Internet Draft
Category: Informational
Expiration Date: December 18, 2010

Loa Andersson, Ed. (Ericsson)
Lou Berger, Ed. (LabN)
Luyuan Fang, Ed. (Cisco)
Nabil Bitar, Ed. (Verizon)

June 18, 2010

MPLS-TP Control Plane Framework

draft-ietf-ccamp-mpls-tp-cp-framework-02.txt

Abstract

The MPLS Transport Profile (MPLS-TP) supports static provisioning of transport paths via a Network Management System (NMS), and dynamic provisioning of transport paths via a control plane. This document provides the framework for MPLS-TP dynamic provisioning, and covers control plane addressing, routing, path computation, signaling, traffic engineering,, and path recovery. MPLS-TP uses GMPLS as the control plane for MPLS-TP~~ LSPs and provides for compatibility with MPLS~~. MPLS-TP may also use~~s~~ the control plane for Pseudowires (PWs). Management plane functions such as manual configuration and the initiation of LSP setup are out of scope of this document.

Status of this Memo

Comment [M1]: Editorial: Add the boiler plate text on joint development

Comment [M2]: Editorial: Add a note to the RFC editor that this Informational RFC has been approved by the IETF consensus process.

Comment [M3]: Path computation is normally out of scope for standards

Comment [M4]: Data plane or control plane?

Comment [M5]: RFC5654 says "The control plane for MPLS-TP MUST fit within the ASON architecture", however, ASON CP and GMPLS don't include the control for PW and the protocols identified for the PW control plane do not comply with the ASON architecture.

Comment [M6]: Current text implies that a control plane is always used for PWs.

Copyright and License Notice

Table of Contents

1. Introduction

The MPLS Transport Profile (MPLS-TP) is being defined in a joint effort between the International Telecommunications Union (ITU) and the IETF. The requirements for MPLS-TP are defined in the requirements document, see [RFC5654]. These requirements state that "A solution MUST be provided to support dynamic provisioning of MPLS-TP transport paths via a control plane." This document provides the framework for such dynamic provisioning.

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 Pseudowire Emulation Edge-to-Edge (PWE3) architectures to support the capabilities and functions of a packet transport network as defined by the ITU-T.

Comment [M7]: Add this text to the Abstract section as per comment M1.

1.1. 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].

1.2. Scope

This document covers the control plane functions involved in establishing MPLS-TP Label Switched Paths (LSPs) and Pseudowires (PWs). The control plane requirements for MPLS-TP are defined in the MPLS-TP requirements document [RFC5654]. These requirements define the role of the control plane in MPLS-TP. In particular, Sections 2.4 and portions of the remainder of Section 2 of [RFC5654] provide specific control plane requirements.

The LSPs provided by MPLS-TP are used as a server layer for IP, MPLS and PWs, as well as other tunneled MPLS-TP LSPs. The PWs are used to carry client signals other than IP or MPLS. The relationship between PWs and MPLS-TP LSPs is exactly the same as between PWs and MPLS LSPs in a Packet switched network (PSN). The PW encapsulation over MPLS-TP LSPs used in MPLS-TP networks is also the same as for PWs over MPLS in an MPLS network. MPLS-TP also defines protection and restoration (or, collectively, recovery) functions. The MPLS-TP control plane provides methods to establish, remove and control MPLS-TP LSPs and PWs. This includes control of data plane, OAM and recovery functions.

A general framework for MPLS-TP has been defined in [TP-FWK], and a survivability framework for MPLS-TP has been defined in [TP-SURVIVE]. These document scope the approaches ~~and protocols~~ that will be used as the foundation for MPLS-TP. Notably, Section 3.5 of [TP-FWK] scopes the IETF protocols that serve as the foundation of the MPLS-TP control plane. The PW control plane is based on the existing PW control plane, see [RFC4447], and the PW end-to-end (PWE3) architecture, see [RFC3985]. The LSP control plane is based on Generalized MPLS (GMPLS), see [RFC3945], which is built on MPLS Traffic Engineering (TE) and its numerous extensions. [TP-SURVIVE] focuses on LSPs, and the ~~protection~~ recovery functions that must be supported within MPLS-TP. It does not specify which control plane mechanisms are to be used.

The remainder of this document discusses the impact of MPLS-TP requirements on the control of PWs as specified in [RFC4447], [SEGMENTED-PW] and [MS-PW-DYNAMIC]. This document also discusses the impact of the MPLS-TP requirements on the GMPLS signaling and routing protocols that are used to control MPLS-TP LSPs.

1.3. Basic Approach

The basic approach taken in defining the MPLS-TP Control Plane framework is:

Comment [M8]: This draft identifies the protocols for the control plane

Comment [M9]: RFC5654 says "The control plane for MPLS-TP MUST fit within the ASON architecture", however, ASON CP and GMPLS don't include the control for PW and the protocols identified for the PW control plane do not comply with the ASON architecture.

Comment [M10]: RFC5654 says "The control plane for MPLS-TP MUST fit within the ASON architecture", however, ASON CP and GMPLS don't include the control for PW and the protocols identified for the PW control plane do not comply with the ASON architecture.

Comment [M11]: PW recovery is for further study

Comment [M12]: TP-SURVIVE describes both protection and restoration

1) MPLS technology as defined by the IETF is the foundation for the MPLS Transport Profile.
2) The data plane for MPLS and MPLS-TP is identical, i.e. any extensions defined for MPLS-TP is also applicable to MPLS. Additionally, the same encapsulation used for MPLS over any layer 2 network is also used for MPLS-TP.
3) MPLS PWs are used as-is by MPLS-TP including the use of targeted-LDP as the foundation for PW signaling [RFC4447], OSPF-TE, ISIS-TE or MP-BGP as they apply for Multi-Segment(MS)-PW routing. However, the PW can be encapsulated over an MPLS-TP LSP (established using methods and procedures for MPLS-TP LSP establishment) in addition to the presently defined methods of carrying PWs over LSP based packet switched networks (PSNs). That is, the MPLS-TP domain is a packet switched network from a PWE3 architecture aspect [RFC3985].
4) The MPLS-TP LSP control plane builds on the GMPLS control plane as defined by the IETF for ~~transport~~ LSPs. The protocols within scope are RSVP-TE [RFC3473], OSPF-TE [RFC4203][RFC5392], and ISIS-TE [RFC5307][RFC5316]. ASON~~/ASTN~~ signaling and routing requirements in the context of GMPLS can be found in [RFC4139] and [RFC4258].
5) Existing IETF MPLS and GMPLS RFCs and evolving Working Group Internet-Drafts should be reused wherever possible.
6) If needed, extensions for the MPLS-TP control plane should first be based on the existing and evolving IETF work, secondly based on work by other Standard bodies only when IETF decides that the work is out of the IETF's scope. New extensions may be defined otherwise.
7) Extensions to the GMPLS control plane may be required in order to fully automate MPLS-TP functions.
8) Control-plane software upgrades to existing (G)MPLS enabled equipment is acceptable and expected.
9) It is permissible for functions present in the GMPLS control plane to not be used in MPLS-TP networks, e.g. the possibility to merge LSPs.
10) One possible use of the control plane is to configure, enable and empower OAM functionality. This will require extensions to existing control plane specifications which will be usable in MPLS-TP as well as MPLS networks.
11) MPLS-TP control plane requirements are primarily defined in Section 2.4 and relevant portions of the remainder Section 2 of [RFC5654].

Comment [M13]: Not exactly identical. See section 3.2 of [TP-FWK]

Comment [M14]: A server layer must support traffic engineering.

Comment [M15]: How is traffic engineering supported as per [RFC5654, requirement 5]

Comment [M16]: Draft-ietf-pwe3-ldp-aii-reachability extends LDP for the MS-PW routing. So, LDP should also be added here.

Comment [M17]: The currently defined control plane is for "general purpose" LSPs the MPLS-TP control plane is for transport applications.

Comment [M18]: ASTN is in old term that is no longer user

Comment [M19]: The requirements state: The MPLS-TP control plane design should as far as reasonably possible reuse existing MPLS standards

Comment [M20]: Is the IETF precluded from adopting work already completed in other standards bodies?

Comment [M21]: The current GMPLS control plane does not include PWs.

Comment [M22]: A GMPLS control plane does not support merging

Comment [M23]: The control plane requirements are provided in Section 2 of this RFC.

1.4. Reference Model

The control plane reference model is based on the general MPLS-TP reference model as defined in the MPLS-TP framework [TP-FWK]. Per the MPLS-TP framework [TP-FWK], the MPLS-TP control plane is based on GMPLS with RSVP-TE for LSP signaling and targeted LDP for PW signaling. In both cases, OSPF-TE or ISIS-TE with GMPLS extensions is used for dynamic routing within an MPLS-TP domain.

From a service perspective, client interfaces are provided for both the PWs and LSPs. PW client interfaces are defined on an interface technology basis, e.g., Ethernet over PW [RFC4448]. In the context of MPLS-TP LSP, the client interface is expected to be provided via a GMPLS based UNI, see [RFC4208], or statically provisioned. As discussed in [TP-FWK], MPLS-TP also presumes an LSP NNI reference point.

Comment [M24]: MPLS-TP LSPs do not cross the UNI as defined in the MPLS-TP Framework

The MPLS-TP end-to-end control plane reference model is shown in Figure 1. The Figure shows the control plane protocols used by MPLS-TP, as well as the UNI and NNI reference points.

```
   |< ---- client signal (IP / MPLS / L2 / PW) ------------ >|
     |< --------- SP1 ----------- >|< ------- SP2 ------- >|
       |< ---------- MPLS-TP End-to-End PW ------------ >|
         |< -------- MPLS-TP End-to-End LSP --------- >|

+---+   +---+  +---+  +---+  +---+   +---+  +---+  +---+   +---+
|CE1|-|-|PE1|--|P1 |--|P2 |--|PE2|-|-|PEa|--|Pa |--|PEb|-|-|CE2|
+---+   +---+  +---+  +---+  +---+   +---+  +---+  +---+   +---+
     UNI                         NNI                     UNI

TE-RTG    |< ---------------- >|< --- >|< ---------- >|
RSVP-TE

   T-LDP    |< --------------------------------------- >|
```

Figure 1. End-to-End MPLS-TP Control Plane Reference Model

Comment [M25]: Can the PW be between CEs, if so the T-LDP session should extend to the CEs

Comment [M26]: This figure is correct however it is inconsistent with the UNI and NNI as defined in the recently published MPLS-TP framework. Is it intended to publish a Bis for the overall framework to correct this inconsistency?

Comment [M27]: Where are the RSVP-TE sessions?

Comment [M28]: T-LDP for PW label assignment

Legend:

CE:	Customer Edge
Client signal:	defined in MPLS-TP Requirements
L2:	Any layer 2 signal that may be carried over a PW, e.g. Ethernet.
NNI:	Network to Network Interface
PE:	Provider Edge
SP:	Service Provider
TE-RTG:	OSPF-TE or ISIS-TE
UNI:	User to Network Interface

Figure 2 adds three hierarchical LSP segments, labeled as "H-LSPs". These segments are present to support scaling, OAM and MEPs within each provider domain and across the inter-provider NNI. The MEPs are used to collect performance information, support ~~diagnostic~~fault management functions, and support OAM triggered survivability schemes as discussed in [TP-SURVIVE]. Each H-LSP may be protected using any of the schemes discussed in [TP-SURVIVE]. End-to-end monitoring is supported via MEPs at the End-to-End LSP and PW end points. Note that segment MEPs ~~are~~ may be collocated with MIPs of the next higher-layer (e.g., end-to-end) LSPs.

Comment [M29]: Use of hierarchical LSP as SPME for OAM alters data plane processing of particular LSP(s) to which the H-LSP been applied. Such effect should be described.

