Manual switch then the LER SHALL remain in remote Protecting administrative state (updating the state information with the proper relevant information) and begin transmitting a NR(0,1) message.

*A remote Signal Fail message indicating a failure on the protection path SHALL cause the LER to go into remote Unavailable state and begin transmitting a NR(0,0) message, if the Protecting administrative state is due to a Manual switch command. It should be noted that this automatically cancels the current Manual switch command and data traffic is reverted to the working path.

*A remote Signal Fail message indicating a failure on the working path SHALL be ignored if there is an active local Forced switch command. If the Protecting state is due to a local or remote Manual switch then the LER SHALL go to remote Protecting failure state and begin transmitting a NR(0,1) message.

*A remote Manual switch message SHALL be ignored by the PSC Control Logic if in Protecting administrative state due to a local or remote Forced switch. If in Protecting administrative state due to a remote Manual switch then the LER SHALL remain in remote Protecting administrative state and continue transmitting the current message. If in local Protecting administrative state due to an active Manual switch then the LER SHALL remain in local Protecting administrative state and continue transmission of the MS(1,1) message.

*A remote DNR(0,1) message SHALL be ignored if in local Protecting administrative state. If in remote Protecting administrative state then the LER SHALL go to Do-not-revert state and continue transmitting the current message.

*A remote NR(0,0) message SHALL be ignored if in local Protecting administrative state. If in remote Protecting administrative state and there is no active local Signal Fail indication then the LER SHALL go to Normal state and begin transmitting a NR(0,0) message. If there is a local Signal Fail on the working path, the LER SHALL go to local Protecting failure state and begin transmitting a SF(1,1) message.

*All other remote messages SHALL be ignored.

4.3.3.4. Protecting failure state

When the protection mechanism has been triggered and the protection domain has performed a protection switch, the domain is in the protecting failure state. In this state the normal data traffic SHALL be transported on the protection path. When an LER is in this state it implies that there was either a local SF condition or received a remote SF PSC message. The SF condition or message indicated that the failure is on the working path.
This state may be overridden by the Unavailable state triggers, i.e. Lockout of Protection or SF on the protection path, or by issuing a FS operator command. This state will be cleared when the SF condition is cleared. In order to prevent flapping due to an intermittent fault, the LER SHOULD employ a Wait-to-restore timer to delay return to Normal state until the network has stabilized (see section 3.5)
The following describe the reaction to local input:

*A local Clear SF SHALL be ignored if in remote Protecting failure state. If in local Protecting failure state and the LER is configured for revertive behavior then this input SHALL cause the LER to go into Wait-to-restore state, start the WTR timer, and begin transmitting a WTR(0,1) message. If in local Protecting failure state and the LER is configured for non-revertive behavior then this input SHALL cause the LER to go into Do-not-revert state and begin transmitting a DNR(0,1) message.

*A local Lockout of protection input SHALL cause the LER to go into Unavailable state and begin transmission of a LO(0,0) message.

*A local Forced switch input SHALL cause the LER to go into Protecting administrative state and begin transmission of a FS(1,1) message.

*A local Signal Fail indication on the protection path SHALL cause the LER to go into Unavailable state and begin transmission of a SF(0,0) message.

*A local Signal Fail indication on the working path SHALL cause the LER to remain in local Protecting failure state and transmit a SF(1,1) message.

*All other local inputs SHALL be ignored.

While in Protecting failure state the LER may receive and react as follows to remote PSC messages:

*A remote Lockout of protection message SHALL cause the LER to go into remote Unavailable state and if in local Protecting failure state then the LER SHALL transmit a SF(1,0) message, otherwise it SHALL transmit a NR(0,0) message. It should be noted that this may cause loss of user data since the working path is still in a failure condition.

*A remote Forced switch message SHALL cause the LER go into remote Protecting administrative state and if in local Protecting failure state the LER SHALL transmit the SF(1,1) message, otherwise it SHALL transmit NR(0,1).

