INTERNET-DRAFT
Intended Status: Informational
Expires: June 16, 2013

L. Fang, Ed.
Cisco
N. Bitar
Verizon
R. Zhang
Alcatel Lucent
M. Daikoku
KDDI
P. Pan
Infinera

December 16, 2012

MPLS-TP Applicability; Use Cases and Design
draft-ietf-mpls-tp-use-cases-and-design-03.txt

Abstract

This document provides applicability, use case studies and network design considerations for the Multiprotocol Label Switching Transport Profile (MPLS-TP). The use cases include Metro Ethernet access and aggregation transport, Mobile backhaul, and packet optical transport.

Table of Contents

1 Introduction

This document provides applicability, use case studies and network design considerations for the Multiprotocol Label Switching Transport Profile (MPLS-TP).

In recent years, the urgency for moving from traditional transport technologies, such as SONET/SDH, TDM, and ATM, to new packet technologies has been rising. This is largely due to the fast growing demand for bandwidth, which has been fueled by the following factors: 1) The growth of new services. This includes: the tremendous success of data services, such as IPTV and IP Video for content downloading, streaming, and sharing; the rapid growth of mobile services, as a consequence of the explosion of smart phone applications; the continued growth of business VPNs and residential broadband services. 2) Network infrastructure evolution. As many legacy transport devices are approaching end of life, Service Providers transition to new packet technologies and evolve their transport network into the next generation packet transport.

As part of MPLS family, MPLS-TP complements existing IP/MPLS technologies; it closes the gaps in the traditional access and aggregation transport to enable end-to-end packet technology solutions in a cost efficient, reliable, and interoperable manner. After several years of industry debate on which packet technology to use, MPLS-TP has emerged as the next generation transport technology of choice for many Service Providers worldwide.

The unified MPLS strategy - using MPLS from core to aggregation and access (e.g. IP/MPLS in the core, IP/MPLS or MPLS-TP in aggregation and access) appear to be very attractive to many SPs. It streamlines the operation, reduces the overall complexity, and improves end-to-end convergence. It leverages the MPLS experience, and enhances the ability to support revenue generating services.

MPLS-TP is a subset of MPLS functions that meet the packet transport requirements defined in [RFC5654]. This subset includes: MPLS data forwarding, pseudo-wire encapsulation for circuit emulation, and dynamic control plane using GMPLS control for LSP and tLDP for pseudo-wire (PW). MPLS-TP also extends previous MPLS OAM functions, such as BFD extension for proactive Connectivity Check and Connectivity Verification (CC-CV) [RFC6428], and Remote Defect Indication (RDI) [RFC6428], LSP Ping Extension for on-demand CC-CV [RFC6426], fault allocation, and remote integrity check. New tools have been defined for alarm suppression with Alarm Indication Signal (AIS) [RFC6427], and switch-over triggering with Link Defect Indication (LDI). Note that since the MPLS OAM feature extensions defined through the process of MPLS-TP development are part of the

MPLS family, the applicability is general to MPLS, and not limited to MPLS-TP.

The requirements of MPLS-TP are provided in MPLS-TP Requirements [RFC 5654], and the architectural framework is defined in MPLS-TP Framework [RFC5921]. This document's intent is to provide the use case studies and design considerations from a practical point of view based on Service Providers deployments plans and actual deployments.

The most common use cases for MPLS-TP include Metro access and aggregation, Mobile Backhaul, and Packet Optical Transport. MPLS-TP data plane architecture, path protection mechanisms, and OAM functionality are used to support these deployment scenarios.

The design considerations discussed in this documents include: role of MPLS-TP in the network; provisioning options; standards compliance; end-to-end forwarding and OAM consistency; compatibility with existing IP/MPLS networks; and optimization vs. simplicity design trade-offs.

2. Terminology

This document uses the terminology and architecture reference defined in MPLS-TP Framework [RFC 5654] and MPLS-TP requirements defined in [RFC 5921].