Comment [M30]: TP-SURVIVE describes both protection and restoration. Restoration has the most impact on the control plane.

Comment [M31]: instantiation of the MIPs is optional.

```
       |< ------- client signal (IP / MPLS / L2 / PW) ------ >|
         |< -------- SP1 ----------- >|< ------- SP2 ----- >|
           |< ----------- MPLS-TP End-to-End PW -------- >|
             |< ------- MPLS-TP End-to-End LSP ------- >|
             |< -- H-LSP1 ---- >|<-H-LSP2->|<- H-LSP3 ->|

   +---+   +---+  +---+  +---+  +---+   +---+  +---+  +---+   +---+
   |CE1|-|-|PE1|--|P1 |--|P2 |--|PE2|-|-|PEa|--|Pa |--|PEb|-|-|CE2|
   +---+   +---+  +---+  +---+  +---+   +---+  +---+  +---+   +---+
        UNI                        NNI                   UNI

           .....                .....   .....          .....
   End2end |MEP|----------------|MIP|---|MIP|----------|MEP|
   OAM     '''''                '''''   '''''          '''''
           ..... ..... ..... ......... ......... ..... .....
   Segment |MEP|-|MIP|-|MIP|-|MEP|MEP|-|MEP|MEP|-|MIP|-|MEP|
   OAM     ''''' ''''' ''''' ''''''''' ''''''''' ''''' '''''

   Seg.TE-RTG|< -- >|< -- >|< -- >||< -- >||< -- >|< -- >|
   RSVP-TE   (within the MPLS-TP domain)

   E2E TE-RTG|< ---------------- >|< ---- >|< --------- >|
   RSVP-TE

      LDP    |< --------------------------------------- >|
```

Figure 2. MPLS-TP Control Plane Reference Model with OAM

Comment [M32]: Comments on Figure 1 also apply to figure 2.

Legend:

CE:	Customer Edge
Client signal:	defined in MPLS-TP Requirements
E2E:	End-to-end
L2:	Any layer 2 signal that may be carried over a PW, e.g. Ethernet.
H-LSP:	Hierarchical LSP
MEP:	Maintenance end point
MIP:	Maintenance intermediate point
NNI:	Network to Network Interface
PE:	Provider Edge
SP:	Service Provider
TE-RTG:	OSPF-TE or ISIS-TE

While not shown in the Figures above, ~~it is worth noting that~~ the MPLS-TP control plane must support the addressing separation and independence between the data, control and management planes as shown in Figure 3 of [TP-FWK]. Address separation between the planes is already included in GMPLS.

Comment [M33]: Editorial

Comment [M34]: Address separation must added to LDP if this is used for PWs

2. Control Plane Requirements

The requirements for the MPLS-TP control plane are derived from the MPLS-TP requirements and framework documents, specifically [RFC5654], [TP-FWK], [RFC5860], [TP-OAM], and [TP-SURVIVE]. The requirements are summarized in this section, but do not replace those documents. If there are differences between this section and those documents, those documents shall be considered authoritative.

2.1. Primary Requirements

These requirements are based on Section 2 [RFC5654]:

1. Any new functionality that is defined to fulfill the requirements for MPLS-TP must be agreed within the IETF through the IETF consensus process as per [RFC4929] [RFC5654, Section 1, Paragraph 15].

2. The MPLS-TP control plane design should as far as reasonably possible reuse existing MPLS standards [RFC5654, requirement 2].

3. The MPLS-TP control plane must be able to interoperate with existing IETF MPLS and PWE3 control planes where appropriate [RFC5654, requirement 3].

4. The MPLS-TP control plane must be sufficiently well-defined to ensure the interworking between equipment supplied by multiple vendors will be possible both within a single domain and between domains [RFC5654, requirement 4].

5. The MPLS-TP control plane must support a connection-oriented packet switching model with traffic engineering capabilities that allow deterministic control of the use of network resources [RFC5654, requirement 5].

6. The MPLS-TP control plane must support traffic-engineered point-to-point (P2P) and point-to-multipoint (P2MP) transport paths [RFC5654, requirement 6].

7. The MPLS-TP control plane must support unidirectional, associated bidirectional and co-routed bidirectional point-to-point transport paths [RFC5654, requirement 7].

8. The MPLS-TP control plane must support unidirectional point-to-multipoint transport paths [RFC5654, requirement 8].

9. All nodes (i.e., ingress, egress and intermediate) must be aware about the pairing relationship of the forward and the backward directions belonging to the same co-routed bidirectional transport path [RFC5654, requirement 10].

Comment [M35]: Reword to make the control plane implications clear e.g. The control plane must make all nodes….

10. Edge nodes (i.e., ingress and egress) must be aware of the pairing relationship of the forward and the backward directions belonging to the same associated bidirectional transport path [RFC5654, requirement 11].

11. Transit nodes should be aware of the pairing relationship of the forward and the backward directions belonging to the same associated bidirectional transport path [RFC5654, requirement 12].

12. The MPLS-TP control plane must support bidirectional transport paths with symmetric bandwidth requirements, i.e. the amount of reserved bandwidth is the same in the forward and backward directions [RFC5654, requirement 13].

13. The MPLS-TP control plane must support bidirectional transport paths with asymmetric bandwidth requirements, i.e. the amount of reserved bandwidth differs in the forward and backward directions [RFC5654, requirement 14].

14. The MPLS-TP control plane must support the logical separation of the control and management planes from the data plane [RFC5654, requirement 15]. Note that this implies that the addresses used in the management, control and data planes are independent.

15. The MPLS-TP control plane must support the physical separation of the control and management planes from the data plane, and no assumptions should be made about the state of the data-plane channels from information about the control or management-plane channels when they are running out-of-band [RFC5654, requirement 16].

16. A control plane must be defined to support dynamic provisioning and restoration of MPLS-TP transport paths, but its use is a network operator's choice [RFC5654, requirement 18].

17. A control plane must not be required to support the static provisioning of MPLS-TP transport paths. [RFC5654, requirement 19].

18. The MPLS-TP control plane must permit the coexistence of statically and dynamically provisioned/managed MPLS-TP transport paths within the same layer network or domain [RFC5654, requirement 20].

19. The MPLS-TP control plane should be operable in a way that is similar to the way the control plane operates in other transport-layer technologies [RFC5654, requirement 21].

Comment [M36]: Reword to make the control plane implications clear

Comment [M37]: Reword to make the control plane implications clear

Comment [M38]: Independence of the management plane is outside the scope of this draft. Reword to make the control plane implications clear

Comment [M39]: Independence of the management plane is outside the scope of this draft. Reword to make the control plane implications clear

Comment [M40]: Independence of the management plane is outside the scope of this draft. Reword to make the control plane implications clear

20. The MPLS-TP control plane must avoid or minimize traffic impact (e.g. packet delay, reordering and loss) during network reconfiguration [RFC5654, requirement 24].

21. The MPLS-TP control plane must work across multiple homogeneous domains [RFC5654, requirement 25].

22. The MPLS-TP control plane should work across multiple non-homogeneous domains [RFC5654, requirement 26].

23. The MPLS-TP control plane must not dictate any particular physical or logical topology [RFC5654, requirement 27].

24. The MPLS-TP control plane must include support of ring topologies which may be deployed with arbitrarily interconnection, support rings of at least 16 nodes [RFC5654, requirement 27.A. and 27.B.].

25. The MPLS-TP control plane must scale gracefully to support a large number of transport paths, nodes and links. That is it must be able to scale at least as well as control planes in existing transport technologies with growing and increasingly complex network topologies as well as with increasing bandwidth demands, number of customers, and number of services [RFC 5654, requirements 53 and 28].

26. The MPLS-TP control plane should not provision transport paths which contain forwarding loops [RFC5654, requirement 29].

27. The MPLS-TP control plane must support multiple client layers. (e.g. MPLS-TP, IP, MPLS, Ethernet, ATM, FR, etc.) [RFC5654, requirement 30].

28. The MPLS-TP control plane must provide a generic and extensible solution to support the transport of MPLS-TP transport paths over one or more server layer networks (such as MPLS-TP, Ethernet, SONET/SDH, OTN, etc.). Requirements for bandwidth management within a server layer network are outside the scope of this document [RFC5654, requirement 31].

29. In an environment where an MPLS-TP layer network is supporting a client layer network, and the MPLS-TP layer network is supported by a server layer network then the control plane operation of the MPLS-TP layer network must be possible without any dependencies on the server or client layer network [RFC5654, requirement 32].

30. The MPLS-TP control plane must allow for the transport of a client MPLS or MPLS-TP layer network over a server MPLS or MPLS-TP layer network [RFC5654, requirement 33].

31. The MPLS-TP control plane must allow the autonomous operation of the layers of a multi-layer network that includes an MPLS-TP layer ~~autonomously~~ [RFC5654, requirement 34].

32. The MPLS-TP control plane must allow the hiding of MPLS-TP layer network addressing and other information (e.g. topology) from client layer networks. However, it should be possible, at the option of the operator, to leak a limited amount of summarized information (such as SRLGs or reachability) between layers [RFC5654, requirement 35].

33. The MPLS-TP control plane must allow for the identification of a transport path on each link within and at the destination (egress) of the transport network. [RFC5654, requirement 38 and 39].

34. The MPLS-TP control plane must allow for the use of P2MP capable server (sub-)layers as well as P2P server (sub-)layer to support P2MP MPLS-TP transport paths [RFC5654, requirement 40].

35. The MPLS-TP control plane must be extensible in order to accommodate new types of client layer networks and services [RFC5654, requirement 41].

36. The MPLS-TP control plane should support the reserved bandwidth associated with a transport path to be increased without impacting the existing traffic on that transport path provided enough resources are available [RFC5654, requirement 42].

37. The MPLS-TP control plane should support the reserved bandwidth of a transport path to be decreased without impacting the existing traffic on that transport path, provided that the level of existing traffic is smaller than the reserved bandwidth following the decrease [RFC5654, requirement 43].

38. The MPLS-TP control plane must support an unambiguous and reliable means of distinguishing users' (client) packets from MPLS-TP control packets (e.g. control plane, management plane, OAM and protection switching packets) [RFC5654, requirement 46].

Comment [M41]: Is this really a control plane requirement? Clarification is needed.

39. The control plane for MPLS-TP must fit within the ASON architecture. The ITU-T has defined an architecture for Automatically Switched Optical Networks (ASON) in G.8080 [ITU.G8080.2006] and G.8080 Amendment 1 [ITU.G8080.2008]. An interpretation of the ASON signaling and routing requirements in the context of GMPLS can be found in [RFC4139] and [RFC4258] [RFC5654, Section 2.4., Paragraph 2 and 3].

40. The MPLS-TP control plane must support control plane topology and data plane topology independence [RFC5654, requirement 47].

41. A failure of the MPLS-TP control plane must not interfere with the deliver of service or recovery of established transport paths [RFC5654, requirement 47].

42. The MPLS-TP control plane must be able to operate independent of any particular client or server layer control plane [RFC5654, requirement 48].

43. The MPLS-TP control plane should support, but not require, an integrated control plane encompassing MPLS-TP together with its server and client layer networks when these layer networks belong to the same administrative domain [RFC5654, requirement 49].

44. The MPLS-TP control plane must support configuration of protection functions and any associated maintenance (OAM) functions [RFC5654, requirement 50 and 7].

45. The MPLS-TP control plane must support the configuration and modification of OAM maintenance points as well as the activation/deactivation of OAM when the transport path or transport service is established or modified [RFC5654, requirement 51].

46. The MPLS-TP control plane must be capable of restarting and relearning its previous state without impacting forwarding [RFC5654, requirement 54].

47. The MPLS-TP control plane must provide a mechanism for dynamic ownership transfer of the control of MPLS-TP transport paths from the management plane to the control plane and vice versa. The number of reconfigurations required in the data plane must be minimized (preferably no data plane reconfiguration will be required) [RFC5654, requirement 55].