*A remote Signal Fail message indicating a failure on the protection path SHALL cause the LER to go into remote Unavailable state and if in local Protecting failure state then the LER SHALL transmit a SF(1,0) message, otherwise it SHALL transmitting NR(0,0) message. It should be noted that this may cause loss of user data since the working path is still in a failure condition.

*If in remote Protecting failure state, a remote Wait-to-Restore message SHALL cause the LER to go into remote Wait-to-Restore state and continue transmission of the current message.

*If in remote Protecting failure state, a remote Do-not-revert message SHALL cause the LER to go into remote Do-not-revert state and continue transmission of the current message.

*If in remote Protecting failure state, a remote NR(0,0) SHALL cause the LER to go to Normal state.

*All other remote messages SHALL be ignored.

4.3.3.5. Wait-to-restore state

The Wait-to-Restore state is used by the PSC protocol to delay reverting to the Normal state, when recovering from a failure condition on the working path, for the period of the WTR timer to allow the recovering failure to stabilize. While in the Wait-to-Restore state the data traffic SHALL continue to be transported on the protection path. The natural transition from the Wait-to-Restore state to Normal state will occur when the WTR timer expires.

When in Wait-to-Restore state the following describe the reaction to local inputs:

- A local Lockout of protection command SHALL cause the LER to Stop the WTR timer, go into local Unavailable state, and begin transmitting a LO(0,0) message.

- A local Forced switch command SHALL cause the LER to Stop the WTR timer, go into local Protecting administrative state, and begin transmission of a FS(1,1) message.

- A local Signal Fail indication on the protection path SHALL cause the LER to Stop the WTR timer, go into local Unavailable state, and begin transmission of a SF(0,0) message.

- A local Signal Fail indication on the working path SHALL cause the LER to Stop the WTR timer, go into local Protecting failure state, and begin transmission of a SF(1,1) message.

- A local Manual switch input SHALL cause the LER to Stop the WTR timer, go into local Protecting administrative state and begin transmission of a MS(1,1) message.

- A local WTR expires input SHALL cause the LER to remain in Wait-to-Restore state and begin transmitting a NR(0,1) message.

- All other local inputs SHALL be ignored.

When in Wait-to-Restore state the following describe the reaction to remote messages:

- A remote Lockout of protection message SHALL cause the LER to Stop the WTR timer, go into remote Unavailable state, and begin transmitting a NR(0,0) message.

- A remote Forced switch message SHALL cause the LER to Stop the WTR timer, go into remote Protecting administrative state, and begin transmission of a NR(0,1) message.

- A remote Signal Fail message for the protection path SHALL cause the LER to Stop the WTR timer, go into remote Unavailable state, and begin transmission of a NR(0,0) message.

- A remote Signal Fail message for the working path SHALL cause the LER to Stop the WTR timer, go into remote Protecting failure state, and begin transmission of a NR(0,1) message.

- A remote Manual switch message SHALL cause the LER to Stop the WTR timer, go into remote Protecting administrative state and begin transmission of a NR(0,1) message.

*If the WTR timer is running then a remote NR message SHALL be ignored. If the WTR timer is stopped then a remote NR message SHALL cause the LER to go into Normal state.

*All other remote messages SHALL be ignored.

4.3.3.6. Do-not-revert state

Do-not-revert state is a continuation of the Protecting failure state. When the protection domain is configured for non-revertive behavior. While in Do-not-revert state, data traffic SHALL continue to be transported on the protection path until the administrator sends a command to revert to the Normal state. It should be noted that there is a fundamental difference between this state and Normal – whereas Forced Switch in Normal state actually causes a switch in the transport path used, in Do-not-revert state the Forced switch just switches the state (to Protecting administrative state) but the traffic would continue to be transported on the protection path! To revert back to Normal state the administrator SHALL issue a Lockout of protection command followed by a Clear command.
When in Do-not-revert state the following describe the reaction to local input:

*A local Lockout of protection command SHALL cause the LER to go into local Unavailable state and begin transmitting a LO(0,0) message.