Term	Definition
2G	2nd Generation Mobile network: GSM/CDMA
3G	3rd Generation Mobile network: UMTS/HSPA/1xEVDO
4G	4th Generation Mobile network: LTE
ADSL	Asymmetric Digital Subscriber Line
AIS	Alarm Indication Signal
ASNGW	Access Service Network Gateway
ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
BTS	Base Transceiver Station
CC-CV	Continuity Check and Connectivity Verification
CDMA	Code Division Multiple Access
E-LINE	Ethernet point-to-point connectivity
E-LAN	Ethernet LAN, provides multipoint connectivity
eNB	Evolved Node B
E-VLAN	Ethernet Virtual Private LAN
EVDO	Evolution-Data Optimized
G-ACh	Generic Associated Channel
GMPLS	Generalized Multi-Protocol Label Switching
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access

IPTV	Internet Protocol television
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LAN	Local Access Network
LDI	Link Down Indication
LDP	Label Distribution Protocol
LSP	Label Switched Path
LTE	Long Term Evolution
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point
NMS	Network Management System
MPLS	MultiProtocol Label Switching
MPLS-TP	MultiProtocol Label Switching Transport Profile
MS-PW	Multi-Segment Pseudowire
OAM	Operations, Administration, and Management
OPEX	Operating Expenses
PE	Provider-Edge device
PSW	Packet Data Network Gateway
RAN	Radio Access Network
RDI	Remote Defect Indication
SDH	Synchronous Digital Hierarchy
SGW	Serving Gateway
SLA	Service Level Agreement
SONET	Synchronous Optical Network
S-PE	PW Switching Provider Edge
SP	Service Provider
SRLG	Shared Risk Link Groups
SS-PW	Single-Segment Pseudowire
TDM	Time Division Multiplexing
tLDP	Targeted Label Distribution Protocol
VPN	Virtual Private Network
UMTS	Universal Mobile Telecommunications System

3. MPLS-TP Use Cases

3.1. Metro Access and Aggregation

The use of MPLS-TP for Metro access and aggregation transport is the most common deployment scenario observed in the field.

Some operators are building green-field access and aggregation transport infrastructure, while others are upgrading/replacing their existing transport infrastructure with new packet technologies. The existing legacy access and aggregation networks are usually based on TDM or ATM technologies. Some operators are replacing these networks with MPLS-TP technologies, since legacy ATM/TDM aggregation and access are becoming inadequate to support the rapid business growth and too expensive to maintain. In addition, in many cases the legacy

devices are facing End of Sale and End of Life issues. As operators must move forward with the next generation packet technology, the adoption of MPLS-TP in access and aggregation becomes a natural choice. The statistical multiplexing in MPLS-TP helps to achieve higher efficiency comparing with the time division scheme in the legacy technologies. MPLS-TP OAM tools and protection mechanisms help to maintain high reliability of transport network and achieve fast recovery.

As most Service Providers core networks are MPLS enabled, extending the MPLS technology to the aggregation and access transport networks with a Unified MPLS strategy is very attractive to many Service Providers. Unified MPLS strategy in this document means having end-to-end MPLS technologies through core, aggregation, and access. It reduces OPEX by streamlining operation and leveraging the operational experience already gained with MPLS technologies; it also improves network efficiency and reduces end-to-end convergence time.

The requirements from the SPs for ATM/TDM aggregation replacement often include: i) maintaining the previous operational model, which means providing a similar user experience in NMS, ii) supporting the existing access network, (e.g., Ethernet, ADSL, ATM, TDM, etc.), and connections with the core networks, and iii) supporting the same operational capabilities and services (L3VPN, L2VPN, E-LINE/E-LAN/E-VLAN, Dedicated Line, etc.). MPLS-TP can meet these requirements and in general the requirements defined in [RFC5654] to support a smooth transition.

3.2. Packet Optical Transport

Many SP's transport networks consist of both packet and optical portions. The transport operators are typically sensitive to network deployment cost and operational simplicity. MPLS-TP supports both static provisioning through NMS and dynamic provisioning via the GMPLS control plane. As such, it is viewed as a natural fit in some of the transport networks, where the operators can utilize the MPLS-TP LSP's (including the ones statically provisioned) to manage user traffic as "circuits" in both packet and optical networks, and when they are ready, move to dynamic control plane for greater efficiency.

Among other attributes, bandwidth management, protection/recovery and OAM are critical in Packet/Optical transport networks. In the context of MPLS-TP, each LSP is expected to be associated with a fixed amount of bandwidth in terms of bits-per-second and/or time-slots. OAM is to be performed on each individual LSP. For some of the performance monitoring (PM) functions, the OAM mechanisms need to be able to transmit and process OAM packets at very high frequency. An overview of MPLS-TP OAM toolset is found in [RFC6669].