48. The MPLS-TP control plane must support protection and restoration mechanisms, i.e., recovery [RFC5654, requirement 52].

    Note that the MPLS-TP Survivability Framework document, [TP-SURVIVE], provides additional useful information related to recovery.

49. The MPLS-TP control plane mechanisms for protection and restoration should be identical (or as similar as possible) to those already used in existing transport networks to simplify implementation and operations. However, this must not override any other requirement [RFC5654, requirement 56 A].

50. The MPLS-TP control plane mechanisms used for P2P and P2MP recovery should be identical to simplify implementation and operation. However, this must not override any other requirement [RFC5654, requirement 56 B].

51. The MPLS-TP control plane must support recovery mechanisms that are applicable at various levels throughout the network including support for link, transport path, segment, concatenated segment and end-to-end recovery [RFC5654, requirement 57].

52. The MPLS-TP control plane must support recovery paths that meet the SLA protection objectives of the service [RFC5654, requirement 58]. Including:

    a. Guarantee 50ms recovery times from the moment of fault detection in networks with spans less than 1200 km.

    b. Protection of up to 100% of the traffic on the protected path.

    c. Recovery must meet SLA requirements over multiple domains.

53. The MPLS-TP control plane should support per transport path Recovery objectives [RFC5654, requirement 59].

54. The MPLS-TP control plane must support recovery mechanisms that are applicable to any topology [RFC5654, requirement 60].

55. The MPLS-TP control plane must operate in synergy with (including coordination of timing/timer settings) the recovery mechanisms present in any client or server transport networks (for example, Ethernet, SDH, OTN, WDM) to avoid race conditions between the layers [RFC5654, requirement 61].

56. The MPLS-TP control plane must support recovery and reversion mechanisms that prevent frequent operation of recovery in the event of an intermittent defect [RFC5654, requirement 62].

57. The MPLS-TP control plane must support revertive and non-revertive protection behavior [RFC5654, requirement 64].

58. The MPLS-TP control plane must support 1+1 bidirectional protection for P2P transport paths [RFC5654, requirement 65 A].

59. The MPLS-TP control plane must support 1+1 unidirectional protection for P2P transport paths [RFC5654, requirement 65 B].

60. The MPLS-TP control plane must support 1+1 unidirectional protection for P2MP transport paths [RFC5654, requirement 65 C].

61. The MPLS-TP control plane must support the ability to share protection resources amongst a number of transport paths [RFC5654, requirement 66].

62. The MPLS-TP control plane must support 1:n bidirectional protection for P2P transport paths, and this should be the default for 1:n protection [RFC5654, requirement 67 A].

63. The MPLS-TP control plane must support 1:n unidirectional protection for P2MP transport paths [RFC5654, requirement 67 B].

64. The MPLS-TP control plane may support 1:n unidirectional protection for P2P transport paths [RFC5654, requirement 65 C].

65. The MPLS-TP control plane ~~may~~ is not required to support extra-traffic [RFC5654, note after requirement 67].

Comment [M42]: To be consistent with RFC5654 Requirement, i.e., extra traffic is not required in MPLS-TP.

66. The MPLS-TP control plane should support 1:n (including 1:1) shared mesh recovery [RFC5654, requirement 68].

67. The MPLS-TP control plane must support sharing of protection resources such that protection paths that are known not to be required concurrently can share the same resources [RFC5654, requirement 69].

68. The MPLS-TP control plane must support the sharing of resources between a restoration transport path and the transport path being replaced [RFC5654, requirement 70].

69. The MPLS-TP control plane must support restoration priority so that an implementation can determine the order in which transport paths should be restored [RFC5654, requirement 71].

70. The MPLS-TP control plane must support preemption priority in order to allow restoration to displace other transport paths in the event of resource constraints [RFC5654, requirement 72 and 86].

71. The MPLS-TP control plane must support revertive and non-revertive restoration behavior [RFC5654, requirement 73].

72. The MPLS-TP control plane must support recovery being triggered by physical (lower) layer fault indications [RFC5654, requirement 74].

73. The MPLS-TP control plane must support recovery being triggered by OAM [RFC5654, requirement 75].

74. The MPLS-TP control plane must support management plane recovery triggers (e.g., forced switch, etc.) [RFC5654, requirement 76].

75. The MPLS-TP control plane must support the differentiation of administrative recovery actions from recovery actions initiated by other triggers [RFC5654, requirement 77].

76. The MPLS-TP control plane should support control plane restoration triggers (e.g., forced switch, etc.) [RFC5654, requirement 78].

77. The MPLS-TP control plane must support priority logic to negotiate and accommodate coexisting requests (i.e., multiple requests) for protection switching (e.g., administrative requests and requests due to link/node failures) [RFC5654, requirement 79].

78. The MPLS-TP control plane must support the relationships ~~of~~between protection paths and ~~protection-to-~~working paths (~~sometimes~~ known as protection groups) [RFC5654, requirement 80].

79. The MPLS-TP control plane must support pre-calculation of recovery paths [RFC5654, requirement 81].

80. The MPLS-TP control plane must support pre-provisioning of recovery paths [RFC5654, requirement 82].

81. The MPLS-TP control plane must support the external commands defined in [RFC4427]. External controls overruled by higher priority requests (e.g., administrative requests and requests due to link/node failures) or unable to be signaled to the remote end (e.g. because of a protection state coordination fail) must be ignored/dropped [RFC5654, requirement 83].

82. The MPLS-TP control plane must permit the testing and validation of the integrity of the protection/recovery transport path [RFC5654, requirement 84 A].

83. The MPLS-TP control plane must permit the testing and validation of protection/ restoration mechanisms without triggering the actual protection/restoration [RFC5654, requirement 84 B].

84. The MPLS-TP control plane must permit the testing and validation of protection/ restoration mechanisms while the working path is in service [RFC5654, requirement 84 C].

85. The MPLS-TP control plane must permit the testing and validation of protection/ restoration mechanisms while the working path is out of service [RFC5654, requirement 84 D].

86. The MPLS-TP control plane must support the establishment and maintenance of all recovery entities and functions [RFC5654, requirement 89 A].

87. The MPLS-TP control plane must support signaling of recovery administrative control [RFC5654, requirement 89 B].

88. The MPLS-TP control plane must support protection state coordination (PSC). Since control plane network topology is independent from the data plane network topology, the PSC supported by the MPLS-TP control plane may run on resources different than the data plane resources handled within the recovery mechanism (e.g. backup) [RFC5654, requirement 89 C].

89. When present, the MPLS-TP control plane must support recovery mechanisms that are optimized for specific network topologies. These mechanisms must be interoperable with the mechanisms defined for arbitrary topology (mesh) networks to enable protection of end-to-end transport paths [RFC5654, requirement 91].

90. When present, the MPLS-TP control plane must support the control of ring topology specific recovery mechanisms [RFC5654, Section 2.5.6.1].

91. The MPLS-TP control plane must include support for differentiated services and different traffic types with traffic class separation associated with different traffic [RFC5654, requirement 110].

92. The MPLS-TP control plane must support the provisioning of services that provide guaranteed Service Level Specifications (SLS), with support for hard ([RFC3209] style) and relative ([RFC3270] style) end-to-end bandwidth guarantees [RFC5654, requirement 111].

93. The MPLS-TP control plane must support the provisioning of services which are sensitive to jitter and delay [RFC5654, requirement 112].

2.2. MPLS-TP Framework Derived Requirements

The following additional requirements are based on [TP-FWK], [TP-P2MP-FWK] and [TP-DATA]:

94. Per-packet equal cost multi-path (ECMP) load balancing is not applicable to MPLS-TP [TP-DATA-PLANE , section 3.1.1., paragraph 6].

95. Penultimate hop popping (PHP) is disabled on MPLS-TP LSPs by default. The applicability of PHP to both MPLS-TP LSPs and MPLS networks generally providing packet transport services will be clarified in a future version [TP-DATA-PLANE , section 3.1.1., paragraph 7].

96. The MPLS-TP control plane must support both E-LSP and L-LSP MPLS DiffServ modes as specified in [RFC3270] [TP-DATA-PLANE , section 3.3.2., paragraph 12].

97. Both single-segment and multi-segment PWs shall be supported by the MPLS-TP control plane. MPLS-TP shall use the definition of multi-segment PWs as defined by the IETF [TP-FWK, section 3.4.4.].

98. The MPLS-TP control plane must support the control of PWs and their associated labels [TP-FWK, section 3.4.4.].

99. The MPLS-TP control plane must support network layer clients, i.e., clients whose traffic is transported over an MPLS-TP network without the use of PWs [TP-FWK, section 3.4.5.].

    a. The MPLS-TP control plane must support the use of network layer protocol-specific LSPs and labels. [TP-FWK, section 3.4.5.]

    b. The MPLS-TP control plane must support the use of a client service-specific LSPs and labels. [TP-FWK, section 3.4.5.]

100. The MPLS-TP control plane is based on the GMPLS control plane for MPLS-TP LSPs. More specifically, GMPLS RSVP-TE [RFC3473] and related extensions are used for LSP signaling, and GMPLS OSPF-TE [RFC5392] and ISIS-TE [RFC5316] are used for routing [TP-FWK, section 3.9.].

101. The MPLS-TP control plane is based on the MPLS control plane for PWs, and more specifically, Targeted LDP (T-LDP) [RFC4447] is used for PW signaling [TP-FWK, section 3.9., paragraph 5].

Comment [M43]: How does this support traffic engineering as per [RFC5654, requirement 5] and the address separation requirements

102. Requirement intentionally blank.

103. The MPLS-TP control plane must ensure its own survivability and to enable it to recover gracefully from failures and degradations. These include graceful restart and hot redundant configurations [TP-FWK, section 3.9., paragraph 16].

104. The MPLS-TP control plane must support linear, ring and meshed protection schemes [TP-FWK, section 3.12., paragraph 3].

2.3. OAM Framework Derived Requirements

The following additional requirements are based on [RFC5860] and [TP-OAM]:

105. ~~The MPLS-TP control plane must support the capability to enable/disable OAM functions as part of service establishment [RFC5860, section 2.1.6., paragraph 1].~~

106. ~~The MPLS-TP control plane must support the capability to enable/disable OAM functions after service establishment. In such cases, the customer must not perceive service degradation as a result of OAM enabling/disabling [RFC5860, section 2.1.6., paragraph 1 and 2].~~

Comment [M44]: Better describe in 108, 109 and 124

107. ~~The MPLS-TP control plane must allow for the IP/MPLS and PW OAM protocols (e.g., LSP-Ping [RFC4379], MPLS-BFD [RFC5884], VCCV [RFC5085] and VCCV-BFD [RFC5885]) [RFC5860, section 2.1.4., paragraph 2].~~

Comment [M45]: This is not a control plane requirement

108. The MPLS-TP control plane must allow for the ability to support experimental OAM functions. These functions must be disabled by default [RFC5860, section 2.2., paragraph 2].

109. The MPLS-TP control plane must support the choice of which (if any) OAM function(s) to use and to which PW, LSP or Section it applies [RFC5860, section 2.2., paragraph 3].

110. ~~The MPLS-TP control plane must provide a mechanism to support the localization of faults and the notification of appropriate nodes. Such notification should trigger corrective (recovery) actions [RFC5860, section 2.2.1., paragraph 1].~~

Comment [M46]: Not a control plane function

111. ~~The MPLS-TP control plane must allow the service provider to be informed of a fault or defect affecting the service(s) it provides, even if the fault or defect is located outside of his domain [RFC5860, section 2.2.1., paragraph 2].~~

Comment [M47]: Not a control plane function

112. Information exchange between various nodes involved in the MPLS-TP control plane should be reliable ~~such that, for example, defects or faults are properly detected or that state changes are effectively known by the appropriate nodes [RFC5860, section 2.2.1., paragraph 3].~~

Comment [M48]: Should be reliable to support restoration – the function s identified should be independent of the control plane.