*A local Forced switch command SHALL cause the LER to go into local Protecting administrative state and begin transmission of a FS(1,1) message.

*A local Signal Fail indication on the protection path SHALL cause the LER to go into local Unavailable state and begin transmission of a SF(0,0) message.

*A local Signal Fail indication on the working path SHALL cause the LER to go into local Protecting failure state and begin transmission of a SF(1,1) message.

*A local Manual switch input SHALL cause the LER to go into local Protecting administrative state and begin transmission of a MS(1,1) message.

*All other local inputs SHALL be ignored.

When in Do-not-revert state the following describe the reaction to remote messages:

*A remote Lockout of protection message SHALL cause the LER to go into remote Unavailable state and begin transmitting a NR(0,0) message.

*A remote Forced switch message SHALL cause the LER to go into remote Protecting administrative state and begin transmission of a NR(0,1) message.

*A remote Signal Fail message for the protection path SHALL cause the LER to go into remote Unavailable state and begin transmission of a NR(0,0) message.

*A remote Signal Fail message for the working path SHALL cause the LER to go into remote Protecting failure state, and begin transmission of a NR(0,1) message.

*A remote Manual switch message SHALL cause the LER to go into remote Protecting administrative state and begin transmission of a NR(0,1) message.

*All other remote messages SHALL be ignored.

5. IANA Considerations

5.1. Pseudowire Associated Channel Type

In the "Pseudowire Name Spaces (PWE3) IANA" maintains the " Pseudowire Associated Channel Types Registry".
IANA is requested to assign a new code point from this registry. The code point shall be assigned form the code point space that requires "IETF Review" as follows:
Registry:

Value	Description	TLV Follows	Reference
0xHH	Protection State	no	[this document]
	Coordination Protocol –		
	Channel Type (PSC-CT)		

5.2. PSC Request Field

The IANA is instructed to create and maintain a new registry within the "Multiprotocol Label Switching Architecture (MPLS)" namespace called "MPLS PSC Request Registry". All code points within this registry shall be allocated according to the "Standards Action" procedures as specified in [RFC5226].

The PSC Request Field is 4 bits and the values shall be allocated as follows:

Value	Description	Reference
0	No Request	[this document]
1	Do not revert	[this document]
2 - 3	Unassigned	
4	Wait to restore	[this document]
5	Manual switch	[this document]
6	Unassigned	
7	Signal Degrade	[this document]
8 - 9	Unassigned	
10	Signal Fail	[this document]
11	Unassigned	
12	Forced switch	[this document]
13	Unassigned	
14	Lockout of protection	[this document]
15	Unassigned	

5.3. Additional TLVs

The IANA is instructed to create and maintain a new registry within the "Multiprotocol Label Switching Architecture (MPLS)" namespace called "MPLS PSC TLV Registry". All code points within this registry shall be allocated according to the "IETF Review" procedures as specified in [RFC5226].

6. Security Considerations

MPLS-TP is a subset of MPLS and so builds upon many of the aspects of the security model of MPLS. MPLS networks make the assumption that it is very hard to inject traffic into a network, and equally hard to cause traffic to be directed outside the network. The control plane protocols utilize hop-by-hop security, and assume a "chain-of-trust" model such that end-to-end control plane security is not used. For more information on the generic aspects of MPLS security, see [RFC5920].
This document describes a protocol carried in the G-ACh [RFC5586], and so is dependent on the security of the G-ACh, itself. The G-ACh is a generalization of the Associated Channel defined in [RFC4385]. Thus, this document relies heavily on the security mechanisms provided for the Associated Channel and described in those two documents.
A specific concern for the G-ACh is that is can be used to provide a covert channel. This problem is wider than the scope of this document and does not need to be addressed here, but it should be noted that the

