Network survivability is the network’s ability to restore traffic following failure or attack; it plays a critical factor in the delivery of reliable services in transport networks. Guaranteed services in the form of Service Level Agreements (SLAs) require a resilient network that detects facility or node failures, very rapidly, and immediately starts to restore network operations in accordance with the terms of the SLA.

The Transport Profile of Multiprotocol Label Switching (MPLS-TP) is a packet transport technology that combines the packet experience of MPLS with the operational experience of SONET/SDH. It provides survivability mechanisms such as protection and restoration, with similar function levels to those found in established transport networks such as in SONET/SDH networks. Some of the MPLS-TP protection mechanisms are data plane-driven and are based on MPLS-TP OAM fault management functions which are used to trigger protection
switching in the absence of a control plane. Other protection mechanisms utilize the MPLS-TP control plane.

This document provides a framework for MPLS-TP survivability.

Table of Contents

1. Introduction                                     3
2. Terminology and References                       6
3. Requirements for Survivability                   6
4. Functional Architecture                          8
  4.1. Elements of Control                            8
    4.1.1. Manual Control                               8
    4.1.2. Failure-Triggered Actions                    9
    4.1.3. OAM Signaling                                9
    4.1.4.                                              9
  4.2. Elements of Recovery                           9
    4.2.1. Span Recovery                                10
    4.2.2. Segment Recovery                             10
    4.2.3.                                              10
  4.3. Levels of Recovery                              11
    4.3.1. Dedicated Protection                         11
    4.3.2. Shared Protection                            11
    4.3.3. Extra Traffic                                12
    4.3.4. Restoration and Repair                       12
    4.3.5.                                              13
  4.4. Mechanisms for Recovery                        13
    4.4.1. Link-Level Protection                        13
    4.4.2. Alternate Paths and Segments                 13
    4.4.3.                                              13
  4.5. Protection in Different Topologies             13
    4.5.1. Mesh Networks                                13
    4.5.2. Ring Networks                                15
    4.5.3.                                              15
  4.6. Recovery in Layered Networks                   15
    4.6.1. Inherited Link-Level Protection              16
    4.6.2. Shared Risk Groups                           16
    4.6.3. Fault Correlation                            16
  5. Mechanisms for Providing Protection in MPLS-TP   16
    5.1. Management Plane                              16
    5.1.1. Configuration of Protection Operation        17
    5.1.2. Forced Protection Actions                    17
    5.1.3. Blocked Protection Actions                   17
    5.2. Fault Detection                                17
    5.3. Fault Isolation                                18
    5.4. OAM Signaling                                  18
    5.4.1. Fault Detection                              18
    5.4.2. Fault Isolation                              18
    5.4.3. Fault Reporting                              18
    5.4.4. Coordination of Recovery Actions             18
    5.5. Control Plane Signaling                        18
    5.5.1. Fault Detection                              18
    5.5.2. Fault Isolation                              18
    5.5.3. Fault Reporting                              18
    5.5.4. Coordination of Recovery Actions             18
6. Pseudowire Protection Considerations

6.1. Utilizing Underlying MPLS-TP Protection

6.2. Protection in the Pseudowire Layer

7. Manageability Considerations

8. Security Considerations

9. IANA Considerations

10. Acknowledgments

11. References

11.1. Normative References

11.2. Informative References

12. Editors’ Addresses

13. Intellectual Property Statement

1. Introduction

Network survivability is the network’s ability to restore traffic following failure or attack; it plays a critical factor in the delivery of reliable services in transport networks. Guaranteed services in the form of Service Level Agreements (SLAs) require a resilient network that very rapidly detects facility or node failures, and immediately starts to restore network operations in accordance with the terms of the SLA.

The Transport Profile of Multiprotocol Label Switching (MPLS-TP) [MPLS-TP-JWT], [MPLS-TP-REQ] is a packet transport technology that combines the packet experience of MPLS with the operational experience of SONET/SDH. MPLS-TP is designed to be consistent with existing transport network operations and management models and provide survivability mechanisms, such as protection and restoration with similar function levels to those found in established transport networks such as the SONET/SDH networks which provided service providers with a high benchmark for reliability.

This document provides a framework for MPLS-TP-based survivability. It uses the recovery terminology defined in [RFC4427] which draws heavily on [G.808.1], and refers to the requirements specified in [MPLS-TP-REQ].