113. ~~The MPLS-TP control plane must provide functionality to control an End Point to monitor the liveness, i.e., continuity check (CC), of a PW, LSP or Section [RFC5860, section 2.2.2., paragraph 1].~~

114. ~~The MPLS-TP control plane must provide functionality to control an End Point's ability to determine, whether or not it is connected to specific End Point(s), i.e., connectivity verification (CV), by means of the expected PW, LSP or Section [RFC5860, section 2.2.3., paragraph 1].~~

Comment [M49]: Repeat of 109

115. The MPLS-TP control plane must provide functionality to control diagnostic testing on a PW, LSP or Section [RFC5860, section 2.2.5., paragraph 1].

116. ~~The MPLS-TP control plane must provide functionality to enable an End Point to discover the Intermediate (if any) and End Point(s) along a PW, LSP or Section, and more generally to trace (record) the route of a PW, LSP or Section [RFC5860, section 2.2.4., paragraph 1].~~

Comment [M50]: 116-123 are all OAM functions that may be enabled by the control plane as per requirement 109

117. ~~The MPLS-TP control plane must provide functionality to enable an End Point of a PW, LSP or Section to instruct its associated End Point(s) to lock the PW, LSP or Section. Note that lock corresponds to an administrative status in which it is expected that only test traffic, if any, and OAM (dedicated to the PW, LSP or Section) can be mapped on that PW, LSP or Section [RFC5860, section 2.2.6., paragraph 1].~~

118. ~~The MPLS-TP control plane must provide functionality to enable an Intermediate Point of a PW or LSP to report, to an End Point of that same PW or LSP, a lock condition indirectly affecting that PW or LSP [RFC5860, section 2.2.7., paragraph 1].~~

119. ~~The MPLS-TP control plane must provide functionality to enable an Intermediate Point of a PW or LSP to report, to an End Point of that same PW or LSP, a fault or defect condition affecting that PW or LSP [RFC5860, section 2.2.8., paragraph 1].~~

120. ~~The MPLS-TP control plane must provide functionality to enable an End Point to report, to its associated End Point, a fault or defect condition that it detects on a PW, LSP or Section for which they are the End Points [RFC5860, section 2.2.9., paragraph 1].~~

121. ~~The MPLS-TP control plane must provide functionality to enable the propagation, across an MPLS-TP network, of information pertaining to a client defect or fault condition detected at an End Point of a PW or LSP, if the client layer mechanisms do not provide an alarm notification/propagation mechanism [RFC5860, section 2.2.10., paragraph 1].~~

122. ~~The MPLS-TP control plane must provide functionality to enable the control of quantification of packet loss ratio over a PW, LSP or Section [RFC5860, section 2.2.11., paragraph 1].~~

123. ~~The MPLS-TP control plane must provide functionality to control the quantification and reporting of the one-way, and if appropriate, the two-way, delay of a PW, LSP or Section [RFC5860, section 2.2.12., paragraph 1].~~

124. The MPLS-TP control plane must support the configuration of MEPs and MIPs.

   a. The CC and CV functions operate between MEPs [TP-OAM, section 5.1., paragraph 3].

   b. All OAM packets coming to a MEP source are tunneled via label stacking, and therefore a MEP can only exist at the beginning and end of an LSP (i.e. at an LSP's ingress and egress nodes and never at an LSP's transit node) [TP-OAM, section 3.2., paragraph 10].

   c. The CC and CV functions may serve as a trigger for protection switching, see requirement 45 above.

   d. This implies that LSP hierarchy must be used in cases where OAM is used to trigger recovery when the recover occurs at points other than an LSPs endpoints. [TP-OAM, section 4., paragraph 5].

Note that MEPs and MIPs configured by the control plane must continue to operate in the absence of the control plane (e.g. due a control plane fault or a change in LSP ownership).

125. ~~The MPLS-TP control plane must support the signaling of the MEP identifier used in CC and CV [TP-OAM, section 5.1., paragraph 4].~~

126. ~~The MPLS-TP control plane must support the signaling of the transmission period used in CC and CV [TP-OAM, section 5.1., paragraph 6].~~

Comment [M51]: Part of MEP/MIP configuration

2.4. Security Requirements

There are no specific MPLS-TP control plane security requirements. The existing framework for MPLS and GMPLS security is documented on [MPLS-SEC] and that document applies equally to MPLS-TP.

3. Relationship of PWs and TE LSPs

The data plane relationship between PWs and LSPs is inherited from standard MPLS and is reviewed in the MPLS-TP Framework [TP-FWK]. Likewise, the control plane relationship between PWs and LSPs is inherited from standard MPLS. This relationship is reviewed in this document. The relationship between the PW and LSP control planes in MPLS-TP is the same as the relationship found in the PWE3 Maintenance Reference Model as presented in the PWE3 Architecture, see Figure 6 of [RFC3985]. The PWE3 Architecture [RFC3985] states: "the PWE3 protocol-layering model is intended to minimize the differences between PWs operating over different PSN types." Additionally, PW control (maintenance) takes place separately from LSP tunnel signaling. [RFC3985] does allow for the extension of the (LSP) tunnel control plane to exchange information necessary to support PWs. [RFC4447] and [MS-PW-DYNAMIC] provide such extensions for the use of LDP as the control plane for PWs. This control can provide PW control without providing LSP control.

Comment [M52]: How are SPMEs established for PWs (PW TCM). How is this coordinated with LSP SPMEs.

Comment [M53]: Please clarify the use of the term “tunnel” in this context. The MPLS-TP identifiers draft uses the term tunnel as a logical relationship between node and is used to name LSPs.

In the context of MPLS-TP, LSP tunnel signaling is provided via GMPLS RSVP-TE. While RSVP-TE could be extended to support PW control much as LDP was extended in [RFC4447], such extensions are out of scope of this document. This means that the control of PWs and LSPs will operate largely independently. The main coordination between LSP and PW control will occur within the nodes that terminate PWs, or PW segments. See Section 5.3.2 for an additional discussion on such coordination.

It is worth noting that the control planes for PWs and LSPs may be used independently, and that one may be employed without the other. This translates into the four possible scenarios: (1) no control plane is employed; (2) a control plane is used for both LSPs and PWs; (3) a control plane is used for LSPs, but not PWs; (4) a control plane is used for PWs, but not LSPs.

The PW and LSP control planes, collectively, must satisfy the MPLS-TP control plane requirements reviewed in this document. When client services are provided directly via LSPs, all requirements must be satisfied by the LSP control plane. When client services are provided via PWs, the PW and LSP control planes operate in combination and some functions may be satisfied via the PW control plane while others are provided to PWs by the LSP control plane. For example, to support the recovery functions described in [TP-SURVIVE] this document focuses on the control of the recovery functions at the

LSP layer. PW based recovery is under development at this time and may be used once defined.

4. TE LSPs

If a control plane is used MPLS-TP LSPs are controlled via Generalized MPLS (GMPLS) signaling and routing, see [RFC3945]. The GMPLS control plane is based on the MPLS control plane. GMPLS includes support for MPLS labeled data and transport data planes. GMPLS includes most of the transport centric features required to support MPLS-TP LSPs. This section will first review the MPLS-TP LSP relevant features of GMPLS, then identify how specific requirements can be met using existing GMPLS functions and will conclude with extensions that are anticipated to support MPLS-TP.

4.1. GMPLS Functions and MPLS-TP LSPs

This section reviews how existing GMPLS functions can be applied to MPLS-TP.

4.1.1. In-Band and Out-Of-Band Control ~~and Management~~

GMPLS supports both in-band and out-of-band control. The terms in-band and out-of-band typically refer to the relationship of the management and control planes relative to the data plane. The terms may be used to refer to the management plane independent of the control plane, or to both of them in concert. There are multiple uses of both terms in-band and out-of-band. The terms may relate to a channel, a path or a network. Each of these can be used independently or in combination. Briefly, some typical usage of the terms are as follows:

o In-band
  This term is used to refer to cases where management and/or control plane traffic is sent ~~using or embedded~~ in the same communication channel used to transport the ~~associated~~ user data. IP, MPLS, and Ethernet networks are all examples where control traffic is typically sent in-band with the data traffic.

o Out-of-band, in-fiber
  This term is used to refer to cases where management and/or control plane traffic is sent using a different communication channel from the associated data traffic, and the control/management communication channel resides in the same fiber as the data traffic. Optical transport networks typically operate in an out-of-band in-fiber configuration.

Comment [M54]: The relationship of management plane with respect to the transport plane should be out of scope of this document.

Comment [M55]: Should define how the terms are used in the context of the MPLS-TP control plane.

Comment [M56]: Please clarify this: Is it on the same wavelength or in the same fiber on a different wavelength.

Comment [M57]: Most use an embedded communications channel but the selection of the route for control/management traffic is independent for the “associated data traffic” and hence is, in effect, out-of-band independent topology.

- o Out-of-band, aligned topology
  This term is used to refer to the cases where management and/or control plane traffic is sent using a different communication channel from the associated data traffic, and the control/management communication must follow the same node-to-node path as the data traffic. Such topologies are usually supported using a parallel fiber or other configurations where multiple data channels are available and one is (dynamically) selected as the control channel.

- o Out-of-band, independent topology
  This term is used to refer to the cases where management and/or control plane traffic is sent using a different communication channel from the associated data traffic, and the control/management communication may follow a path that is completely independent of the data traffic. Such configurations do not preclude the use of in-fiber or aligned topology links, but alignment is not required.

In the context of MPLS-TP, requirement 14 (see Section 2 above) can be met using out-of-band in-fiber or aligned topology types of control. Requirement 15 can only be met by using Out-of-band, independent topology. GMPLS routing and signaling can be used to support in-band and all of the out-of-band forms of control, see [RFC3945].

4.1.2. Addressing

MPLS-TP reuses and supports the addressing mechanisms supported by MPLS. MPLS, and consequently, MPLS-TP uses the IPv4 and IPv6 address families to identify MPLS-TP nodes by default for network management and signaling purposes. The control, management and data planes used in an MPLS-TP network may be completely separated or combined at the discretion of an MPLS-TP operator and based on the equipment capabilities of a vendor. The separation of the control and management planes from the data plane allows each plane to be independently addressable. Each plane may use addresses that are not mutually reachable, e.g., it is likely that the data plane will not be able to reach an address from the management or control planes and vice versa. Each plane may also use a different address family. It is even possible to reuse addresses in each plane, but this is not recommended as it may lead to operational confusion.

4.1.3. Routing

Routing support for MPLS-TP LSPs is based on GMPLS routing. GMPLS routing builds on TE routing and has been extended to support multiple switching technologies per [RFC3945] and [RFC4202] as well as multiple levels of packet switching (PSC) within a single network.

Comment [M58]: How is this different from Out-of-band in-fiber

Comment [M59]: If it is in-fiber or aligned topology links are used, please clarify what “alignment is not required” means in this context.

Comment [M60]: Addressing in the context of the MPLS-TP data plane is defined in the MPLS-TP identifiers draft

Comment [M61]: Does “family” mean Format? Please clarify

Comment [M62]: See the identifiers draft.

Comment [M63]: Do you mean “The address space(s) of the control, management and data planes used …..”?

IS-IS extensions for GMPLS are defined in [RFC5307] and [RFC5316], which build on the TE extensions to IS-IS defined in [RFC5305]. OSPF extensions for GMPLS are defined in [RFC4203] and [RFC5392], which build on the TE extensions to OSPF defined in [RFC3630]. The listed RFCs should be viewed as a starting point rather than an comprehensive list as there are other IS-IS and OSPF extensions, as defined in IETF RFCs, that can be used within an MPLS-TP network.