channel provides end-to-end connectivity and SHOULD NOT be policed by transit nodes. Thus, there is no simple way of preventing any traffic being carried between in the G-ACh consenting nodes.
A good discussion of the data plane security of an associated channel may be found in [RFC5085]. That document also describes some mitigation techniques.
It should be noted that the G-ACh is essentially connection-oriented so injection or modification of control messages specified in this document require the subversion of a transit node. Such subversion is generally considered hard in MPLS networks, and impossible to protect against at the protocol level. Management level techniques are more appropriate.
However, a new concern for this document is the accidental corruption of messages (through faulty implementations, or random corruption). The main concern is around the Request, FPath and Path fields as a change to these fields would change the behavior of the peer end point. Although this document does not define a way to avoid a change in network behavior upon receipt of a message indicating a change in protection status, the transition between states will converge on a known and stable behavior in the face of messages which do not match reality.

7. 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.

8. References

8.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC5654]	Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N. and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.
[RFC5586]	Vigoureux,, M., Bocci, M., Swallow, G., Aggarwal, R. and D. Ward, "MPLS Generic Associated Channel", RFC 5586, May 2009.
[RFC4385]	Bryant, S., Swallow, G., Martini, L. and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, Feb 2006.

8.2. Informative References

[RFC3031]	

	Rosen, E., Viswanathan, A. and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, Jan 2001.
[RFC3032]	Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T. and A. Conta, "MPLS Label Stack Encoding", RFC 3032, Jan 2001.
[RFC5659]	Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, October 2009.
[RFC5920]	Fang, Luyuan, "Security Framework for MPLS and GMPLS Networks", RFC 5920, July 2010.
[RFC3985]	Bryant, S. and P. Pate, "Pseudowire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.
[RFC5085]	Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, December 2007.
[TPFwk]	Bocci, M., Bryant, S., Frost, D., Levrau, L. and L. Berger, "A Framework for MPLS in Transport Networks", RFC 5921, July 2010.
[RFC4427]	Mannie, E. and D. Papadimitriou, "Recovery Terminology for Generalized Multi-Protocol Label Switching", RFC 4427, Mar 2006.
[RFC5226]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
[SurvivFwk]	Sprecher, N., Farrel, A. and H. Shah, "Multi-protocol Label Switching Transport Profile Survivability Framework", ID draft-ietf-mpls-tp-survive-fwk-06.txt, June 2010.
[RFC4872]	Lang, J.P., Papadimitriou, D. and Y. Rekhter, "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, May 2007.
[RFC4873]	Berger, L., Bryskin, I., Papadimitriou, D. and A. Farrel, "GMPLS Segment Recovery", RFC 4873, May 2007.
[RFC3945]	Mannie, E., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, Oct 2004.

Appendix A. PSC state machine tables

The PSC state machine is described in section 4.3.3. This appendix provides the same information but in tabular format. In the event of a mismatch between these tables and the text in section 4.3.3, the text is authoritative. Note that this appendix is intended to be a functional description, not an implementation specification.
For the sake of clarity of the table the six states listed in the text are split into thirteen states. The logic of the split is to differentiate between the different cases given in the conditional

statements in the descriptions of each state in the text. In addition, the remote and local states were split for the Unavailable, Protecting failure, and Protecting administrative states.
There is only one table for the PSC state machine, but it is broken into two parts for space reasons. The first part lists the thirteen possible states, the eight possible local inputs (that is, inputs which are generated by the node in question) and the action taken when a given input is received when the node is in a particular state. The second part of the table lists the thirteen possible states and the eight remote inputs (inputs which come from a node other than the one executing the state machine).
There are thirteen rows in the table, headers notwithstanding. These rows are the thirteen possible extended states in the state machine. The text in the first column is the current state. Those states which have both source and cause are formatted as State:Cause:Source. For example, the string UA:LO:L indicates that the current state is 'Unavailable', that the cause of the current state is a Lockoutof protection that was a Local input. In contrast, the state N simply is Normal; there is no need to track the cause for entry into Normal state.
The thirteen extended states, as they appear in the table, are:

N	Normal state
UA:LO:L	Unavailable state due to local Lockout
UA:P:L	Unavailable state due to local SF on protection path
UA:LO:R	Unavailable state due to remote Lockout message
UA:P:R	Unavailable state due to remote SF message on protection path
PF:W:L	Protecting failure state due to local SF on working path
PF:W:R	Protecting failure state due to remote SF message on working path
PA:F:L	Protecting administrative state due to local FS operator command
PA:M:L	Protecting administrative state due to local MS operator command
PA:F:R	Protecting administrative state due to remote FS message
PA:M:R	Protecting administrative state due to remote MS message
WTR	Wait-to-restore state
DNR	Do-not-revert state

Each state corresponds to the transmission of a particular set of Request, FPath and Path bits. The table below lists the message that is generally sent in each particular state. If the message to be sent in a particular state deviates from the table below, it is noted in the footnotes to the state-machine table.

State	REQ(FP,P)
N	NR(0,0)
UA:LO:L	LO(0,0)
UA:P:L	SF(0,0)
UA:LO:R	NR(0,0)
UA:P:R	NR(0,0)
PF:W:L	SF(1,1)
PF:W:R	NR(0,1)
PA:F:L	FS(1,1)
PA:M:L	MS(1,1)
PA:F:R	NR(0,1)
PA:M:R	NR(0,1)
WTR	WTR(0,1)
DNR	DNR(0,1)

The top row in each table is the list of possible inputs. The local inputs are:

NR	No Request
OC	Operator Clear
LO	Lockout of protection
SF-P	Signal Fail on protection path
SF-W	Signal Fail on working path
FS	Forced Switch
SFc	Clear Signal Fail
MS	Manual Switch
WTRExp	WTR Expired

and the remote inputs are:

LO	remote LO message
SF-P	remote SF message indicating protection path
SF-W	remote SF message indicating working path
FS	remote FS message
MS	remote MS message
WTR	remote WTR message
DNR	remote DNR message
NR	remote NR message

Section 4.3.3 refers to some states as 'remote' and some as 'local'. By definition, all states listed in the table of local sources are local states, and all states listed in the table of remote sources are remote states. For example, section 4.3.3.1 says "A local Lockout of protection input SHALL cause the LER to go into local Unavailable State". As the trigger for this state change is a local one, 'local Unavailable State' is by definition displayed in the table of local sources. Similarly, "A remote Lockout of protection message SHALL cause the LER to go into remote Unavailable state" means that the state represented in the Unavailable rows in the table of remote sources is by definition a remote Unavailable state.
Each cell in the table below contains either a state, a footnote, or the letter 'i'. 'i' stands for Ignore, and is an indication to continue with the current behavior. See section 4.3.3. The footnotes are listed below the table.
Part 1: Local input state machine

	OC	LO	SF-P	FS	SF-W	SFc	MS	WTRExp
N	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i
UA:LO:L	N	i	i	i	i	i	i	i
UA:P:L	i	UA:LO:L	i	PA:F:L	i	[5]	i	i
UA:LO:R	i	UA:LO:L	[1]	i	[2]	[6]	i	i
UA:P:R	i	UA:LO:L	UA:P:L	PA:F:L	[3]	[6]	i	i
PF:W:L	i	UA:LO:L	UA:P:L	PA:F:L	i	[7]	i	i
PF:W:R	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	i	i
PA:F:L	N	UA:LO:L	i	i	i	i	i	i
PA:M:L	N	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	i	i
PA:F:R	i	UA:LO:L	i	PA:F:L	[4]	[8]	i	i
PA:M:R	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i
WTR	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	[9]
DNR	i	UA:LO:L	UA:P:L	PA:F:L	PF:W:L	i	PA:M:L	i