Various recovery schemes (for protection and restoration) and processes have been defined and analyzed in [RFC4427] and [RFC4428]. These schemes may also be applied in MPLS-TP networks to re-establish end-to-end traffic delivery within the agreed service level and so recover from ‘failed’ or ‘degraded’ transport entities (links or nodes). Such actions are normally initiated by the detection of a defect or performance degradation, or by an external request (e.g., an operator request for manual control of protection switching).

[RFC4427] makes a distinction between protection switching and restoration mechanisms. Protection switching makes use of pre-assigned capacity between nodes, where the simplest scheme has
one dedicated protection entity for each working entity, while the
most complex scheme has m protection entities shared between n
working entities (m:n). Protection switching may be either
unidirectional or bidirectional. Restoration uses any capacity
available between nodes and usually involves re-routing. The
resources used for restoration may be pre-planned and recovery
priority may be used as a differentiation mechanism to determine
which services are recovered and which are not recovered or are
sacrificed in order to achieve recovery of other services. In
general, protection actions are completed within time frames of tens
of milliseconds, while restoration actions are normally completed in
periods ranging from hundreds of milliseconds to a maximum of a few
seconds.

However, the recovery schemes described in [RFC4427] and evaluated in
[RFC4428] assume some control plane-driven actions that are performed
in the recovery context. As for other transport technologies and
associated transport networks, the presence of a distributed control
plane in support of MPLS-TP network operations is optional, and the
absence of such a control plane does not affect the ability to
operate the network and to use MPLS-TP forwarding, OAM, and
protection capabilities.

Thus, some of the MPLS-TP recovery mechanisms do not depend on a
control plane and rely on MPLS-TP OAM capabilities to trigger
protection switching. These mechanisms are data plane-driven and are
based on MPLS-TP OAM fault management functions. "Fault management"
in this context refers to failure detection, localization, and
notification (where the term "failure" is used to represent both
signal failure and signal degradation).

The principles of MPLS-TP protection switching operation are similar
to those defined in [RFC4427], as the protection mechanism is based
on the ability to detect certain defects in the transport entities
within the protected domain. The protection switching controller does
not care which monitoring method is used, as long as it can be given
information about the status of the transport entities within the
recovery domain (e.g., ‘OK’, signal failure, signal degradation,
etc.).

An MPLS-TP OAM Automatic Protection Switching (APS) protocol may be
used as an in-band (i.e., data plane-based) control protocol to align
both ends of the protected domain.

The MPLS-TP protection mechanisms may be applied at various levels
throughout the MPLS-TP network, as is the case with the recovery
schemes defined in [RFC4427] and [RFC4873]. A Label Switching Path
(LSP) may be subject to span, segment, and/or end-to-end recovery,
where:
- span protection refers to the protection of an individual link (and hence all or a subset of the LSPs routed over the link) between two neighboring switches;

- segment protection refers to the recovery of an LSP segment (i.e., tandem connection in the language of [MPLS-TP-REQ]) between two nodes which are the boundary nodes of the segment; and

- end-to-end protection refers to the protection of an entire LSP from the ingress to the egress node.

Multiple recovery levels may be used concurrently by a single LSP for added resiliency.

It is a basic requirement of MPLS-TP that both directions of a bidirectional LSP should be co-routed (that is, share the same route within the network) and be fate-sharing (that is, if one direction fails, both directions should cease to operate) [MPLS-TP-REQ]. This causes a direct interaction between the protection levels affecting the directions of an LSP such that both directions of the LSP are switched to a new span, segment, or end-to-end path together.

The protection scheme operating at the data plane level can function in a multi-domain environment; it should also protect against a failure of a boundary node in the case of inter-domain operation.

The MPLS-TP recovery schemes apply to LSPs and PWE3. This document focuses on LSPs and handles both point-to-point (P2P) and point-to-multipoint (P2MP) LSPs.

This framework introduces the architecture of the MPLS-TP recovery domain and describes the recovery schemes in MPLS-TP (based on the recovery types defined in [RFC4427]) as well as the principles of operation, recovery states, recovery triggers, and information exchanges between the different elements that sustain the reference model. The reference model is based on the MPLS-TP OAM reference model which is defined in [MPLS-TP-OAM].

This framework also refers to recovery schemes that are optimized for specific topologies, such as linear, ring, and mesh, in order to handle protection switching in a cost-efficient manner.

This document takes into account the timing co-ordination of protection switches at multiple layers. This prevents races and allows the protection switching mechanism of the server layer to fix a problem before switching at the MPLS-TP layer.