4.1.4. TE LSPs and Constraint-Based Path Computation

Both MPLS and GMPLS allow for traffic engineering and constraint-based path computation. MPLS path computation provides paths for MPLS TE unidirectional P2P and P2MP LSPs. GMPLS path computation adds bidirectional LSPs, explicit recovery path computation as well as support for the other functions discussed in this section.

Both MPLS and GMPLS path computation allow for the restriction of path selection based on the use of Explicit Route Objects (EROs) and other LSP attributes, see [RFC3209] and [RFC3473]. In all cases, no specific algorithm is standardized by the IETF. This is anticipated to continue to be the case for MPLS-TP LSPs.

4.1.4.1. Relation to PCE

Path Computation Element (PCE) Based approaches, see [RFC4655], may be used for path computation of a GMPLS LSP, and consequently an MPLS-TP LSP, across domains and in a single domain. In cases where the architecture is used, the PCE Communication Protocol (PCECP), see [RFC5440], will be used to communicate PCE requests and responses. MPLS-TP specific extensions to PCECP are currently out of scope of the MPLS-TP project and this document.

4.1.5. Signaling

GMPLS signaling is defined in [RFC3471] and [RFC3473], and is based on RSVP-TE [RFC3209]. CR-LDP based GMPLS, [RFC3472] is no longer under active development within the IETF, i.e., is deprecated, and must not be used for MPLS-TP. In general, all RSVP-TE extensions that apply to MPLS may also be used for GMPLS and consequently MPLS-TP. Most notably this includes support for P2MP signaling as defined in [RFC4875].

GMPLS signaling includes a number of MPLS-TP required functions. Notably support for out-of-band control, bidirectional LSPs, and independent control and data plane fault management. There are also numerous other GMPLS and MPLS extensions that can be used to provide specific functions in MPLS-TP networks. Specific references are provided below.

4.1.6. Unnumbered Links

Support for unnumbered links (i.e., links that do not have IP addresses) is permitted in MPLS-TP and its usage is at the discretion of the network operator. Support for unnumbered links is included for routing in [RFC4203] for OSPF and [RFC5307] for IS-IS, and for signaling in [RFC3477].

4.1.7. Link Bundling

Link bundling provides a local construct that can be used to improve scaling of TE routing when multiple data links are shared between node pairs. Link bundling for MPLS and GMPLS networks is defined in [RFC4201]. Link bundling may be used in MPLS-TP networks and its use is at the discretion of the network operator.

Comment [M64]: RFC 4201 defines mechanism by which allocated label is valid across all component links of given Link Bundle. Is this Link Bundle technique as well applicable to MPLS-TP?

4.1.8. Hierarchical LSPs

This section reuses text from [HIERARCHY-BIS].

[RFC3031] describes how MPLS labels may be stacked so that LSPs may be nested with one LSP running through another. This concept of Hierarchical LSPs is formalized in [RFC4206] with a set of protocol mechanisms for the establishment of a hierarchical LSP that can carry one or more other LSPs.

[RFC4206] goes on to explain that a hierarchical LSP may carry other LSPs only according to their switching types. This is a function of the way labels are carried. In a packet switch capable (PSC) network, the hierarchical LSP can carry other PSC LSPs using the MPLS label stack.

Signaling mechanisms defined in [RFC4206] allow a hierarchical LSP to be treated as a single hop in the path of another LSP. This mechanism is known as "non-adjacent signaling."

A Forwarding Adjacency (FA) is defined in [RFC4206] as a data link created from an LSP and advertised in the same instance of the control plane that advertises the TE links from which the LSP is constructed. The LSP itself is called an FA-LSP.

Thus, a hierarchical LSP may form an FA such that it is advertised as a TE link in the same instance of the routing protocol as was used to advertise the TE links that the LSP traverses.

As observed in [RFC4206] the nodes at the ends of an FA would not usually have a routing adjacency.

4.1.9. LSP Recovery

Comment [M65]: Is this consistent with the Survivability framework?

GMPLS defines RSVP-TE extensions in support for end-to-end GMPLS LSPs recovery in [RFC4872], and segment recovery in [RFC4873] . GMPLS segment recovery provides a superset of the function in end-to-end recovery. End-to-end recovery can be viewed as a special case of segment recovery where there is a single recovery domain whose borders coincide with the ingress and egress of the LSP, although specific procedures are defined.

The five defined types of recovery defined in MPLS-TP are:

- 1+1 bidirectional protection for P2P LSPs
- 1+1 unidirectional protection for P2MP LSPs
- 1:n (including 1:1) protection with or without extra traffic
- Rerouting without extra traffic (sometimes known as soft rerouting), including shared mesh restoration
- Full LSP rerouting

Comment [M66]: Not a control plane function

Comment [M67]: Where is this defined?

Recovery for MPLS-TP LSPs is signaled using the mechanism defined in [RFC4872] and [RFC4873]. Note that when MEPs are required for the OAM CC function and the MEPs exists at LSP transit nodes, each MEP is instantiated at a hierarchical LSP end point, and protection is provided end-to-end for the hierarchical LSP. (Protection can be signaled using either [RFC4872] and [RFC4873] defined procedures.) The use of Notify messages to trigger protection switching and recovery is not required in MPLS-TP as this function is expected to be supported via OAM. However, it's use is not precluded.

4.1.10. Control Plane Reference Points (E-NNI, I-NNI, UNI)

The majority of GMPLS control plane related RFCs define the control plane from the context of an internal network-to-network interface (I-NNI). In the MPLS-TP context, some operators may choose to deploy signaled interfaces across user-to-network (UNI) interfaces and across inter-provider, external network-to-network (E-NNI), interfaces. Such support is embodied in [RFC4208] for UNIs and [RFC5787] for routing areas in support of E-NNIs. This work may require extensions in order to meet the specific needs of an MPLS-TP UNI and E-NNI.

4.2. OAM, MEP (Hierarchy) Configuration and Control

Comment [M68]: Should include MIP configuration

MPLS-TP is being defined to support a comprehensive set of MPLS-TP OAM functions. Specific OAM requirements for MPLS-TP are documented in [RFC5860]. In addition to the actual OAM requirements, it is also required that the control plane be able to configure and control OAM entities. This requirement is not yet addressed by the existing RFCs, but such work is now underway, e.g., [CCAMP-OAM-FWK] and [CCAMP-OAM-EXT].

Many OAM functions occur on a per-LSP basis, are typically in-band, and are initiated immediately after LSP establishment. Hence, it is desirable that OAM is setup together with the establishment of the data path (i.e., with the same signaling). This way OAM setup is bound to connection establishment signaling, avoiding two separate management/configuration steps (connection setup followed by OAM configuration) which would increases delay, processing and more importantly may be prune to misconfiguration errors.

It must be noted that although the control plane is used to establish OAM maintenance entities, OAM messaging and functions occur independently from the control plane. That is, in MPLS-TP OAM mechanisms are responsible for monitoring and initiating recovery actions (driving switches between primary and backup paths).

4.2.1. Management Plane Support

There is no MPLS-TP requirement for a standardized management interface to the MPLS-TP control plane. That said, MPLS and GMPLS support a number of standardized management functions. These include the MPLS-TE/GMPLS TE Database Management Information Base (MIB), [TE-MIB]; the MPLS TE MIB, [RFC3812]; the MPLS LSR MIB, [RFC3813]; the GMPLS TE MIB [RFC4802]; and the GMPLS LSR MIB, [RFC4803]. These MIBs may be used in MPLS-TP networks.

4.2.1.1. Recovery Triggers

The GMPLS control plane allows for management plane recovery triggers and directly supports control plane recovery triggers. Support for control plane recovery triggers is defined in [RFC4872] which refers to the triggers as "Recovery Commands". These commands can be used with both end-to-end and segment recovery, but are always controlled on an end-to-end basis. The recovery triggers/commands defined in [RFC4872] are:

a. Lockout of recovery LSP
b. Lockout of normal traffic
c. Forced switch for normal traffic
d. Requested switch for normal traffic
e. Requested switch for recovery LSP

Note that control plane triggers are typically invoked in response to a management plane request at the ingress.

4.2.1.2. Management Plane / Control Plane Ownership Transfer

In networks where both control plane and management plane are provided, LSP provisioning can be bone either by control plane or management plane. As mentioned in the requirements section above, it must be possible to transfer, or handover, management plane created LSP to the control plane domain and vice versa. [RFC5493] defines the specific requirements for an LSP ownership handover procedure. It must be possible for the control plane to notify, in a reliable manner, the management plane about the status/result of either synchronous or asynchronous, with respect to the management plane, operation performed. Moreover it must be possible to monitor, via query or spontaneous notify, the status of the control plane object such as the TE Link status, the available resources, etc. A mechanism must be made available by the control plane to the management plane to log control plane LSP related operation, that is, it must be possible from the NMS to have a clear view of the life, (traffic hit, action performed, signaling etc.) of a given LSP. The LSP handover procedure for MPLS-TP LSPs is supported via [RFC5852].

4.3. GMPLS and MPLS-TP Requirements Table

The following table shows how the MPLS-TP control plane requirements can be met using existing the GMPLS control plane (which builds on top of the MPLS control plane). Areas where additional specifications are required are also identified. The table lists references based on the control plane requirements as identified and numbered above in section 2.

Req #	References
1	Generic requirement met by using Standards Track RFCs
2	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
3	[RFC5145] + Formal Definition (See Section 4.4.1)
4	Generic requirement met by using Standards Track RFCs
5	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
6	[RFC3471], [RFC3473], [RFC4875]
7	[RFC3471], [RFC3473] + Associated bidirectional LSPs (See Section 4.4.2)
8	[RFC4875]
9	[RFC3473]
10	Associated bidirectional LSPs (See Section 4.4.2)
11	Associated bidirectional LSPs (See Section 4.4.2)
12	[RFC3473]
13	[RFC5467] (Currently Experimental, See Section 4.4.3)
14	[RFC3945], [RFC3473], [RFC4202], [RFC4203], [RFC5307]
15	[RFC3945], [RFC3473], [RFC4202], [RFC4203], [RFC5307]
16	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
17	[RFC3945], [RFC4202] + proper vendor implementation
18	[RFC3945], [RFC4202] + proper vendor implementation
19	[RFC3945], [RFC4202]
20	[RFC3473]
21	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307], [RFC5151]

22	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307], [RFC5151]
23	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
24	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
25	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307], [HIERARCHY-BIS]
26	[RFC3473], [RFC4875]
27	[RFC3473], [RFC4875]
28	[RFC3945], [RFC3471], [RFC4202]
29	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
30	[RFC3945], [RFC3471], [RFC4202]
31	[RFC3945], [RFC3471], [RFC4202]
32	[RFC4208], [RFC4974], [RFC5787], [GMPLS-MLN]
33	[RFC3473], [RFC4875]
34	[RFC4875]
35	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
36	[RFC3473], [RFC3209] (Make-before-break)
37	[RFC3473], [RFC3209] (Make-before-break)
38	[RFC3945], [RFC4202], [RFC5718]
39	[RFC4139], [RFC4258], [RFC5787]
40	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
41	[RFC3473], [RFC5063]
42	[RFC3945], [RFC3471], [RFC4202], [RFC4208]
43	[RFC3945], [RFC3471], [RFC4202]
44	[RFC4872], [RFC4873], [CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
45	[HIERARCHY-BIS], [CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
46	[RFC3473], [RFC4203], [RFC5307], [RFC5063]
47	[RFC5493]
48	[RFC4872], [RFC4873]
49	[RFC3945], [RFC3471], [RFC4202]
50	[RFC4872], [RFC4873] + Recovery for P2MP (see Sec. 4.4.4)
51	[RFC4872], [RFC4873]
52	[RFC4872], [RFC4873] + proper vendor implementation
53	[RFC4872], [RFC4873], [GMPLS-PS]
54	[RFC4872], [RFC4873]
55	[RFC3473], [RFC4872], [RFC4873], [GMPLS-PS] Timers are a local implementation matter
56	[RFC4872], [RFC4873, [GMPLS-PS] + implementation of timers
57	[RFC4872], [RFC4873], [GMPLS-PS]
58	[RFC4872], [RFC4873]
59	[RFC4872], [RFC4873]
60	[RFC4872], [RFC4873]
61	[RFC4872], [RFC4873], [HIERARCHY-BIS]
62	[RFC4872], [RFC4873]
63	[RFC4872], [RFC4873] + Recovery for P2MP (see Sec. 4.4.4)
64	[RFC4872], [RFC4873]
65	[RFC4872], [RFC4873]
66	[RFC4872], [RFC4873]
67	[RFC4872], [RFC4873], [HIERARCHY-BIS]
68	[RFC4872], [RFC4873]

