Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 4, 2009

B. Niven-Jenkins, Ed.
BT
D. Brungard, Ed.
AT&T
M. Betts, Ed.
Nortel Networks
N. Sprecher
Nokia Siemens Networks
October 31, 2008

MPLS-TP Requirements
draft-jenkins-mpls-mpls-tp-requirements-01

Status of this Memo

Abstract

This document specifies the requirements for a MPLS Transport Profile (MPLS-TP). This document is a product of a joint International Telecommunications Union (ITU)-IETF effort to include a MPLS Transport Profile within the IETF MPLS architecture to support the capabilities and functionalities of a packet transport network as defined by International Telecommunications Union - Telecommunications Standardization Sector (ITU-T).

This work is based on two sources of requirements, MPLS architecture as defined by IETF and packet transport networks as defined by ITU-T.

Requirements Language

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].

Table of Contents

1. Introduction

For many years, Synchronous Optical Networking (SONET)/Synchronous Digital hierarchy (SDH) has provided carriers with a high benchmark for reliability and operational simplicity. With the accelerating growth of packet-based services (such as Ethernet, Voice over IP (VoIP), Layer 2 (L2)/Layer 3 (L3) Virtual Private Networks (VPNs), IP Television (IPTV), Radio Access Network (RAN) backhauling, etc.), carriers are in need of capabilities to efficiently support packet-based services on their transport networks. The need to increase their revenue while remaining competitive forces operators to look for the lowest network Total Cost of Ownership (TCO). Investment in equipment and facilities (Capital Expenditure (CAPEX)) and Operational Expenditure (OPEX) should be minimized.

Carriers are considering migrating or evolving to packet transport networks in order to reduce their costs and to improve their ability to support services with guaranteed Service Level Agreements (SLAs). For carriers it is important that migrating from SONET/SDH to packet transport networks should not involve dramatic changes in network operation, should not necessitate extensive retraining, and should not require major changes to existing work practices. The aim is to preserve the look-and-feel to which carriers have become accustomed in deploying their SONET/SDH networks, while providing common, multi-layer operations, resiliency, control and management for packet, circuit and lambda transport networks.

Transport carriers require control and deterministic usage of network resources. They need end-to-end control to engineer network paths and to efficiently utilize network resources. They require capabilities to support static (Operational Support System (OSS) based) or dynamic (control plane) provisioning of deterministic, protected and secured services and their associated resources.

Carriers will still need to cope with legacy networks (which are composed of many layers and technologies), thus the packet transport network should interwork with other packet and transport networks (both horizontally and vertically). Vertical interworking is also known as client/server or network interworking. Horizontal interworking is also known as peer-partition or service interworking. For more details on each type of interworking and some of the issues that may arise (especially with horizontal interworking) see [ITU.Y1401.2008].

MPLS is a maturing packet technology and it is already playing an important role in transport networks and services. However, not all of MPLS's capabilities and mechanisms are needed and/or consistent with transport network operations. There is therefore the need to

define an MPLS Transport Profile (MPLS-TP) in order to support the capabilities and functionalities needed for packet transport network services and operations through combining the packet experience of MPLS with the operational experience of SONET/SDH.

MPLS-TP will enable the migration of SONET/SDH networks to a packet-based network that will efficiently scale to support packet services in a simple and cost effective way. MPLS-TP needs to combine the necessary existing capabilities of MPLS with additional minimal mechanisms in order that it can be used in a transport role.

This document specifies the requirements for a MPLS Transport Profile (MPLS-TP). This document is a product of a joint ITU-IETF effort to include a MPLS Transport Profile within the IETF MPLS architecture to support the capabilities and functionalities of a packet transport network as defined by ITU-T.

This work is based on two sources of requirements, MPLS architecture as defined by IETF and packet transport networks as defined by ITU-T. The requirements of MPLS-TP are provided below. The relevant functions of MPLS are included in MPLS-TP, except where explicitly excluded.