This framework also specifies the functions that must be supported by MPLS-TP OAM (e.g., APS) and the management and/or the control plane in order to support the recovery mechanisms.
MPLS-TP introduces a tool kit to enable recovery in MPLS-TP-based transport networks and to ensure that affected traffic is restored in the event of a failure.

Different recovery levels may be used concurrently by a single LSP for added resiliency.

Generally, network operators aim to provide the fastest, most stable, and the best protection mechanism available at a reasonable cost. The higher the levels of protection, the greater the number of resources consumed. It is therefore expected that network operators will offer a wide spectrum of service levels. MPLS-TP-based recovery offers the flexibility to select the recovery mechanism, choose the granularity at which traffic is protected, and also choose the specific types of traffic that are to be protected. With MPLS-TP-based recovery, it is possible to provide different levels of protection for different classes of service, based on their service requirements.

2. Terminology and References

The terminology used in this document is consistent with that defined in [RFC4427]. That RFC is, itself, consistent with [G.808.1].

However, certain protection concepts (such as ring protection) are not discussed in [RFC4427], and for those concepts, terminology in this document is drawn from [G.841].

Readers should refer to those documents for normative definitions. This document supplies brief summaries of some terms for clarity and to aid the reader, but does not re-define terms.

In particular, note the distinction and definitions made in [RFC4427] for the following three terms.

- Protection: re-establishing end-to-end traffic using pre-allocated resources.
- Restoration: re-establishing end-to-end traffic using resources allocated at the time of need. Sometimes referred to as "repair".
- Recovery: a generic term covering both Protection and Restoration.

Important background information can be found in [RFC3386], [RFC3469], [RFC4426], [RFC4427], and [RFC4428].

3. Requirements for Survivability

MPLS-TP requirements are presented in [MPLS-TP-REQ]. Survivability is presented as a critical factor in the delivery of reliable services, and the requirements for survivability are set out using the recovery terminology defined in [RFC4427].
These requirements are summarized below. This section may be updated if changes are made to [MPLS-TP-REQ], and that document should be regarded as normative for the definition of all MPLS-TP requirements including those for survivability.

General:
- Must support tandem network connection protection.
- Must support LSP protection.
- Must support pseudowire protection.
- Must provide appropriate recovery times.
- Must scale when many services are affected by a single fault.
- Should support span protection.
- Should support tandem connection protection.
- Should support end-to-end protection.
- Must support management plane control.
- Must support control plane control.

Restoration:
- May support pre-planning of restoration resources.
- May support computation of restoration resources after failure.
- May support shared mesh restoration.
- Should support soft LSP restoration (Make-before-break).
- May support hard LSP restoration (break-before-make).
- Must be topology agnostic.
- May support restoration priority.
- May utilize preemption during restoration, but only under operator configuration.

Protection:
- Should be able to apply protection at different levels in the network.
- Should operate in conjunction with protection in under-lying networks.
- Must support data plane triggered recovery.
- Should be equally applicable to LSPs and pseudowires.
- Must include mechanisms to detect, locate, notify, and remedy network faults.
- May support 1:1 bidirectional protection switching in which case protection switching must be synchronized.
- May support 1+1 unidirectional protection switching.
- Must be applicable to P2P LSPs
- Should be applicable to P2MP LSPs.
- Must support protection ration of 100%.
- Must support operator’s QoS objectives on protection path.
- May support extra traffic in 1:1 protection modes.
- Must provide operator control and protection prioritization.
- Must support revertive and non-revertive behavior.
- Must provide mechanisms to prevent protection switching thrashing.
- Must provide coordination between protection mechanisms at different layers.
- May provide different mechanisms optimized for specific topologies.

4. Functional Architecture

This section presents an overview of the elements of the functional architecture for survivability within an MPLS-TP network. The intention is to break the components out as separate items so that it can be seen how they may be combined to provide different levels of recovery to meet the requirements set out in the previous section.

4.1. Elements of Control

Survivability is achieved through specific actions taken to repair network resources or to redirect traffic onto paths that avoid failures in the network. Those actions may be triggered automatically by the network devices, may be enhanced by data plane (i.e., OAM) control plane signaling, and may be under direct the control of an operator.

These different options are explored in the next sections.