69	[RFC3473], [RFC4872], [RFC4873]
70	[RFC3473]
71	[RFC3473], [RFC4872], [GMPLS-PS]
72	[RFC3473], [RFC4872]
73	[RFC4872], [RFC4873], [CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
74	[RFC4426], [RFC4872], [RFC4873]
75	[RFC4426], [RFC4872], [RFC4873]
76	[RFC4426], [RFC4872], [RFC4873]
77	[RFC4426], [RFC4872], [RFC4873]
78	[RFC4426], [RFC4872], [RFC4873]
79	[RFC4426], [RFC4872], [RFC4873] + vendor implementation
80	[RFC4426], [RFC4872], [RFC4873]
81	[RFC4426], [RFC4872], [RFC4873]
82	[RFC4872], [RFC4873] + Testing control (See Sec. 4.4.5)
83	[RFC4872], [RFC4873] + Testing control (See Sec. 4.4.5)
84	[RFC4872], [RFC4873] + Testing control (See Sec. 4.4.5)
85	[RFC4872], [RFC4873] + Testing control (See Sec. 4.4.5)
86	[RFC4872], [RFC4873], [CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
87	[RFC4872], [RFC4873]
88	[RFC4872], [RFC4873]
89	[RFC4872], [RFC4873], [TP-RING]
90	[RFC4872], [RFC4873], [TP-RING]
91	[RFC3270], [RFC3473], [RFC4124] + GMPLS Usage (See 4.4.6)
92	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307]
93	[RFC3945], [RFC3473], [RFC2210], [RFC2211], [RFC2212]
94	Generic requirement on data plane (correct implementation)
95	[RFC3473], [NO-PHP]
96	[RFC3270], [RFC3473], [RFC4124] + GMPLS Usage (See 4.4.6)
97	PW only requirement, see PW Requirements Table (5.2)
98	PW only requirement, see PW Requirements Table (5.2)
99	[RFC3945], [RFC3473], [HIERARCHY-BIS]
100	[RFC3945], [RFC4202], [RFC3473], [RFC4203], [RFC5307] + [RFC5392] and [RFC5316]
101	PW only requirement, see PW Requirements Table (5.2)
102	(Requirement intentionally blank.)
103	[RFC3473], [RFC4203], [RFC5307], [RFC5063]
104	[RFC4872], [RFC4873], [TP-RING]
105	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
106	[RFC3473], [CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
107	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
108	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT] + (See Sec. 4.4.5)
109	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
110	[RFC3473], [RFC4872], [RFC4873]
111	[RFC3473], [RFC4872], [RFC4873]
112	[RFC3473], [RFC4783]
113	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
114	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT] + (See Sec. 4.4.5)
115	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT] + (See Sec. 4.4.5)
116	[RFC3473]
117	[RFC4426], [RFC4872], [RFC4873]
118	[RFC3473], [RFC4872], [RFC4873]

119	[RFC3473], [RFC4783]
120	[RFC3473]
121	[RFC3473], [RFC4783]
122	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT] + (See Sec. 4.4.5)
123	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT] + (See Sec. 4.4.5)
124	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT], [HIERARCHY-BIS]
125	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT]
126	[CCAMP-OAM-FWK], [CCAMP-OAM-EXT]

4.4. Anticipated MPLS-TP Related Extensions and Definitions

This section identifies the extensions and other documents that have been identified as likely to be needed to support the full set of MPLS-TP control plane requirements.

4.4.1. MPLS to MPLS-TP Interworking

[RFC5145] identifies a set of solutions that are aimed to aid in the interworking of MPLS-TE and GMPLS control planes. This work will serve as the foundation for a formal definition of MPLS to MPLS-TP control plane interworking.

4.4.2. Associated Bidirectional LSPs

GMPLS signaling, [RFC3473], supports unidirectional, and co-routed bidirectional point-to-point LSPs. MPLS-TP also requires support for associated bidirectional point-to-point LSPs. Such support will require an extension or a formal definition of how the LSP endpoints supporting an associated bidirectional service will coordinate the two LSPs used to provide such a service. Per requirement 11, transit nodes that support an associated bidirectional service should be aware of the association of the LSPs used to support the service. There are several existing protocol mechanisms on which to base such support, including, but not limited to:

o GMPLS calls, [RFC4974].

o The ASSOCIATION object, [RFC4872].

o The LSP_TUNNEL_INTERFACE_ID object, [HIERARCHY-BIS].

4.4.3. Asymmetric Bandwidth LSPs

[RFC5467] defines support for bidirectional LSPs which have different (asymmetric) bandwidth requirements for each direction. This RFC can be used to meet the related MPLS-TP technical requirement, but this RFC is currently an Experimental RFC. To fully satisfy MPLS-TP requirement this document will need to become a Standards Track RFC.

4.4.4. Recovery for P2MP LSPs

The definitions of P2MP, [RFC4875], and GMPLS recovery, [RFC4872] and [RFC4873], do not explicitly cover their interactions. MPLS-TP requires a formal definition of recovery techniques for P2MP LSPs. Such a formal definition will be based on existing RFCs and may not require any new protocol mechanisms, but nonetheless, must be documented.

4.4.5. Test Traffic Control and other OAM functions

[CCAMP-OAM-FWK] and [CCAMP-OAM-EXT] are works in progress that extend the OAM related control capabilities of GMPLS. These extensions cover a portion, but not all OAM related control functions that have been identified in the context of MPLS-TP. As discussed above, the MPLS-TP control plane must support the selection of which (if any) OAM function(s) to use (including support to select experimental OAM functions) and what OAM functionality to run, including, continuity check (CC), connectivity verification (CV), packet loss and delay quantification, and diagnostic testing of a service. As OAM configuration is directly linked to data plane OAM, it is expected that [CCAMP-OAM-EXT] will evolve in parallel with the specification of data plane OAM functions.

4.4.6. DiffServ Object usage in GMPLS

[RFC3270] and [RFC4124] defines support for DiffServ enabled MPLS LSPs. While the document references GMPLS signaling, there is no explicit discussion on the use of the DiffServ related objects in GMPLS signaling. A (possibly Information) document on how GMPLS supports DiffServ LSPs is likely to prove useful in the context of MPLS-TP.

5. Pseudowires

5.1. LDP Functions and Pseudowires

MPLS PWs are defined in [RFC3985] and [RFC5659], and provide for emulated services over an MPLS Packet Switched Network (PSN). Several types of PWs have been defined: (1) Ethernet PWs providing for Ethernet port or Ethernet VLAN transport over MPLS [RFC4448], (2) HDLC/PPP PW providing for HDLC/PPP leased line transport over MPLS[RFC4618], (3) ATM PWs [RFC4816], (4) Frame Relay PWs [RFC4619], and (5) circuit Emulation PWs [RFC4553].

Today's transport networks based on PDH, WDM, or SONET/SDH provide transport for PDH or SONET (e.g., ATM over SONET or Packet PPP over SONET) client signals with no payload awareness. Implementing PW capability allows for the use of an existing technology to substitute the TDM transport with packet based transport, using well-defined PW encapsulation methods for carrying various packet services over MPLS, and providing for potentially better bandwidth utilization.

There are two general classes of PWs: (1) Single-Segment Pseudowires (SS-PW) [RFC3985], and (2) Multi-segment Pseudowires (MS-PW) [RFC5659]. An MPLS-TP domain may transparently transport a PW whose endpoints are within a client network. Alternatively, an MPLS-TP edge node may be the Terminating PE (T-PE) for a PW, performing adaptation from the native attachment circuit technology (e.g. Ethernet 802.1Q) to an MPLS PW which is then transported in an LSP over an MPLS-TP domain. In this way, the PW is analogous to a transport channel in a TDM network and the LSP is equivalent to a container of multiple non-concatenated channels, albeit they are packet containers. The MPLS-TP domain may also contain Switching PEs (S-PEs) for a multi-segment PW whereby the T-PEs may be at the edge of the MPLS-TP domain or in a client network. In this latter case, a T-PE in a client network is a T-PE performing the adaptation of the native service to MPLS and the MPLS-TP domain performs Pseudo-wire switching.

SS-PW signaling control plane is based on LDP with specific procedures defined in [RFC4447]. [RFC5659], [SEGMENTED-PW] and [MS-PW-DYNAMIC] allow for static switching of multi-segment Pseudowires in data and control plane and for dynamic routing and placement of an MS-PW whereby signaling is still based on Targeted LDP (T-LDP). The MPLS-TP domain shall use the same PW signaling protocols and procedures for placing SS-PWs and MS-PWs. This will leverage existing technology as well as facilitate interoperability with client networks with native attachment circuits or PW segment that is switched across the MPLS-TP domain.

Comment [M69]: A routing sub section should be add here. It is essential for MS-PW. Furthermore, the TE mechanism for MS-PW should be described

Comment [M70]: Specification for PW QoS, TE parameters, explicit route control and OAM configuration (for MS-PW) should be provided

5.2. PW Control (LDP) and MPLS-TP Requirements Table

The following table shows how the MPLS-TP control plane requirements can be met using the existing LDP control plane for Pseudowires (targeted LDP). Areas where additional specifications are required are also identified. The table lists references based on the control plane requirements as identified and numbered above in section 2.

In the table below, several of the requirements shown are addressed - in part or in full - by the use of MPLS-TP LSPs to carry pseudo-wires. This is reflected by including "TP-LSPs" as a reference for those requirements. Section 5.3.2 provides additional context for the binding of PWs to TP-LSPs.