Although both static and dynamic configuration of MPLS-TP transport paths (including Operations, Administration and Maintenance (OAM) and protection capabilities) is required by this document, it MUST be possible for operators to be able to completely operate (including OAM and protection capabilities) an MPLS-TP network in the absence of any control plane protocols for dynamic configuration.

1.1. Terminology

Domain: A domain represents a collection of entities (for example network elements) that are grouped for a particular purpose, examples of which are administrative and/or managerial responsibilities, trust relationships, addressing schemes, infrastructure capabilities, survivability techniques, distributions of control functionality, etc. Examples of such domains include IGP areas and Autonomous Systems.

Layer network: A layer network as defined in G.805 [ITU.G805.2000] provides for the transfer of client information and independent operations (OAM) of the client OAM. For an explanation of how a layer network as described by G.805 relates to the OSI concept of layering see Appendix I of Y.2611 [ITU.Y2611.2006].

Link: A link as defined in G.805 [ITU.G805.2000] is used to describe a fixed relationship between two ports.

Path: See Transport path.

Section: A section is a MPLS-TP network server layer which provides for encapsulation and OAM of a MPLS-TP transport path client layer. A section layer may provide for aggregation of multiple MPLS-TP clients.

Segment: A segment corresponds to part of a path. A segment may be a single link (hop) within a path, a series of adjacent links (hops) within a path, or the entire end-to-end-path.

Service layer: A layer network in which transport paths are used to carry a customer's (individual or bundled) service (may be point-to-point, point-to-multipoint or multipoint-to-multipoint services).

Span: A span is synonymous with a link.

Tandem Connection: A tandem connection corresponds to a segment of a path. This may be either a segment of an LSP (i.e. a sub-path), or one or more segment(s) of a PW.

Transport path: A connection as defined in G.805 [ITU.G805.2000]. The combination of a PW (Single Segment or Multi-Segment) and LSP corresponds to an MPLS-TP transport path.

Transport path layer: A layer network which provides point-to-point or point-to-multipoint transport paths which are used to carry a higher (client) layer network or aggregates of higher (client) layer networks, for example the network service layer. It provides for independent OAM (of the client OAM) in the transport of the clients.

Transmission media layer: A layer network which provides sections (two-port point-to-point connections) to carry the aggregate of network transport path or network service layers on various physical media.

1.2. Transport network overview

The connection (or transport path) service is the basic service provided by a transport network. The purpose of a transport network is to carry its clients (i.e. the stream of client PDUs or client bits) between endpoints in the network (typically over several intermediate nodes). These endpoints may be service switching points or service terminating points. The connection services offered to customers are aggregated into large transport paths with long-holding times and independent OAM (of the client OAM), which contribute to enabling the efficient and reliable operation of the transport network. These transport paths are modified infrequently.

Aggregation and hierarchy are beneficial for achieving scalability and security since:

1. They reduce the number of provisioning and forwarding states in the network core.

2. They reduce load and the cost of implementing service assurance and fault management.

3. Clients are encapsulated and layer associated OAM overhead is added. This allows complete isolation of customer traffic and its management from carrier operations.

An important attribute of a transport network is that it is able to function regardless of which clients are using its connection service or over which transmission media it is running. The client, transport network and server layers are from a functional and operations point of view independent layer networks. Another key characteristic of transport networks is the capability to maintain the integrity of the client across the transport network. A transport network must provide the means to commit quality of service objectives to clients. This is achieved by providing a mechanism for client network service demarcation for the network path together with an associated network resiliency mechanism. A transport network must also provide a method of service monitoring in order to verify the delivery of an agreed quality of service. This is enabled by means of carrier-grade OAM tools.

Clients are first encapsulated. These encapsulated client signals may then be aggregated into a connection for transport through the network in order to optimize network management. Server layer OAM is used to monitor the transport integrity of the client layer or client aggregate. At any hop, the aggregated signals may be further aggregated in lower layer transport network paths for transport across intermediate shared links. The encapsulated client signals are extracted at the edges of aggregation domains, and are either delivered to the client or forwarded to another domain. In the core of the network, only the server layer aggregated signals are monitored; individual client signals are monitored at the network boundary in the client layer network.