4.1.1. Manual Control

Of course, the survivability behavior of the network as a whole, and the reaction of each LSP when a fault is reported, may be under operator control. That is, the operator may establish network-wide or local policies that determine what actions will be taken when different failures are reported that affect different LSPs. At the same time, when a service request is made to cause the establishment of one or more LSPs in the network, the operator (or requesting application) may express a required or desired level of service, and this will be mapped to particular survivability actions taken before and during LSP setup, after the failure of network resources, and upon recovery of those resources.

The operator can also be given manual control of survivability actions and events. For example, the operator may force a switchover from a working path to a recovery path (for network optimization purposes with minimal disturbance of services, like when modifying protected or unprotected services, when replacing network elements, etc.), inhibit survivability actions, enable or disable survivability function, or induce the simulation of a network fault.
4.1.2. Failure-Triggered Actions

Survivability actions may be directly triggered by network failures. That is, the device that detects the failure (for example, Loss of Light on an optical interface) may immediately perform a survivability action. Note that the term "failure" is used to represent both signal failure and signal degradation.

This behavior can be subject to management plane or control plane control, but does not require any messages exchanges in any of the management plane, control plane, or data plane to trigger the recovery action - it is directly triggered by data plane stimuli. Note, however, that coordination of recovery actions may require message exchanges.

4.1.3. OAM Signaling

OAM signaling refers to message exchanges in-band or closely coupled to the data channel. Such messages may be used to detect and isolate faults, but in this context we are concerned with the use of these messages to control or trigger survivability actions.

Note that in some cases, it may be the failure to receive an OAM signaling message that causes the survivability action to be taken.

OAM signaling may also be used to coordinate recovery actions within the network.

4.1.4. Control Plane Signaling

The control plane signaling is responsible for setup and teardown of LSPs that are not under management plane control. The control plane can also be used to detect, isolate, and communicate network failures pertaining to peer relationships (neighbor-to-neighbor, or end-to-end). Thus, control plane signaling can initiate and coordinate survivability actions.

The control plane can also be used to distribute topology and resource-availability information. In this way, "graceful shutdown" of resources may be effected by withdrawing them, and this can be used as a stimulus to survivability action in a similar way to the reporting or discovery of a fault as described in the previous sections.

4.2. Elements of Recovery

This section describes the elements of recovery. These are the quantitative aspects of recovery; that is the pieces of the network for which recovery can be provided.
4.2.1. Span Recovery

A span is a single hop between neighboring nodes in the same network layer. A span is sometimes referred to as a link although this may cause some confusion between the concept of a data link and a traffic engineering (TE) link. LSPs traverse TE links between neighboring label switching routers (LSRs) in the MPLS-TP network, however, a TE link may be provided by:

- a single data link
- a series of data links in a lower layer established as an LSP and presented to the upper layer as a single TE link
- a set of parallel data links in the same layer presented either as a bundle of TE links or a collection of data links that, together, provide data link layer protection scheme.

Thus, span recovery may be provided by:

- moving the TE link to be supported by a different data link between the same pair of neighbors
- re-routing the LSP in the lower layer.

Moving the protected LSP to another TE link between the same pair of neighbors is known as segment recovery and is described in Section 4.2.2.

4.2.2. Segment Recovery

An LSP segment is one or more hops on the path of the LSP. (Note that recovery of pseudowire segments is discussed in Section 6).

Segment recovery involves redirecting traffic from one end of a segment of an LSP on an alternate path to the other end of the segment. This redirection may be on a pre-established LSP segment, through re-routing of the protected segment, or by tunneling the protected LSP on a "bypass" LSP.

Note that protecting an LSP against the failure of a node requires the use of segment recovery, while a link could be protected using span or segment recovery.

4.2.3. End-to-End Recovery

End-to-end recovery is a special case of segment recovery where the protected LSP segment is the whole of the LSP. End-to-end recovery may be provided as link-diverse or node-diverse recovery where the recovery path shares no links or no nodes with the recovery path. Note that node-diverse paths are necessarily link-diverse, and that full, end-to-end node-diversity is required to guarantee recovery.
4.3. Levels of Recovery

This section describes the qualitative levels of survivability function that can be provided. The level of recovery offered has a direct effect on the service level provided to the end-user in the event of a network fault. This will be observed as the amount of data lost when a network fault occurs, and the length of time to recovery connectivity.

In general there is a correlation between the service level (i.e., the rapidity of recovery and reduction of data loss) and the cost to the network; better service levels require pre-allocation of resources to the recovery paths, and those resources cannot be used for other purposes if high quality recovery is required.