Part 2: Remote messages state machine

	LO	SF-P	FS	SF-W	MS	WTR	DNR	NR
N	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	i
UA:LO:L	i	i	i	i	i	i	i	i
UA:P:L	[10]	i	i	PF:W:R	i	i	i	i
UA:LO:R	i	i	i	i	i	i	i	[16]
UA:P:R	UA:LO:R	i	i	PF:W:R	i	i	i	[16]
PF:W:L	[11]	[12]	PA:F:R	i	i	i	i	i
PF:W:R	UA:LO:R	UA:P:R	PA:F:R	i	i	[14]	[15]	N
PA:F:L	UA:LO:R	i	i	i	i	i	i	i
PA:M:L	UA:LO:R	UA:P:R	PA:F:R	[13]	i	i	i	i
PA:F:R	UA:LO:R	i	i	i	i	i	i	[17]
PA:M:R	UA:LO:R	UA:P:R	PA:F:R	[13]	i	i	i	N
WTR	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	[18]
DNR	UA:LO:R	UA:P:R	PA:F:R	PF:W:R	PA:M:R	i	i	i

The following are the footnotes for the table:
[1] Remain in the current state (UA:LO:R) and transmit SF(0,0)
[2] Remain in the current state (UA:LO:R) and transmit SF(1,0)
[3] Remain in the current state (UA:P:R) and transmit SF(1,0)
[4] Remain in the current state (PA:F:R) and transmit SF(1,1)
[5] If the SF being cleared is SF-P, Transition to N. If it's SF-W, ignore the clear.
[6] Remain in current state (UA:x:R), if the SFc corresponds to a previous SF then begin transmitting NR(0,0).
[7] If domain configured for revertive behavior transition to WTR, else transition to DNR
[8] Remain in PA:F:R and transmit NR(0,1)
[9] Remain in WTR, send NR(0,1)
[10] Transition to UA:LO:R continue sending SF(0,0)
[11] Transition to UA:LO:R and send SF(1,0)
[12] Transition to UA and send SF(1,0)
[13] Transition to PF:W:R and send NR(0,1)
[14] Transition to WTR state and continue to send the current message.
[15] Transition to DNR state and continue to send the current message.
[16] If the local input is SF-P then transition to UA:P:L. If the local input is SF-W then transition to PF:W:L. Else - transition to N state and continue to send the current message.
[17] If the local input is SF-W then transition to PF:W:L. Else - transition to N state and continue to send the current message.
[18] If the receiving LER's WTR timer is running, maintain current state and message. If the WTR timer is stopped, transition to N.

Appendix B. Exercising the protection domain

There is a requirement in [RFC5654] (number 84) that discusses a requirement to verify that the protection path is viable. While the PSC protocol does not define a specific operation for this functionality,

it is possible to perform this operation by combining operations of the PSC and other OAM functionalities. One such possible combination would be to issue a Lockout of Protection operation and then use the OAM function for diagnostic testing of the protection path. Similarly, to test the paths when the working path is not active would involve performing a Forced Switch to protection and then perform the diagnostic function on either the working or protection path.

Authors' Addresses

Stewart Bryant Bryant Cisco United Kingdom EMail: stbryant@cisco.com

Eric Osborne Osborne Cisco United States EMail: eosborne@cisco.com

Nurit Sprecher Sprecher Nokia Siemens Networks 3 Hanagar St. Neve Ne'eman B Hod Hasharon, 45241 Israel EMail: nurit.sprecher@nsn.com

Annamaria Fulignoli editor Fulignoli Ericsson Italy EMail: annamaria.fulignoli@ericsson.com

Yaacov Weingarten editor Weingarten Nokia Siemens Networks 3 Hanagar St. Neve Ne'eman B Hod Hasharon, 45241 Israel EMail: yaacov.weingarten@nsn.com