Protection [RFC6372] is another important element in transport networks. Typically, ring and linear protection can be readily applied in metro networks. However, as long-haul networks are sensitive to bandwidth cost and tend to have mesh-like topology, shared mesh protection is becoming increasingly important.

In some cases, SPs plan to deploy MPLS-TP from their long haul optical packet transport all the way to the aggregation and access in their networks.

3.3. Mobile Backhaul

Wireless communication is one of the fastest growing areas in communication worldwide. In some regions, the tremendous mobile growth is fueled by the lack of existing land-line and cable infrastructure. In other regions, the introduction of smart phones is quickly driving mobile data traffic to become the primary mobile bandwidth consumer (some SPs have already observed more than 85% of total mobile traffic are data traffic). MPLS-TP is viewed as a suitable technology for Mobile backhaul.

3.3.2. 2G and 3G Mobile Backhaul

MPLS-TP is commonly viewed as a very good fit for 2G/3G Mobile backhaul. 2G (GSM/CDMA) and 3G (UMTS/HSPA/1xEVDO) Mobile Backhaul Networks are still currently dominating the mobile infrastructure.

The connectivity for 2G/3G networks is point to point (P2P). The logical connections are hub-and-spoke. Networks are physically constructed using a star or ring topology. In the Radio Access Network (RAN), each mobile Base Transceiver Station (BTS/Node B) is communicating with a Radio Controller (BSC/RNC). These connections are often statically set up.

Hierarchical or centralized architectures are often used for pre-aggregation and aggregation layers. Each aggregation network inter-connects with multiple access networks. For example, a single aggregation ring could aggregate traffic for 10 access rings with total 100 base stations.

The technology used today is largely ATM based. Mobile providers are replacing the ATM RAN infrastructure with newer packet technologies. IP RAN networks with IP/MPLS technologies are deployed today by many SPs with great success. MPLS-TP is another suitable choice for Mobile RAN. The P2P connections from base station to Radio Controller can be set statically to mimic the operation of today's RAN environments; in-band OAM and deterministic path protection can support fast failure detection and switch-over to satisfy the SLA agreements.

Bidirectional LSPs may help to simplify the provisioning process. The deterministic nature of MPLS-TP LSP set up can also support packet based synchronization to maintain predictable performance regarding packet delay and jitters.

3.3.2. 4G/LTE Mobile Backhaul

One key difference between LTE and 2G/3G Mobile networks is that the logical connection in LTE is a mesh, while in 2G/3G is a P2P star. In LTE, the base stations eNB/BTS communicate with multiple Network controllers (PSW/SGW or ASNGW), and the radio elements communicate with one another for signal exchange and traffic offload to wireless or wireline infrastructures.

IP/MPLS has a great advantage in any-to-any connectivity environment. Thus, the use of mature IP or L3VPN technologies is particularly common in the design of SP's LTE deployment plans.

The extended OAM functions defined in MPLS-TP, such as in-band OAM and path protection mechanisms bring additional advantages to support SLAs. The dynamic control-plane with GMPLS signaling is especially suited for the mesh environment, to support dynamic topology changes and network optimization.

5. Network Design Considerations

5.1. The role of MPLS-TP

The role of MPLS-TP is to provide a solution to help evolving traditional transport towards packet. It is designed to support the transport characteristics/behavior described in [RFC5654]. The primary use of MPLS-TP is largely to replace legacy transport technologies, such as SONET/SDH. MPLS-TP is not designed to replace the service support capabilities of IP/MPLS, such as L2VPN, L3VPN, IPTV, Mobile RAN, etc.

5.2 Provisioning mode

MPLS-TP supports two provisioning modes: i) a mandatory static provisioning mode, which must be supported without dependency on dynamic routing or signaling; and ii) an optional distributed dynamic control plane, which is used to enable dynamic service provisioning.

The decision on which mode to use is largely dependent on the operational feasibility and the stage of evolution transition. Operators who are accustomed with the transport-centric operational

model (e.g., NMS configuration without control plane) typically prefer the static provisioning mode. This is the most common choice in current deployments. The dynamic provisioning mode can be more powerful but it is more suited for operators who are familiar with the operation and maintenance of IP/MPLS technologies or ready to step up through training and planned transition.

There may be also cases where operators choose to use the combination of both modes. This is appropriate when parts of the network are provisioned in a static fashion and other parts are controlled by dynamic signaling. This combination may also be used to transition from static provisioning to dynamic control plane.

5.3. Standards compliance

It is generally recognized by SPs that standards compliance is important for lowering cost, accelerating product maturity, achieving multi-vendor interoperability, and meeting the expectations of their enterprise customers.

MPLS-TP is a joint work between IETF and ITU-T. In April 2008, IETF and ITU-T jointly agreed to terminate T-MPLS and progress MPLS-TP as joint work [RFC5317]. The transport requirements are provided by ITU-T, the protocols are developed in IETF.

5.4. End-to-end MPLS OAM consistency

End-to-end MPLS OAM consistency is highly desirable in order to enable Service Providers to deploy end-to-end MPLS solution with a combination of IP/MPLS (for example, in the core including service edge) and MPLS-TP (for example, in the aggregation/access networks). Using MPLS based OAM in MPLS-TP can help achieving such a goal.

5.5. PW Design considerations in MPLS-TP networks

In general, PWs in MPLS-TP work the same as in IP/MPLS networks. Both Single-Segment PW (SS-PW) and Multi-Segment PW (MS-PW) are supported. For dynamic control plane, Targeted LDP (tLDP) is used. In static provisioning mode, PW status is a new PW OAM feature for failure notification. In addition, both directions of a PW must be bound to the same transport bidirectional LSP.

In the common network topology involving multi-tier rings, the design choice is between using SS-PW or MS-PW. This is not a discussion unique to MPLS-TP, as it applies to PW design in general, but it is relevant here, since MPLS-TP is more sensitive to the operational complexities, as noted by operators. If MS-PW is used, Switched PE (S-PE) must be deployed to connect the rings. The advantage of this

choice is that it provides domain isolation, which in turn facilitates trouble shooting and allows for faster PW failure recovery. On the other hand, the disadvantage of using S-PE is that it adds more complexity. Using SS-PW is simpler, since it does not require S-PEs, but less efficient because the paths across primary and secondary rings are longer. If operational simplicity is a higher priority, some SPs choose the latter.

Another design trade-off is whether to use PW protection in addition to LSP protection or rely solely on LSP protection. By definition, MPLS-TP LSPs are protected. If the working LSP fails, the protect LSP assures that the connectivity is maintained and the PW is not impacted. However, in the case of simultaneous failure of both working and protect LSPs, the attached PW would fail. By adding PW protection, and attaching the protect PW to a diverse LSP not in the same Shared Risk Link Group (SRLG), the PW is protected even when the primary PW fails. Clearly, using PW protection adds considerably more complexity and resource usage, and thus operators often may choose not to use it, and consider protection against single point of failure as sufficient.

5.6. Proactive and on-demand MPLS-TP OAM tools

MPLS-TP provide both proactive and on-demand OAM Tools. As a proactive OAM fault management tool, BFD hellos can be sent at regular intervals for Connectivity Check; 3 missed hellos trigger the failure protection switch-over. BFD sessions are configured for both working and protecting LSPs.

A design decision is choosing the value of the BFD hello interval. The shorter the interval (3.3ms is the minimum allowed interval), the faster the detection time is, but also the higher the resource utilization is. The proper value depends on the application and the service needs.

As an on-demand OAM fault management mechanism, for example when there is a fiber cut, Link Down Indication (LDI) message [RFC6427] is generated from the failure point and propagated to the Maintenance End Points (MEPs) to trigger immediate switch-over from working to protect path. An Alarm Indication Signal (AIS) propagates from the Maintenance Intermediate Point (MIP) to the MEPs for alarm suppression.

In general, both proactive and on-demand OAM tools should be enabled to guarantee short switch-over times.

5.7. MPLS-TP and IP/MPLS Interworking considerations

Since IP/MPLS is largely deployed in most SPs' networks, MPLS-TP and IP/MPLS interworking is a reality.

The interworking issues are addressed in a separate document [Interworking].

6. Security Considerations

In the use case of Metro access and aggregation, in the scenario where some of the access equipment is placed in facilities not owned by the SP, the static provisioning mode of MPLS-TP is often preferred over the control plane option because it eliminates the possibility of a control plane attack which may potentially impact the whole network.

Similar location issues apply to the mobile use cases, since equipment is often placed in remote and outdoor environment, which can increase the risk of un-authorized access to the equipment.

In general, NMS access can be a common point of attack in all MPLS-TP use cases. General security considerations for MPLS and GMPLS networks are addressed in Security Framework for MPLS and GMPLS Networks [RFC5920]. General MPLS-TP security considerations are described in MPLS-TP Security Framework [MPLS-TP Sec FW].

7. IANA Considerations

This document contains no new IANA considerations.

8. Acknowledgements

The authors wish to thank Adrian Farrel for his review as Routing Area Director, Adrian's detailed comments were of great help for improving the quality of this document. The authors would also like to thank Loa Andersson for his continued support and guidance.

9. References

9.1 Normative References

[RFC5317] Bryant, S., Ed., and L. Andersson, Ed., "Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile", RFC 5317, February 2009.

[RFC5654] Niven-Jenkins, B., Ed., Brungard, D., Ed., Betts, M., Ed., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS Networks", RFC 5920, July 2010.

[RFC6426] Gray, E., Bahadur, N., Boutros, S., and R. Aggarwal, "MPLS On-Demand Connectivity Verification and Route Tracing", RFC 6426, November 2011.

[RFC6427] Swallow, G., Ed., Fulignoli, A., Ed., Vigoureux, M., Ed., Boutros, S., and D. Ward, "MPLS Fault Management Operations, Administration, and Maintenance (OAM)", RFC 6427, November 2011.

[RFC6428] Allan, D., Ed., Swallow Ed., G., and J. Drake Ed., "Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile", RFC 6428, November 2011.

9.2 Informative References

[RFC5921] Bocci, M., Ed., Bryant, S., Ed., Frost, D., Ed., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks", RFC 5921, July 2010.

[RFC6372] Sprecher, N., Ed., and A. Farrel, Ed., "MPLS Transport Profile (MPLS-TP) Survivability Framework", RFC 6372, September 2011.

[RFC6669] Sprecher, N. and L. Fang, "An Overview of the Operations, Administration, and Maintenance (OAM) Toolset for MPLS-Based Transport Networks", RFC 6669, July 2012.

[Interworking] Martinotti, R., et al., "Interworking between MPLS-TP and IP/MPLS," draft-martinotti-mpls-tp-interworking-02.txt, June 2011.

[MPLS-TP Sec FW] Fang, L. ED., et al., "MPLS-TP Security Framework," draft-ietf-mpls-tp-security-framework-05.txt, October 2012.

Authors' Addresses

Luyuan Fang
Cisco Systems, Inc.
111 Wood Ave. South
Iselin, NJ 08830
United States
Email: lufang@cisco.com

Nabil Bitar
Verizon
40 Sylvan Road
Waltham, MA 02145
United States
Email: nabil.bitar@verizon.com

Raymond Zhang
Alcatel-Lucent
701 Middlefield Road
Mountain View, CA 94043
United States
Email: raymond.zhang@alcatel-lucent.com

Masahiro DAIKOKU
KDDI corporation
3-11-11.Iidabashi, Chiyodaku, Tokyo
Japan
Email: ms-daikoku@kddi.com

Ping Pan
Infinera
United States
Email: ppan@infinera.com

Contributors' Address

Kam Lee Yap
XO Communications
13865 Sunrise Valley Drive,
Herndon, VA 20171
United States
Email: klyap@xo.com

Dan Frost
Cisco Systems, Inc.
United Kingdom
Email:danfrost@cisco.com

Henry Yu
TW Telecom
10475 Park Meadow Dr.
Littleton, CO 80124
United States
Email: henry.yu@twtelecom.com

Jian Ping Zhang   China Telecom, Shanghai
Room 3402, 211 Shi Ji Da Dao

Pu Dong District, Shanghai
China
Email: zhangjp@shtel.com.cn

Lei Wang
Lime Networks
Strandveien 30, 1366 Lysaker
Norway
Email: lei.wang@limenetworks.no

Mach(Guoyi) Chen
Huawei Technologies Co., Ltd.
No. 3 Xinxi Road
Shangdi Information Industry Base
Hai-Dian District, Beijing 100085
China
Email: mach@huawei.com

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