Sections 6 and 7 of [RFC4427] provide a full break down of protection and recovery schemes. This section summarizes the qualitative levels available.

4.3.1. Dedicated Protection

In dedicated protection, the resources for the recovery LSP are pre-assigned for use only by the protected service. This will clearly be the case in 1+1 protection, and may also be the case in 1:1 protection where extra traffic (see Section 4.3.3) is not supported.

Note that in the bypass tunnel recovery mechanism (see Section 4.4.3) resources may also be dedicated to protecting a specific service. In some cases (one-for-one protection) the whole of the bypass tunnel may be dedicated to provide recovery for a specific LSP, but in other cases (such as facility backup) a subset of the resources of the bypass tunnel may be pre-assigned for use to recover a specific service. However, as described in Section 4.4.3, the bypass tunnel approach can also be used for shared protection (Section 4.3.2), to carry extra traffic (Section 4.3.3), or without reserving resources to achieve best-effort recovery.

4.3.2. Shared Protection

In shared protection, the resources for the recovery LSPs of several services are shared. These may be shared as 1:n or m:n, and may be shared on individual links, on LSP segments, or on end-to-end LSPs.

Where a bypass tunnel is used (Section 4.4.3) the tunnel might not have sufficient resources to simultaneously protect all of the LSPs to which it offers protection so that if they were all affected by network failures at the same time, they would not all be recovered.

Shared protection is a trade-off between expensive network resources being dedicated to protection that is not required most of the time,
and the risk of unrecoverable services in the event of multiple network failures. There is also a trade-off between rapid recovery (that can be achieved with dedicated protection, but which is delayed by message exchanges in the management, control, or data planes for shared protection) and the reduction of network cost by sharing protection resources. These trade-offs may be somewhat mitigated by using m:n for some value of m <> 1, and by establishing new protection paths as each available protection path is put into use.

4.3.3. Extra Traffic

A way to utilize network resources that would otherwise be idle awaiting use to protect services, is to use them to carry other traffic. Obviously, this is not practical in dedicated protection (Section 4.3.1), but is practical in shared protection (Section 4.3.2) and bypass tunnel protection (Section 4.4.3).

When a network resource that is carrying extra traffic is required for protection, the extra traffic is disrupted - essentially it is pre-empted by the recovery LSP. This may require some additional messages exchanges in the management, control, or data planes, with the consequence that recovery may be delayed somewhat. This provides an obvious trade-off against the cost reduction (or rather, revenue increase) achieved by carrying extra traffic.

4.3.4. Restoration and Repair

If resources are not pre-assigned for use by the recovery LSP, the recovery LSP must be established "on demand" when the network failure is detected and reported, or upon instruction from the management plane.

Restoration represents the most cost-effective use of network resources as no resources are tied up for specific protection usage. However, restoration requires computation of a new path and activation of a new LSP (through the management or control plane). These steps can take much more time than is required for recovery using protection techniques.

Furthermore, there is no guarantee that restoration will be able to recover the service. It may be that all suitable network resources are already in use for other LSPs so that no new path can be found. This problem can be partially mitigated by the use of LSP setup priorities so that recovery LSPs can pre-empt other low priority LSPs.

Additionally, when a network failure occurs, multiple LSPs may be disrupted by the same event. These LSPs may have been established by different Network Management Stations (NMSs) or signaled by different head-end LSRs, and this means that multiple points in the network
will be trying to compute and establish recovery LSPs at the same
time. This can lead to contention within the network meaning that
some recovery LSPs must be retried resulting in very slow recovery
times for some services.

4.3.5. Reversion

When a service has been recovered so that traffic is flowing on the
recovery LSP, the faulted network resource may be repaired. The
choice must be made about whether to redirect the traffic back on to
the original working LSP, or to leave it where it is on the recovery
LSP. These behaviors are known as "revertive" and "non-revertive",
respectively.

In "revertive" mode, care should be taken to prevent frequent
operation of the recovery operation due to an intermittent defect.
Therefore, when the failure condition of a recovery element has been
handled, a fixed period of time should elapse before normal data
traffic is redirected back onto the original working entity.

4.4. Mechanisms for Recovery

The purpose of this section is to describe in general (MPLS-TP
non-specific) terms the mechanisms that can be used to provide
protection.