Req #	References
1	Generic requirement met by using Standards Track RFCs
2	[RFC3985], [RFC4447], Together with TP-LSPs (Sec. 4.3)
3	[RFC3985], [RFC4447]
4	Generic requirement met by using Standards Track RFCs
5	[RFC3985], [RFC4447], Together with TP-LSPs
6	[RFC3985], [RFC4447], [PW-P2MPR], [PW-P2MPE] + TP-LSPs
7	[RFC3985], [RFC4447], + TP-LSPs
8	[PW-P2MPR], [PW-P2MPE]
9	[RFC3985], end-node only involvement for PW
10	[RFC3985], proper vendor implementation
11	[RFC3985], end-node only involvement for PW
12-13	[RFC3985], [RFC4447], See Section 5.3.4
14	[RFC3985], [RFC4447]
15	[RFC4447], [RFC3478], proper vendor implementation
16	[RFC3985], [RFC4447]
17-18	[RFC3985], proper vendor implementation
19-26	[RFC3985], [RFC4447], [RFC5659], implementation
27	[RFC4448], [RFC4816], [RFC4618], [RFC4619], [RFC4553]
	[RFC4842], [RFC5287]
28	[RFC3985]
29-31	[RFC3985], [RFC4447]
32	[RFC3985], [RFC4447], [RFC5659], See Section 5.3.6.
33	[RFC4385], [RFC4447], [RFC5586]
34	[PW-P2MPR], [PW-P2MPE]
35	[RFC4863]
36-37	[RFC3985], [RFC4447], See Section 5.3.4
38	[RFC5586]
39	Provided by TP-LSPs
40	[RFC3985], [RFC4447], + TP-LSPs
41	[RFC3478]
42-43	[RFC3985], [RFC4447]
44-45	[RFC3985], [RFC4447], + TP-LSPs - See Section 5.3.5
46	[RFC3985], [RFC4447], [RFC5659] + TP-LSPs
47	[RFC3985], [RFC4447], + TP-LSPs - See Section 5.3.3
48	[PW-RED], [PW-REDB]
49-50	[RFC3985], [RFC4447], + TP-LSPs, implementation
51-53	Provided by TP-LSPs, and Section 5.3.5
54-56	[RFC3985], [RFC4447], See Section 5.3.5
57	[PW-RED], [PW-REDB]
	revertive/non-revertive behavior is a local matter for PW
58-59	[PW-RED], [PW-REDB]
60-82	[RFC3985], [RFC4447], [PW-RED], [PW-REDB], Section 5.3.5
83-84	[RFC5085], [RFC5586], [RFC5885]
85-90	[RFC3985], [RFC4447], [PW-RED], [PW-REDB], Section 5.3.5
91-96	[RFC3985], [RFC4447], + TP-LSPs, implementation
97	[RFC4447], [MS-PW-DYNAMIC]
98	[RFC4447]
99 -	

100	Not Applicable to PW
101	[RFC4447]
102	(Requirement intentionally blank.)
103	[RFC3478]
104	[RFC3985], + TP-LSPs
105	[PW-OAM]
106	[PW-OAM]
107 - 109	[RFC5085], [RFC5586], [RFC5885]
110	[RFC5085], [RFC5586], [RFC5885] fault reporting and protection triggering is a local matter for PW
111	[RFC5085], [RFC5586], [RFC5885] fault reporting and protection triggering is a local matter for PW
112	[RFC4447]
113	[RFC4447], [RFC5085], [RFC5586], [RFC5885]
114	[RFC5085], [RFC5586], [RFC5885]
115	[RFC5085], [RFC5586], [RFC5885]
116	path traversed by PW is determined by LSP path, see GMPLS and MPLS-TP Requirements Table, 4.3
117	[PW-RED], [PW-REDB], administrative control of redundant PW is a local matter at the PW head-end
118	[PW-RED], [PW-REDB], [RFC5085], [RFC5586], [RFC5885]
119	[RFC3985], [RFC4447], [PW-RED], [PW-REDB], Section 5.3.5
120	[RFC4447]
121 - 126	[RFC5085], [RFC5586], [RFC5885]

5.3. Anticipated MPLS-TP Related Extensions

The same control protocol and procedures will be reused as much as possible. However, when using PWs in MPLS-TP, a set of new requirements are defined which may require extensions of the existing control mechanisms. This section clarifies the areas where extensions are needed based on the PW Control Plane related requirements documented in [RFC5654].

See the table in the section above for a list of how requirements defined in [RFC5654] are expected to be addressed.

The baseline requirement for extensions to support transport applications is that any new mechanisms and capabilities must be able to interoperate with existing IETF MPLS [RFC3031] and IETF PWE3 [RFC3985] control and data planes where appropriate. Hence, extensions of the PW Control Plane must be in-line with the procedures defined in [RFC4447], [SEGMENTED-PW] and [MS-PW-DYNAMIC].

5.3.1. Extensions to Support Out-of-Band PW Control

For MPLS-TP, it is required that the data and control planes can be both logically and physically separated. That is, the PW Control Plane must be able to operate out-of-band (OOB). This separation ensures, among other things, that in the case of control plane failures the data plane is not affected and can continue to operate normally. This was not a design requirement for the current PW Control Plane. However, due to the PW concept, i.e., PWs are connecting logical entities ('forwarders'), and the operation of the PW control protocol, i.e., only edge PE nodes (T-PE, S-PE) take part in the signaling exchanges: moving T-LDP out-of-band seems to be, theoretically, a straightforward exercise.

In fact, as a strictly local matter, ensuring that Targeted LDP (T-LDP) uses out-of-band signaling requires only that the local implementation is configured in such a way that reachability for a target LSR address is via the out-of-band channel.

More precisely, if IP addressing is used in the MPLS-TP control plane then T-LDP addressing can be maintained, although all addresses will refer to control plane entities. Both, the PWid FEC and Generalized PWid FEC Elements can possibly be used in an OOB case as well. (Detailed evaluation is outside the scope of this document). The PW Label allocation and exchange mechanisms should be reused without change.

5.3.2. Support for Explicit Control of PW-to-LSP Binding

Comment [M71]: Is this binding only for dynamic PW and dynamic LSP? What will it be if a dynamic PW is bound to a static LSP and the reverse?

Binding a PW to an LSP, or PW segments to LSPs is left to networks elements acting as T-PEs and S-PEs or a control plane entity that may be the same one signaling the PW. However, an extension of the PW signaling protocol is required to allow the LSR at signal initiation end to inform the targeted LSR (at the signal termination end) which LSP the resulting PW is to be bound to, in the event that more than one such LSP exists and the choice of LSPs is important to the service being setup (for example, if the service requires co-routed bidirectional paths). This is also particularly important to support transport path (symmetric and asymmetric) bandwidth requirements.

If the control plane is physically separated from the forwarder, the control plane must be able to program the forwarders with necessary information.

For transport services, it may be required that bidirectional traffic follows congruent paths. Currently, each direction of a PW or a PW segment is bound to a unidirectional LSP that extends between two T-PEs, S-PEs, or a T-PE and an S-PE. The unidirectional LSPs in both directions are not required to follow congruent paths, and therefore both directions of a PW may not follow congruent paths, i.e., they are associated bidirectional paths. The only requirement in [RFC5659] is that a PW or a PW segment shares the same T-PEs in both directions, and same S-PEs in both directions.

MPLS-TP imposes new requirements on the PW Control Plane, in requiring that PW or PW segment both end points map the PW or PW segment to the same transport path for the case where this is an objective of the service. When a bidirectional LSP is selected on one end to transport the PW, a mechanism is needed that signals to the remote end which LSP has been selected locally to transport the PW. This would be accomplished by adding a new TLV to PW signaling.

Note that this coincides with the gap identified for OOB support: a new mechanism is needed to allow explicit binding of a PW to the supporting transport LSP.

The case of unidirectional transport paths may also require additional protocol mechanisms as today's PWs are always bidirectional. One potential approach for providing a unidirectional PW based transport path is for the PW to associate different (asymmetric) bandwidths in each direction, with a zero or minimal bandwidth for the return path.

5.3.3. Support for Dynamic Transfer of PW Control/Ownership

In order to satisfy requirement 47 (as defined in section 2) it will be necessary to specify methods for transfer of PW ownership from the management to the control plane (and vice versa).

5.3.4. Interoperable Support for PW/LSP Resource Allocation

Transport applications may require resource guarantees. For such transport LSPs, resource reservation mechanisms are provided via RSVP-TE and the use of DiffServ. If multiple PWs are multiplexed into the same transport LSP resources, contention may occur. However, local policy at PEs should ensure proper resource sharing among PWs mapped into a resource guaranteed LSP. In the case of MS-PWs, signaling carries the PW traffic parameters [MS-PW-DYNAMIC] to enable admission control of a PW segment over a resource-guaranteed LSP.

In conjunction with explicit PW-to-LSP binding, existing mechanisms may be sufficient, however this needs to be verified in detailed evaluation.

5.3.5. Support for PW Protection and PW OAM Configuration

The PW control plane must be able to establish and configure all of the available features manageable for the PW, including protection and OAM entities and mechanisms. There is ongoing work on PW protection and MPLS-TP OAM.

5.3.6. Client Layer Interfaces to Pseudowire Control

Additional work is likely to be required to define consistent access by a client layer network to control information available to the client layer network, for example, about the topology of an MS-PW. This information may be required by the client layer network in order to provide hints that may help to avoid establishment of fate-sharing alternate paths.

5.4. Pseudowire OAM and Recovery (Redundancy)

Many of the requirements listed in section 2 are intended to support connectivity and performance monitoring (grouped together as OAM) and protection conformant with the transport services model.

In general, protection of MPLS-TP transported services is provided by way of protection of transport LSPs. PW protection requires that mechanisms be defined to support redundant Pseudowires, including a mechanism already described above for associating such Pseudowires with specific protected ("working" and "protection") LSPs. Also required are definitions of local protection control functions, to include test/verification operations, and protection status signals needed to ensure that PW termination points are in agreement as to which of a set of redundant Pseudowires are in use for which transport services at any given point in time.

Comment [M72]: MS-PW recovery that is independent of LSP recovery should considered. This would allow recovery in the event of a PE node failure.

Much of this work is currently being done in drafts [PW-RED] and [PW-REDB] that define - respectively - how to establish redundant Pseudowires and how to indicate which is in use. Additional work may be required.

Protection switching may be triggered manually by the operator, or as a result of loss of connectivity (detected using the mechanisms of [RFC5085] and [RFC5586]), or service degradation (detected using mechanisms yet to be defined).

Automated protection switching is but one of the functions that a transport service requires OAM for. OAM is generally referred to as either "proactive" or "on-demand", where the distinction is whether a specific OAM tool is being used continuously over time (for the purpose of detecting a need for protection switching, for example) or is only used - either a limited number of times, or over a short period of time - when explicitly enabled (for diagnostics, for example).

PW OAM currently consists of connectivity verification defined by [RFC5085]. Work is currently in progress to extend PW OAM to include bidirectional forwarding detection (BFD) in [RFC5885], and work has begun on extending BFD to include performance related monitor functions.

6. Security Considerations

This document primarily describes how exiting mechanisms can be used to meet the MPLS-TP control plane requirements. The documents that describe each mechanism contain their own security considerations sections. For a general discussion on MPLS and GMPLS related security issues, see the MPLS/GMPLS security framework [MPLS-SEC].

This document also identifies a number of needed control plane extensions. It is expected that the documents that define such extensions will also include any appropriate security considerations.

7. IANA Considerations

There are no new IANA considerations introduced by this document.

8. Acknowledgments

The authors would like to acknowledge the contributions of Yannick Brehon, Diego Caviglia, Nic Neate, and Dave Mcdysan to this work.

9. References

9.1. Normative References

[RFC2210] Wroclawski, J., "The Use of RSVP with Integrated Services", RFC 2210, September 1997.

[RFC2211] Wroclawski, J., "Specification of the Controlled Load Quality of Service", RFC 2211, September 1997.

[RFC2212] Shenker, S., Partridge, C., and R Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, September 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119.

[RFC3031] Rosen, E., Viswanathan, A., Callon, R., "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3471] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.

[RFC3473] Berger, L. Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC3478] Leelanivas, M, et al, "Graceful Restart Mechanism for Label Distribution Protocol", RFC 3478, February 2003.

[RFC3630] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, September 2003.

[RFC4124] Le Faucheur, F., Ed. "Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering", RFC 4124, June 2005.

[RFC4202] Kompella, K. and Y. Rekhter, "Routing Extensions in Support of Generalized Multi-Protocol Label Switching(GMPLS)", RFC 4202, October 2005.

[RFC4203] Kompella, K. and Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, October 2005.

[RFC4206] Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, October 2005.

[RFC4385] Bryant, S., et al, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, February 2006.

[RFC4447] Martini, L., Ed., "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

[RFC4448] Martini, L., Ed., "Encapsulation Methods for Transport Ethernet over MPLS Network", RFC 4448, April 2006.

[RFC4842] Malis, A., et al, "Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Circuit Emulation over Packet (CEP)", RFC 4842, April 2007.

[RFC4863] Martini, L. and G. Swallow, "Wildcard Pseudowire Type", RFC 4863, May 2007.