Quality-of-service mechanisms are required in the packet transport network to ensure the prioritization of critical services, to guarantee BW and to control jitter and delay.

2. MPLS-TP Requirements

2.1. General requirements

1 MPLS-TP MUST be compatible with the MPLS data plane as defined by IETF. When MPLS offers multiple options in this respect, MPLS-TP SHOULD select the minimum sub-set (necessary and sufficient subset) applicable to a transport network application.

2 Any new functionality that is defined to fulfil the requirements for MPLS-TP MUST be agreed within IETF and re-use (as far as practically possible) existing MPLS standards.

3 Mechanisms and capabilities MUST be able to interoperate with existing IETF MPLS [RFC3031] and IETF PWE3 [RFC3985] control and data planes where appropriate.

4 MPLS-TP MUST support a connection-oriented packet switching paradigm with traffic engineering capabilities that allow deterministic control of the use of network resources.

5 MPLS-TP MUST support traffic engineered point to point (P2P) or point to multipoint (P2MP) transport paths.

6 MPLS-TP MUST support the logical separation of the control and management planes from the data plane.

7 MPLS-TP MUST allow the physical separation of the control and management planes from the data plane.

8 MPLS-TP MUST support static provisioning of transport paths via a Network Management System (NMS) or OSS (i.e. via the management plane).

9 Static provisioning MUST NOT depend on routing or signaling protocols (e.g. Generalized Multiprotocol Label Switching (GMPLS), Open Shortest Path First (OSPF), Intermediate System to Intermediate Systems (ISIS), Resource Reservation Protocol (RSVP), Border gateway Protocol (BGP), Label Distribution Protocol (LDP) etc.).

10 MPLS-TP MUST support the capability for network operation (including OAM) via an NMS/OSS (without the use of any control plane protocols).

11 A solution MUST be provided to suppor dynamic provisioning of MPLS-TP transport paths via a control plane.

12 The MPLS-TP data plane MUST be capable of functioning independently of the control or management plane used to operate the MPLS-TP layer network. That is the MPLS-TP data plane operation MUST continue to operate normally if the management plane or control plane that configured the transport paths fails.

13 MPLS-TP MUST support transport paths through multiple homogeneous domains.

14 MPLS-TP MUST NOT dictate the deployment of any particular network topology either physical or logical.

15 MPLS-TP MUST be able to scale with growing and increasingly complex network topologies as well as increasing bandwidth demands, number of customers or number of services.

16 MPLS-TP SHOULD support mechanisms to safeguard against the provisioning of transport paths which contain forwarding loops.

2.2. Layering requirements

17 An MPLS-TP network MUST operate in a multiple layer network environment consisting of independent service, transport path and transmission media layers.

MPLS-TP may be used as the service layer (for P2P and P2MP services) and/or as the transport path layer within a packet transport network.

18 A solution MUST be provided to support the transport of MPLS-TP and non MPLS-TP client layer networks over an MPLS-TP layer network.

19 A solution MUST be provided to support the transport of an MPLS-TP layer network over MPLS-TP and non MPLS-TP server layer networks (such as Ethernet, OTN, etc.)

20 In an environment where an MPLS-TP layer network is supporting a client network, and the MPLS-TP layer network is supported by a server layer network then operation of the MPLS-TP layer network MUST be possible without any dependencies on the server or client network.

The above are not only technology requirements, but also operational. Different administrative groups may be responsible for the same layer network or different layer networks, and require the capability for

autonomous network operations.

21 It MUST be possible to hide MPLS-TP layer network addressing and other information (e.g. topology) from client layers.

2.3. Data plane requirements

22 The identification of each transport path within its aggregate MUST be supported.

23 A label in a particular section MUST uniquely identify the transport path.

24 A transport path's source MUST be identifiable at its destination.

Transport paths can be aggregated by pushing and de-aggregated by popping labels. MPLS-TP labels are swapped within a transport path in a layer network instance when the traffic is forwarded from one MPLS-TP link to another MPLS-TP link.

25 MPLS-TP MUST support MPLS labels that are assigned by the downstream (with respect to data flow) node per [RFC3031] and [RFC3473] and MAY support context-specific MPLS labels as defined in [RFC5331].

26 It MUST be possible to operate and configure the MPLS-TP data (transport) plane without any IP forwarding capability in the MPLS-TP data plane.

27 MPLS-TP MUST support both unidirectional and bi-directional point-to-point transport paths.

28 An MPLS-TP network MUST require the forward and backward directions of a bi-directional transport path to follow the same path at each layer.

29 The intermediate nodes at each layer MUST be aware about the pairing relationship of the forward and the backward directions belonging to the same bi-directional transport path.

30 MPLS-TP MUST support unidirectional point-to-multipoint transport paths.

31 MPLS-TP transport paths MUST NOT perform merging in a way that prevents the unique identification of the source at the destination (e.g. no use of LDP mp2p signaling in order to avoid losing LSP head-end information, no use of PHP, etc).

32 MPLS-TP MUST be able to accommodate new types of client networks and services.

33 MPLS-TP SHOULD support mechanisms to minimize traffic impact during network reconfiguration.

34 MPLS-TP SHOULD support mechanisms which ensure the integrity of the transported customer's service traffic.

35 MPLS-TP 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).

2.4. Control plane requirements

The requirements for ASON signalling and routing and the requirements for multi-region and multi-layer networks as specified in [RFC4139], [RFC4258] and [RFC5212] respectively apply to MPLS-TP.

Additionally:

36 MPLS-TP SHOULD support control plane topologies that are independent of the data plane topology.

37 The MPLS-TP control plane MUST be able to be operated independent of any particular client or server layer control plane.

38 The MPLS-TP control plane MUST support establishing all the connectivity patterns defined for the MPLS-TP data plane (e.g., uni-directional and bidirectional P2P, uni-directional P2MP, etc.) including configuration of protection functions and any associated maintenance functions.

39 The MPLS-TP control pane MUST support the configuration and modification of OAM maintenance points as well as the activation/ deactivation of OAM when the transport path is established or modified.

40 An MPLS-TP control plane MUST support pre-allocated path protection.

In some situations it is impractical to expect acceptable recovery performance to be achieved using dynamic recalculation of transport path routes. For this reason, it is necessary to allow for pre-planning of protection routes for selected transport paths.

41 An MPLS-TP control plane MUST scale gracefully to support a large number of transport paths.

42 An MPLS-TP control plane SHOULD provide a common control mechanism for architecturally similar operations.

2.5. Network Management (NM) requirements

For requirements related to NM functionality for MPLS-TP, see the MPLS-TP NM requirements document [I-D.gray-mpls-tp-nm-req].

2.6. Operation, Administration and Maintenance (OAM) requirements

For requirements related to OAM functionality for MPLS-TP, see the MPLS-TP OAM requirements document [I-D.vigoureux-mpls-tp-oam-requirements].

2.7. Network performance management (PM) requirements

For requirements related to PM functionality for MPLS-TP, see the MPLS-TP OAM requirements document [I-D.vigoureux-mpls-tp-oam-requirements].

2.8. Protection & Survivability requirements

Network survivability plays a critical factor in the delivery of reliable services. Network availability is a significant contributor to revenue and profit. Service guarantees in the form of SLAs require a resilient network that rapidly detects facility or node failures and restores network operation in accordance with the terms of the SLA.

The requirements in this section use the recovery terminology defined in RFC 4427 [RFC4427].

43 MPLS-TP MUST support transport network style protection switching mechanisms (tandem network connection protection, LSP protection and PW protection) to provide the appropriate recovery time required to maintain customer SLAs when potentially thousands of services are simultaneously affected by a single failure.

44 MPLS-TP recovery mechanisms MUST be applicable at various levels throughout the network including support for span, tandem connection and end-to-end recovery.

45 MPLS-TP MUST support network restoration mechanisms controlled by a distributed control plane and MUST support network restoration mechanisms controlled by a management plane.

A. The restoration resources MAY be pre-planned and selected a priori, or computed after failure occurrence.

B. MPLS-TP MAY support shared-mesh restoration.

C. MPLS-TP MUST support soft (make before break) LSP restoration.

D. MPLS-TP MAY support hard (break before make) LSP restoration.

E. The restoration mechanism MUST be applicable to any topology.

F. Restoration priority MUST be implemented to determine the order in which transport paths should be restored (to minimize service restoration time as well as to gain access to available spare capacity on the best paths). Preemption priority MUST be supported, so that in the event that not all transport paths can be restored transport paths with lower preemption priority can be released. When preemption is supported, its use MUST be operator configurable.

G. The restoration mechanism MUST operate in synergy with other transport network technologies (SDH, OTN, WDM).

46 MPLS-TP MUST support inband OAM driven protection mechanisms (without any dependency on a control plane) to enable fast recovery from failure.

47 If protection is supported then:

A. MPLS-TP protection mechanisms MUST apply to LSPs and PWs.

B. MPLS-TP MUST support mechanisms that rapidly detect, locate, notify and remedy network faults.

C. MPLS-TP MAY support 1:1 bidirectional protection switching. If bi-directional 1:1 protection switching is activated then the protection state of both ends of the protected entity MUST be synchronized.

D. MPLS-TP MAY support 1+1 unidirectional protection switching.

E. MPLS-TP protection mechanisms MUST be applicable to point-to-point and point-to-multipoint transport paths.

F. Protection ratio MUST be of 100%, i.e. 100% of impaired working traffic MUST be protected for a failure on the working path. Additionally:

   1. The QoS objectives defined by the operator MUST also be met along the protection path.

   2. In the case of 1:1 protection mechanisms, the bandwidth reserved for the protection path MAY be available for other traffic when the working path is operational.

G. Operator requests for manual control of protection switching such as clear, lockout of protection, forced-switch and manual-switch commands MUST be supported. Prioritized protection between Signal Fail (SF), Signal Degradation (SD) and operator switch requests MUST be supported.

H. MPLS-TP protection mechanisms 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).

I. MPLS-TP protection mechanisms MUST support revertive and non-revertive behaviour.

J. MPLS-TP protection switching mechanisms MUST prevent frequent operation of the protection switch due to an intermittent defect.

K. MPLS-TP protection mechanisms MUST ensure co-ordination of timing of protection switches at multiple layers to avoid races and to allow the protection switching mechanism of the server layer to fix the problem before switching at the MPLS-TP layer.

L. MPLS-TP MAY support mechanisms that are optimized for specific network topologies (e.g. ring). These mechanisms MUST be interoperable with the mechanisms defined for arbitrary topology (mesh) networks.

M. If optimised mechanisms for ring topologies are supported then they MUST support switching times within 50 ms (depending on CV rate configuration) assuming a reference network of a 16 node ring with less than 1200 Km of fiber, as defined by ITU SG15, Question 9.

2.9. QoS requirements

Carriers require advanced traffic management capabilities to enforce and guarantee the QoS parameters of customers' SLAs.

Quality of service mechanisms are required to ensure:

48 Support for differentiated services and different traffic types with traffic class separation associated with different traffic.

49 Prioritization of critical services.

50 Enabling the provisioning and the guarantee of Service Level Specifications (SLS), with support for hard and relative end-to-end BW guaranteed.

51 Controlled jitter and delay.

52 Guarantee of fair access to shared resources in an MPLS-TP network.

53 Resources for control and management plane packets so that data plane traffic, regardless of the amount, will not cause control and management functions to become inoperative.

54 MPLS-TP MUST support a flexible bandwidth allocation scheme. This will provide carriers with the capability to efficiently support service demands over the MPLS-TP network.

[Should we refer here to the requirements specified in RFC 2702?]

2.10. Security requirements

For a description of the security threats relevant in the context of MPLS and GMPLS and the defensive techniques to combat those threats see the Security Framework for MPLS & GMPLS Networks [I-D.draft-ietf-mpls-mpls-and-gmpls-security-framework].

3. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

4. Security Considerations

For a description of the security threats relevant in the context of MPLS and GMPLS and the defensive techniques to combat those threats see the Security Framework for MPLS & GMPLS Networks [I-D.draft-ietf-mpls-mpls-and-gmpls-security-framework].

5. Acknowledgements

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

The authors would also like to thank Loa Andersson, Italo Busi, John Drake, Neil Harrison, Wataru Imajuku, Julien Meuric, Tom Nadeau, Hiroshi Ohta, Tomonori Takeda and Satoshi Ueno for their comments and enhancements to the text.

6. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC3473] Berger, L., "Multiprotocol Label Switching Architecture", RFC 3473, January 2003.

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

[RFC4139] Papadimitriou, D., Drake, J., Ash, J., Farrel, A., and L. Ong, "Requirements for Generalized MPLS (GMPLS) Signaling Usage and Extensions for Automatically Switched Optical Network (ASON)", RFC 4139, July 2005.

[RFC4258] Brungard, D., "Requirements for Generalized Multi-Protocol Label Switching (GMPLS) Routing for the Automatically Switched Optical Network (ASON)", RFC 4258, November 2005.

[RFC4427] Mannie, E. and D. Papadimitriou, "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, March 2006.

[RFC5212] Shiomoto, K., Papadimitriou, D., Le Roux, JL., Vigoureux, M., and D. Brungard, "Requirements for GMPLS-Based Multi-Region and Multi-Layer Networks (MRN/MLN)", RFC 5212, July 2008.

[RFC5331] Aggarwal, R., Rekhter, Y., and E. Rosen, "MPLS Upstream Label Assignment and Context-Specific Label Space", RFC 5331, August 2008.

[I-D.gray-mpls-tp-nm-req] Lam, H., Mansfield, S., and E. Gray, "MPLS TP Network Management Requirements", draft-gray-mpls-tp-nm-req-01 (work in progress), July 2008.

[I-D.vigoureux-mpls-tp-oam-requirements] Vigoureux, M., Ward, D., and M. Betts, "Requirements for OAM in MPLS Transport Networks", draft-vigoureux-mpls-tp-oam-requirements-00 (work in progress), July 2008.

[I-D.draft-ietf-mpls-mpls-and-gmpls-security-framework] Fang, L. and M. Behringer, "Security Framework for MPLS and GMPLS Networks", draft-ietf-mpls-mpls-and-gmpls-security-framework-03 (work in progress), July 2008.

[ITU.Y2611.2006] International Telecommunications Union, "High-level architecture of future packet-based networks", ITU-T Recommendation Y.2611, December 2006.

[ITU.Y1401.2008] International Telecommunications Union, "Principles of interworking", ITU-T Recommendation Y.1401, February 2008.

[ITU.G805.2000] International Telecommunications Union, "Generic functional architecture of transport networks", ITU-T Recommendation G.805, March 2000.

Authors' Addresses

Ben Niven-Jenkins (editor)
BT
208 Callisto House, Adastral Park
Ipswich, Suffolk IP5 3RE
UK

Email: benjamin.niven-jenkins@bt.com

Deborah Brungard (editor)
AT&T
Rm. D1-3C22 - 200 S. Laurel Ave.
Middletown, NJ 07748
USA

Email: dbrungard@att.com

Malcolm Betts (editor)
Nortel Networks
3500 Carling Avenue
Ottawa, Ontario K2H 8E9
Canada

Email: betts01@nortel.com

Nurit Sprecher
Nokia Siemens Networks
3 Hanagar St. Neve Ne'eman B
Hod Hasharon, 45241
Israel

Email: nurit.sprecher@nsn.com

Full Copyright Statement

Intellectual Property