4.4.1. Link-Level Protection

4.4.2. Alternate Paths and Segments

4.4.3. Bypass Tunnels

4.5. Protection in Different Topologies

As described in the requirements listed in Section 3 and detailed in
[MPLS-TP-REQ], the recovery techniques used may be optimized for
different network topologies. This section describes two different
topologies and explains how recovery may be markedly different in
those different scenarios. It also introduces the concept of a
recovery domain and shows how end-to-end survivability may be
achieved through a concatenation of recovery domains each providing
some level of recovery in part of the network.

4.5.1. Mesh Networks

Linear protection provides a fast and simple protection switching
mechanism and it fits best in mesh networks. It can protect against a
failure that may happen on an entity (element of recovery that may
constitute a span, LSP segment, PW segment, end-to-end LSP or end-to-
end PW).
In order to guarantee the protection, two entities are pre-provisioned. One of the pre-provisioned entities is configured to be the ‘working’ entity (primary) and the other is configured as the ‘protection’ entity (backup).

The Protection switching occurs at the protection controllers which reside at the edges of the protected entity. Between these endpoints, there are working and protection entities.

In linear protection, a protection entity is pre-provisioned to protect the working entity. In order to guarantee protection switching in case of a ‘failed’ condition, the physical routes of the working and the protection entities should have complete physical diversity.

[MPLS-TP-REQ] requires that both 1:1 linear protection scheme and 1+1 protection schemes are supported. The 1:1 protection switching, bi-directional protection switching should be supported. In 1+1 linear protection switching unidirectional protection switching should be supported.

1:1 linear protection:

- In normal conditions the data traffic is transmitted either over the working entity or the ‘protection’ entity. Normal conditions are defined when there is no failure on the ‘working’ entity and there is no administrative configuration or requests that cause traffic to transmit over the ‘protection’ entity. Upon a failure condition or a specific administrative request, the traffic is switched over to the ‘protection’ entity.

- In each transmission direction, the source of the protection domain bridges the traffic into the appropriate entity and the sink of the protected domain selects the traffic from the appropriate entity. The source and the sink need to be coordinated to ensure that the bridging and the selection are done to and from the same entity. For that sake a signaling coordination protocol is needed.

- In bi-directional protection switching, both ends of the protection domain should switch to the ‘protection’ entity (even when the failure is unidirectional).

- When there is no failure, the resources of the ‘idle’ entity may be used for less priority traffic, extra traffic. When protection switching is performed, the extra traffic is required for protection, the extra traffic is pre-empted by the protected traffic.
1+1 linear protection:

- The data traffic is copied at fed to both the ‘working’ and the ‘protection’ entities. The traffic on the ‘working’ and the ‘protection’ entities is transmitted simultaneously to the sink of the protected domain, where a selection between the ‘working’ and ‘protection’ entities is made (based on some predetermined criteria). Since only uni-directional protection switching is supported in the 1+1 linear protection scheme, there is no need to coordinate between the protection controllers.

4.5.2. Ring Networks

4.5.3. Protection and Restoration Domains

Protection and restoration are performed in the context of a recovery domain. A recovery domain is defined between two recovery reference points which are located at the edges of the recovery domain and are responsible for performing recovery for a ‘working’ entity (which may be one of the elements of recovery defined above) when an appropriate trigger is received. These reference points function as recovery controllers.

As described in section 4.2 above, the recovery element may constitute a spam, a tandem connection (i.e. either an LSP segment or a PW segment), an end-to-end LSP, or an end-to-end PW.

The method used to monitor the health of the recovery element is unimportant, provided that the recovery controllers receive information on its condition. The condition of the recovery element may be OK, ‘failed’, or degraded.

When the recovery operation is launched by an OAM trigger, the recovery domain is equivalent to the OAM maintenance entity which is defined in [MPLS-TP-OAM], and the recovery reference points are defined at the same location as the OAM MEPs.

4.6. Recovery in Layered Networks

In multi-layer or multi-region networking, recovery may be performed at multiple layers or across cascaded recovery domains.

The MPLS-TP recovery mechanism must ensure that the timing of recovery is co-ordinated in order to avoid races, and to allow either the recovery mechanism of the server layer to fix the problem before recovery takes place at the MPLS-TP layer, or to allow an upstream recovery domain to perform recovery before a downstream domain. In inter-connected rings, for example, it may be preferable to allow the upstream ring to perform recovery before the downstream ring, in order to ensure that recovery takes place in the ring in which the
failure occurred.