[RFC4872] Lang, J., Rekhter, Y., and Papadimitriou, D., "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., Farrel, A., "GMPLS Segment Recovery", RFC 4873, May 2007.

[RFC4929] Andersson, L. and A. Farrel, "Change Process for Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Protocols and Procedures", BCP 129, RFC 4929, June 2007.

[RFC4974] Papadimitriou, D., Farrel, A., "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls", RFC 4974, August 2007.

[RFC5063] Satyanarayana, A., Ed., "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart", RFC 5063, September 2007.

[RFC5287] Vainshtein, A. and Y. Stein, "Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks", RFC 5287, August 2008.

[RFC5305] Smit, H. and T. Li, "IS-IS Extensions for Traffic Engineering", RFC 5305, October 2008.

[RFC5307] Kompella, K. and Rekhter, Y., "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 5307, October 2008.

[RFC5316] Chen, M., Zhang, R., and Duan, X., "ISIS Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering", RFC 5316, December 2008.

[RFC5392] Chen, M., Zhang, R., and Duan, X., "OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering", RFC 5392, January 2009.

[RFC5151] Farrel, A., Ed., "Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 5151, February 2008.

[RFC5654] Niven-Jenkins, B., et al, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC5467] Berger, L., et al, "GMPLS Asymmetric Bandwidth Bidirectional Label Switched Paths (LSPs)", RFC 5467, March 2009.

[RFC5586] Bocci, M., et al, "MPLS Generic Associated Channel", RFC 5586, June 2009.

[RFC5860] Vigoureux, M., Ward, D., Betts, M., "Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks", RFC 5860, May 2010.

[TP-DATA] Frost, D., Bryant, S., Bocci, M., "MPLS Transport Profile Data Plane Architecture", work in progress, draft-ietf-mpls-tp-data-plane.

[TP-FWK] Bocci, M., Ed., et al, "A Framework for MPLS in Transport Networks", work in progress, draft-ietf-mpls-tp-framework.

[TP-OAM] Busi, I., Ed., Niven-Jenkins, B., Ed., "MPLS-TP OAM Framework and Overview", work in progress, draft-ietf-mpls-tp-oam-framework.

[TP-SURVIVE] Sprecher, N., et al., "Multiprotocol Label Switching Transport Profile Survivability Framework", work in progress, draft-ietf-mpls-tp-survive-fwk.

9.2. Informative References

[CCAMP-OAM-FWK] A. Takacs, D. Fedyk, and J. He, "OAM Configuration Framework and Requirements for GMPLS RSVP-TE", work in progress, draft-ietf-ccamp-oam-configuration-fwk.

[CCAMP-OAM-EXT] Bellagamba, E., et.al., "RSVP-TE Extensions for MPLS-TP OAM Configuration", work in progress, draft-bellagamba-ccamp-rsvp-te-mpls-tp-oam-ext.

[GMPLS-MLN] Papadimitriou, D., et al, "Generalized Multi-Protocol Label Switching (GMPLS) Protocol Extensions for Multi-Layer and Multi-Region Networks (MLN/MRN)", work in progress, draft-ietf-ccamp-gmpls-mln-extensions.

[GMPLS-PS] Takacs, A., et al, "GMPLS RSVP-TE Recovery Extension for data plane initiated reversion and protection timer signalling", work in progress, draft-takacs-ccamp-revertive-ps.

[HIERARCHY-BIS] Shiomoto, K, Ed., Farrel, A, Ed., "Procedures for Dynamically Signaled Hierarchical Label Switched Paths", work in progress, draft-ietf-ccamp-lsp-hierarchy-bis.

[TE-MIB] T Otani, et.al., "Traffic Engineering Database Management Information Base in support of MPLS-TE/GMPLS", work in progress, draft-ietf-ccamp-gmpls-ted-mib.

[MS-PW-DYNAMIC] L. Martini, M Bocci, and F Balus "Dynamic Placement of Multi Segment Pseudo Wires", work in progress, draft-ietf-pwe3-dynamic-ms-pw.

[ITU.G8080.2006] International Telecommunications Union, "Architecture for the automatically switched optical network (ASON)", ITU- T Recommendation G.8080, June 2006.

[ITU.G8080.2008] International Telecommunications Union, "Architecture for the automatically switched optical network (ASON) Amendment 1", ITU-T Recommendation G.8080 Amendment 1, March 2008.

[MPLS-SEC] Fang, L., et al, "Security Framework for MPLS and GMPLS Networks", work in progress, draft-ietf-mpls-mpls-and-gmpls-security-framework.

[NO-PHP] Ali, z., et al, "Non PHP Behavior and out-of-band mapping for RSVP-TE LSPs", work in progress, draft-ietf-mpls-rsvp-te-no-php-oob-mapping

[SEGMENTED-PW] Martini, L., Nadeau, T., and Duckett M., "Segmented Pseaudowire", work in progress, draft-ietf-pwe3-segmented-pw.

[TP-P2MP-FWK] D. Frost, M. Bocci, and L. Berger, "A Framework for Point-to-Multipoint MPLS in Transport Networks", draft-fbb-mpls-tp-p2mp-framework.

[RFC3270] Le Faucheur, F., et al, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", RFC 3270, May 2002.

[RFC3472] Ashwood-Smith, P., Ed, Berger, L. Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions", RFC 3472, January 2003.

[RFC3477] Kompella, K., Rekhter, Y., "Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)", RFC 3477, January 2003.

[RFC3478] Leelanivas, M., Rekhter, Y., Aggarwal, R., "Graceful Restart Mechanism for Label Distribution Protocol", RFC 3478, February 2003.

[RFC3812] Srinivasan, C., Viswanathan, A., and T. Nadeau, "Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)", RFC 3812, June 2004.

[RFC3813] Srinivasan, C., Viswanathan, A., and T. Nadeau, "Multiprotocol Label Switching (MPLS) Label Switching (LSR) Router Management Information Base (MIB)", RFC 3813, June 2004.

[RFC3945] Mannie, E., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, October 2004.

[RFC3985] Bryant, S. and P. Pate, "Pseudowire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.

[RFC4139] Papadimitriou, D., et al, "Requirements for Generalized MPLS (GMPLS) Signaling Usage and Extensions for Automatically Switched Optical Network (ASON)", RFC4139, July 2005.

[RFC4201] Kompella, K., Rekhter, Y., Berger, L., "Link Bundling in MPLS Traffic Engineering (TE)", RFC 4201, October 2005.

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and Rekhter, Y., "Generalized Multi-Protocol Label Switching (GMPLS) User-Network Interface (UNI) : Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, October 2005.

[RFC4258] Brungard, D., et al, "Requirements for Generalized Multi-Protocol Label Switching (GMPLS) Routing for the Automatically Switched Optical Network (ASON)", RFC4258, November 2005.

[RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[RFC4426] Lang, J., Rajagopalan B., and D.Papadimitriou, Editors, "Generalized Multiprotocol Label Switching (GMPLS) Recovery Functional Specification", RFC 4426, March 2006.

[RFC4427] Mannie, E., Papadimitriou, D., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC4427, March 2006.

[RFC4553] Vainshtein, A., Ed., and Stein, YJ., Ed.,"Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)", RFC 4553, June 2006.

[RFC4618] Martini, L., Rosen, E., Heron, G., and Malis, A., "Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks", RFC 4618, September 2006.

[RFC4619] Martini, L., Ed., Kawa, C., Ed., and Malis, A., Ed., "Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks", September 2006.

[RFC4655] Farrel, A., Vasseur, J.-P., Ash, J., "A Path Computation Element (PCE)-Based Architecture", RFC 4655, August 2006.

[RFC4783] Berger, L.,Ed., "GMPLS - Communication of Alarm Information", RFC 4763, December 2006.

[RFC4802] T. D. Nadeu and A. Farrel, "Generalized Multiprotocol Label Switching (GMPLS) Traffic Engineering Management Information Base", RFC 4802, February 2007.

[RFC4803] T. D. Nadeu and A. Farrel, "Generalized Multiprotocol Label Switching (GMPLS) Label Switching Router (LSR) Management Information Base", RFC 4803, February 2007.

[RFC4816] Malis, A., Martini, L., Brayley, J., and Walsh, T., "Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service", RFC 4816, February 2007.

[RFC4875] Aggarwal, R., Papadimitriou, D., Yasukawa, S., "Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)", RFC 4875, May 2007.

[RFC5085] Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV) : A Control Channel for Pseudowires", RFC 5085, December 2007.

[RFC5145] Shiomoto, K., "Framework for MPLS-TE to GMPLS Migration", RFC 5145, March 2008.

[RFC5440] Vasseur, JP., Le, JL., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, March 2009.

[RFC5493] Caviglia, D., et al, "Requirements for the Conversion between Permanent Connections and Switched Connections in a Generalized Multiprotocol Label Switching (GMPLS) Network", RFC 5493, April 2009.

[RFC5659] Bocci, M., and Bryant, B., "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, October 2009.

[RFC5718] Bellar, D., Farrel, A., "An In-Band Data Communication Network For the MPLS Transport Profile", RFC 5718, January 2010.

[RFC5787] Papadimitriou, D., "OSPFv2 Routing Protocols Extensions for ASON Routing", RFC 5787, March 2010.

[RFC5852] Caviglia, D., Ceccarelli, D., Bramanti, D., Li, D., Bardalai, S., "RSVP-TE Signaling Extension for LSP Handover from the Management Plane to the Control Plane in a GMPLS-Enabled Transport Network", RFC 5852, April 2010.

[RFC5884] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "Bidirectional Forwarding Detection (BFD) For MPLS Label Switched Paths (LSPs)", RFC 5884, June 2010.

[RFC5885] Nadeau, T. and C. Pignataro, "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", RFC 5885, June 2010.

[PW-RED] Muley, P., et al, "Pseudowire (PW) Redundancy", work in progress, draft-ietf-pwe3-redundancy.

[PW-REDB] Muley, P., et al, "Preferential Forwarding Status bit definition", work in progress, draft-ietf-pwe3-redundancy-bit.

[PW-OAM] Zhang, F., et al, "LDP Extensions for MPLS-TP PW OAM configuration", work in progress, draft-zhang-mpls-tp-pw-oam-config.

[PW-P2MPE] Aggarwal, R. and F. Jounay, "Point-to-Multipoint Pseudo-Wire Encapsulation", work in progress, draft-raggarwa-pwe3-p2mp-pw-encaps.

[PW-P2MPR] Jounay, F., et al, "Requirements for Point-to-Multipoint Pseudowire", work in progress, draft-ietf-pwe3-p2mp-pw-requirements.

[TP-RING] Weingarten, Y., Ed., "MPLS-TP Ring Protection", work in progress, draft-weingarten-mpls-tp-ring-protection.

10. Authors' Addresses

Loa Andersson (editor)
Ericsson
Phone: +46 10 717 52 13
Email: loa.andersson@ericsson.com

Lou Berger (editor)
LabN Consulting, L.L.C.
Phone: +1-301-468-9228
Email: lberger@labn.net

Luyuan Fang (editor)
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA
Email: lufang@cisco.com

Nabil Bitar (editor)
Verizon,
40 Sylvan Rd.,
Waltham, MA 02451
Email: nabil.n.bitar@verizon.com

Attila Takacs
Ericsson
1. Laborc u.
Budapest, HUNGARY 1037
Email: attila.takacs@ericsson.com

Martin Vigoureux
Alcatel-Lucent
Email: martin.vigoureux@alcatel-lucent.fr

Elisa Bellagamba
Ericsson
Farogatan, 6
164 40, Kista, Stockholm, SWEDEN
Email: elisa.bellagamba@ericsson.com

Eric Gray
Ericsson
900 Chelmsford Street
Lowell, MA, 01851
Phone: +1 978 275 7470
Email: Eric.Gray@Ericsson.com