A hold-off timer is required to coordinate the timing of recovery at multiple layers or across cascaded recovery domains. Setting this configurable timer involves a trade-off between rapid recovery and the creation of a race condition where multiple layers respond to the same fault, potentially allocating resources in an inefficient manner. Thus, the detection of a failure condition in the MPLS-TP layer should not immediately trigger the recovery process if the hold-off timer is set to a value other than zero. The hold-off timer should be started and, on expiry, the recovery element should be checked to determine whether the failure condition still exists. If it does exist, the defect triggers the recovery operation.

In other configurations, where the lower layer does not have a restoration capability, or where it is not expected to provide protection, the lower layer needs to trigger the higher layer to immediately perform recovery.

[RFC3386]

4.6.1. Inherited Link-Level Protection

4.6.2. Shared Risk Groups

4.6.3. Fault Correlation

5. Mechanisms for Providing Protection in MPLS-TP

This section describes the existing mechanisms available to provide protection within MPLS-TP networks and highlights areas where new work is required. It is expected that, as new protocol extensions and techniques are developed, this section will be updated to convert the statements of required work into references to those protocol extensions and techniques.

5.1. Management Plane

As described above, a fundamental requirement of MPLS-TP is that recovery mechanisms should be capable of functioning in the absence of a control plane. Recovery may be triggered by MPLS-TP OAM fault management functions or by external requests (e.g. an operator request for manual control of protection switching).

The management plane may be used to configure the recovery domain by setting the reference points (recovery controllers), the ‘working’ and ‘protection’ entities, and the recovery type (e.g. 1:1 bi-directional linear protection, ring protection, etc.). Additional parameters associated with the recovery process (such as a hold-off timer, revertive/non-revertive operation, etc.) may also be
In addition, the management plane may initiate manual control of the protection switching function. Either the fault condition or the operator request should be prioritized.

Since provisioning the recovery domain involves the selection of a number of options, mismatches may occur at the different reference points. The MPLS-TP OAM Automatic Protection Switching (APS) protocol may be used as an in-band (i.e., data plane-based) control protocol to align both ends of the protected domain.

It should also be possible for the management plane to monitor the recovery status.

5.1.1. Configuration of Protection Operation

In order to implement the protection switching mechanism, the following entities and information should be provisioned:

- The protection controllers (reference points)

- The protection group consisting of a ‘working’ entity (which may be one of the recovery elements defined above) and a ‘protection’ entity. To guarantee protection, the paths of the ‘working’ and the ‘protection’ entities should have complete physical diversity.

- The protection type that should be applied

- Revertive/non-revertive behavior

5.1.2. External manual commands

The following external, manual commands may be applied to a protection group; they are listed in descending order of priority:

- Blocked protection action - a manual command to prevent data traffic from switching to the ‘protection’ entity. This command actually disables the protection group.

- Force protection action - a manual command that forces a switch of normal data traffic to the ‘protection’ entity.

- Manual protection action - a manual command that forces a switch of data traffic to the ‘protection’ entity when there is no failure in the ‘working’ or the ‘protection’ entity

5.2. Fault Detection

5.3. Fault Isolation
6. Pseudowire Protection Considerations

The main application for the MPLS-TP network is currently identified as the pseudowire. Pseudowires provide end-to-end connectivity over the MPLS-TP network and may be comprised of a single pseudowire segment, or multiple segments "stitched" together to provide end-to-end connectivity.

The pseudowire service may, itself, require a level of protection as part of its SLA. This protection could be provided by the MPLS-TP LSPs that support the pseudowire, or could be a feature of the pseudowire layer itself.

6.1. Utilizing Underlying MPLS-TP Protection

6.2. Protection in the Pseudowire Layer

7. Manageability Considerations

8. Security Considerations

9. IANA Considerations

This informational document makes no requests for IANA action.

10. Acknowledgments
11. References

11.1. Normative References


11.2. Informative References


12. Editors’ Addresses

Nurit Sprecher  
Nokia Siemens Networks  
3 Hanagar St. Neve Ne’eman B  
45241 Hod Hasharon, Israel  
Tel. +972 9 7751229  
Email: nurit.sprecher@nsn.com

Adrian Farrel  
Old Dog Consulting  
Email: adrian@olddog.co.uk

Vach Kompella  
Alcatel-Lucent  
701 East Middlefield Rd.  
Mountain View, CA 94043  
Email: vach.kompella@alcatel.com

13. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY