Internet Engineering Task Force (IETF)
Request for Comments: 6941
Category: Informational
ISSN: 2070-1721

L. Fang, Ed.
Cisco
B. Niven-Jenkins, Ed.
Velocix
S. Mansfield, Ed.
Ericsson
R. Graveman, Ed.
RFG Security

April 2013

MPLS Transport Profile (MPLS-TP) Security Framework

Abstract

This document provides a security framework for the MPLS Transport Profile (MPLS-TP). MPLS-TP extends MPLS technologies and introduces new Operations, Administration, and Maintenance (OAM) capabilities, a transport-oriented path protection mechanism, and strong emphasis on static provisioning supported by network management systems. This document addresses the security aspects relevant in the context of MPLS-TP specifically. It describes potential security threats as well as mitigation procedures related to MPLS-TP networks and to MPLS-TP interconnection to other MPLS and GMPLS networks. This document is built on RFC 5920 ("Security Framework for MPLS and GMPLS Networks") by providing additional security considerations that are applicable to the MPLS-TP extensions. All the security considerations from RFC 5920 are assumed to apply.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunication Union Telecommunication 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 functionality of a packet transport network.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document provides a security framework for the MPLS Transport Profile (MPLS-TP).

As defined in "Requirements of an MPLS Transport Profile" [RFC5654] and "A Framework for MPLS in Transport Networks" [RFC5921], MPLS-TP uses a subset of MPLS features and introduces extensions to reflect the characteristics of the transport technology. The additional functionality includes in-band OAM, transport-oriented path protection and recovery mechanisms, and new OAM capabilities that were developed for MPLS-TP but that also apply to MPLS and GMPLS. There is strong emphasis in MPLS-TP on static provisioning support through Network Management Systems (NMSs) or Operational Support Systems (OSSs).

This document is built on [RFC5920] by providing additional security considerations that are applicable to the MPLS-TP extensions. The security models, threats, and defense techniques previously defined in [RFC5920] are assumed to apply to general aspects of MPLS-TP.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunication Union Telecommunication Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionality of a packet transport network.

Readers can refer to [RFC5654] and [RFC5921] for MPLS-TP terminologies and to [RFC5920] for security terminologies that are relevant to MPLS and GMPLS.

1.1. Terminology

Term	Definition
AC	Attachment Circuit
BFD	Bidirectional Forwarding Detection
CE	Customer Edge
DoS	Denial of Service
G-ACh	Generic Associated Channel
GAL	G-ACh Label
GMPLS	Generalized Multiprotocol Label Switching
IP	Internet Protocol
LDP	Label Distribution Protocol
LSP	Label Switched Path
NMS	Network Management System
MPLS	Multiprotocol Label Switching
MPLS-TP	MPLS Transport Profile

MS-PW	Multi-Segment Pseudowire
OAM	Operations, Administration, and Maintenance
PE	Provider Edge
PSN	Packet-Switched Network
PW	Pseudowire
S-PE	PW Switching Provider Edge
SP	Service Provider
SS-PW	Single-Segment Pseudowire
T-PE	PW Terminating Provider Edge

2. Security Reference Models

This section defines reference models for security in MPLS-TP networks.

The models are built on the architecture of MPLS-TP, as defined in [RFC5921]. The placement of SP boundaries plays an important role in determining the security models for any particular deployment.

This document defines a trusted zone as being where a single SP has total operational control over that part of the network. A primary concern is about security aspects that relate to breaches of security from the "outside" of a trusted zone to the "inside" of this zone.

2.1. Security Reference Model 1

In reference model 1, a single SP has total control of the "PE/T-PE to PE/T-PE" part of the MPLS-TP network.

Security reference model 1(a) shows an MPLS-TP network with Single-Segment Pseudowire (SS-PW) from PE1 to PE2. The trusted zone is PE1 to PE2, as illustrated in Figure 1.

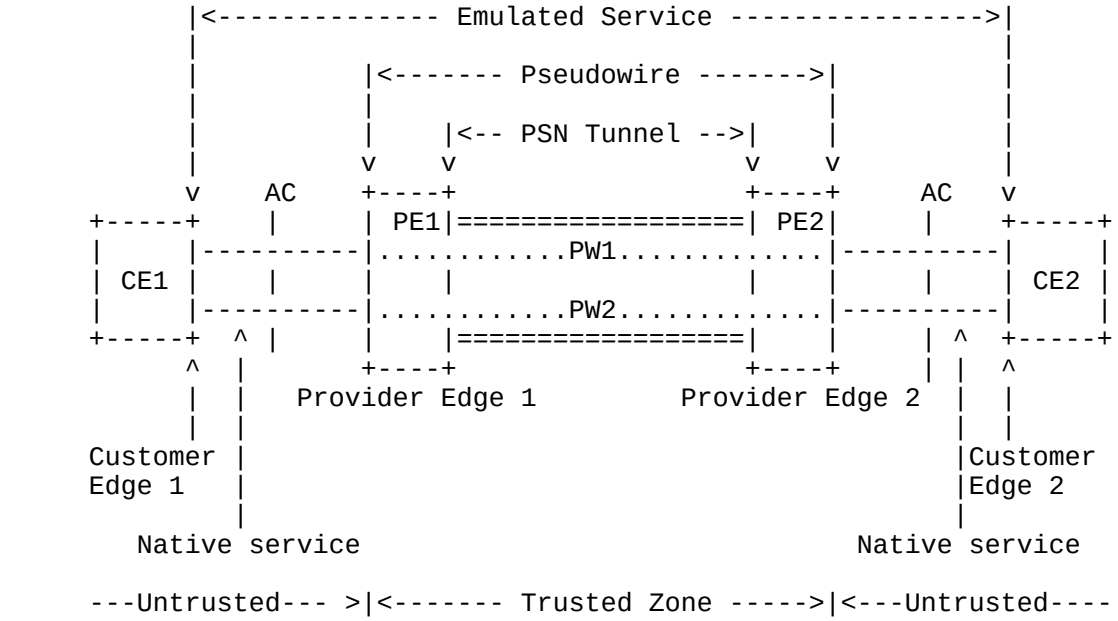

Figure 1. MPLS-TP Security Model 1(a)

Security reference model 1(b) shows an MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE1 to T-PE2. The trusted zone is T-PE1 to T-PE2, as illustrated in Figure 2.

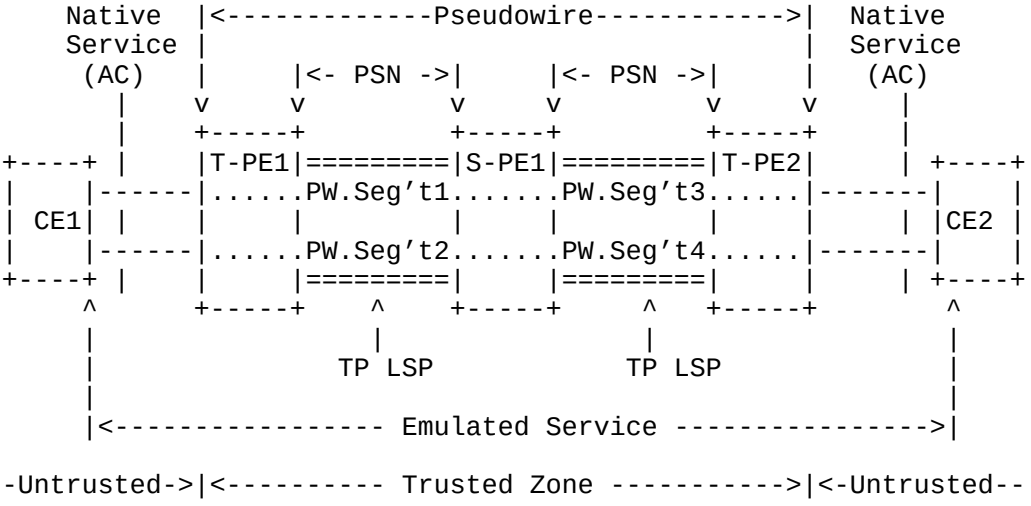

Figure 2. MPLS-TP Security Model 1(b)

2.2. Security Reference Model 2

In reference model 2, a single SP does not have the end-to-end control of the segment from PE/T-PE to PE/T-PE. A given S-PE or T-PE may be under the control of another SP, that SP's customers, or its partners. In this case, the MPLS-TP network is not contained within a single trusted zone.

Security reference model 2(a) shows an MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE1 to T-PE2. The trusted zone is T-PE1 to S-PE1, as illustrated in Figure 3.

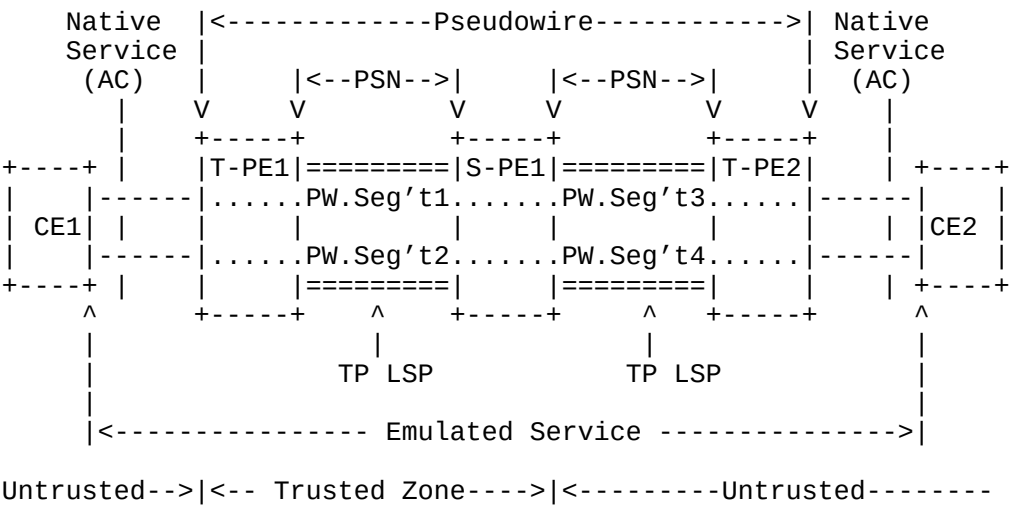

Figure 3. MPLS-TP Security Model 2(a)

Security reference model 2(b) shows an MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE1 to T-PE2. The trusted zone is the S-PE1 only, as illustrated in Figure 4.

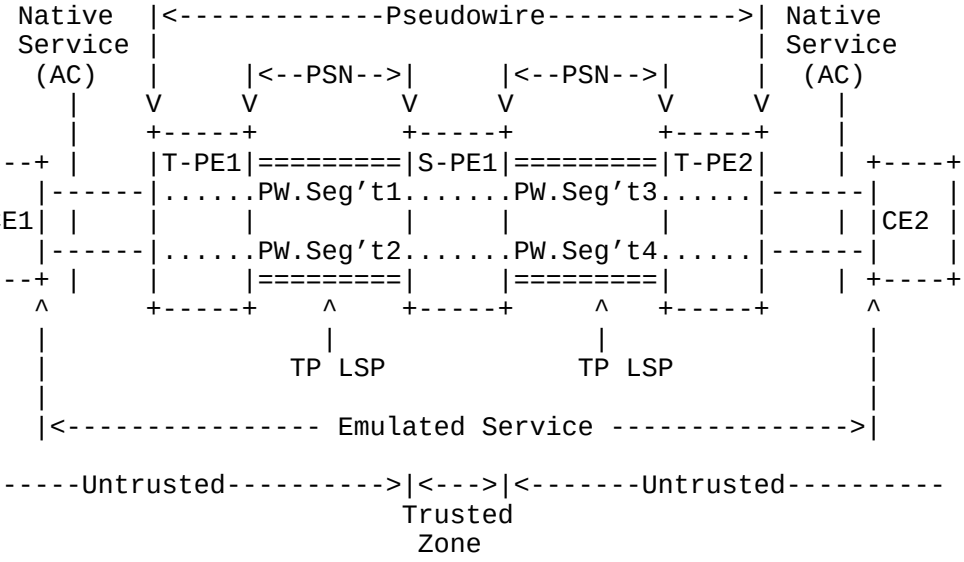

Figure 4. MPLS-TP Security Model 2(b)

Security reference model 2(c) shows an MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from different SPs with inter-provider PW connections. The trusted zone is T-PE1 to S-PE3, as illustrated in Figure 5.

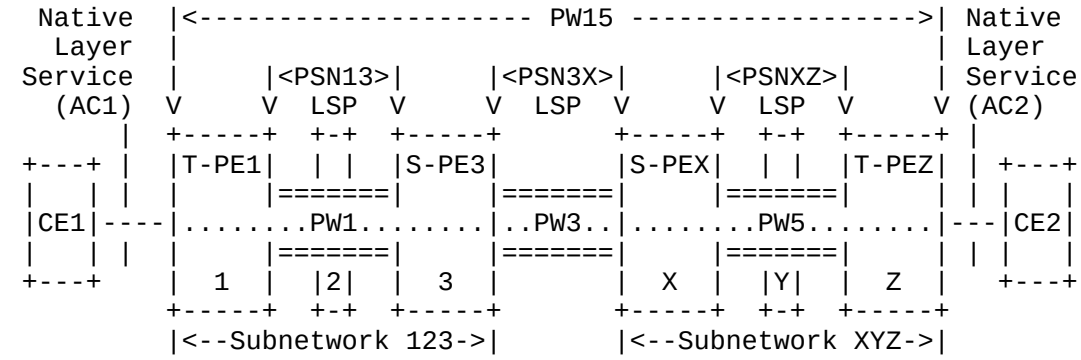

Figure 5. MPLS-TP Security Model 2(c)

In general, the boundaries of a trusted zone must be carefully defined when analyzing the security properties of each individual network. The security boundaries determine which reference model should be applied to a given network topology.

3. Security Threats

This section discusses various network security threats that are unique to MPLS-TP and may endanger MPLS-TP networks.

Attacks against a GAL or G-ACh may include the following:

- GAL or BFD label manipulation, which includes insertion of false labels and modification, deletion, or replay of messages.

- DoS attacks through in-band OAM by generating excessive G-ACh/GAL and BFD messages that consume significant bandwidth and potentially cause congestion.

These attacks can cause unauthorized protection switchover, inability to restore one or more LSPs, or loss of network connectivity.

When an NMS is used for LSP setup, attacks on the NMS can cause the above effects as well. Although this is not unique to MPLS-TP, MPLS-TP networks can be particularly vulnerable to NMS attacks, due to the fact that static provisioning through NMSs is a commonly used model. In the static provisioning model, a compromised NMS can potentially be comparable to a compromised control plane plus a compromised management plane in the dynamic controlled network model.

Attacks on NMSs may come from either external attackers or insiders. Outside attacks are initiated outside of the trusted zone by unauthorized users of the MPLS-TP NMSs. Insider attacks are initiated from inside the trusted zone by an entity that has authorized access to the management systems but that performs unapproved functions that are harmful to the MPLS-TP networks. These attacks may directly target the NMS; they may also take place via the compromised communication channels between the NMS and the network devices that are being provisioned, or through user access to the provisioning tools. This type of security threat may include disclosure of information, generating false OAM messages, taking down MPLS-TP LSPs, connecting to the wrong MPLS-TP tunnel endpoints, and DoS attacks on the MPLS-TP networks.

There are other more generic security threats, such as unauthorized observation of data traffic (including traffic pattern analysis), modification or deletion of a provider’s or user’s data, and replay or insertion of inauthentic data into a provider’s or user’s data

stream. These types of attacks apply to MPLS-TP traffic regardless of how the LSP or PW is set up, in a way that is similar to how they apply to MPLS traffic regardless of how the LSP is set up. More details on the above-mentioned threats are documented in [RFC5920].

Such threats may result from malicious behavior or accidental errors:

Example 1: Attacks from users: Users of the MPLS-TP network may attack the network infrastructure or attack other users.

Example 2: Attacks from insiders: Employees of the operators may attack the MPLS-TP network, especially through NMSs.

Example 3: Attacks from interconnecting SPs or other partners: Other SPs may attack the MPLS-TP network, particularly through the inter-provider connections.

Example 4: Attacks as the result of operational errors: Operations staff may fail to follow operational procedures or may make operational mistakes.

4. Defensive Techniques

The defensive techniques presented in this document and in [RFC5920] are intended to describe methods by which some security threats can be addressed. They are not intended as requirements for all MPLS-TP deployments. The specific operational environment determines the security requirements for any instance of MPLS-TP. Therefore, protocol designers should provide a full set of security capabilities that can be selected and used where appropriate. The MPLS-TP provider should determine the applicability of these techniques to the provider’s specific service offerings, and the end user may wish to assess the value of these techniques to the user’s service requirements.

Authentication is the primary defense technique to mitigate the risk of the MPLS-TP security threats discussed in Section 3 (GAL or BFD label manipulation, and DoS attacks through in-band OAM). Authentication refers to methods to ensure that message sources are properly identified by the MPLS-TP devices with which they communicate. Authentication includes the following:

- entity authentication for identity verification

- management system authentication

- peer-to-peer authentication

- message integrity and replay detection to ensure the validity of message streams

- network-based access controls such as packet filtering and firewalls

- host-based access controls

- isolation

- aggregation

- protection against denial of service

- event logging

Section 5.2 of [RFC5920] describes these techniques where they apply to MPLS and GMPLS in general.

In addition to authentication, the following defense should also be considered in order to protect MPLS-TP networks:

- Use of isolated infrastructure for MPLS-TP

One way to protect the MPLS-TP infrastructure is to use dedicated network resources to provide MPLS-TP transport services. For example, in security model 2 (Section 2.2), the potential risk of attacks on the S-PE1 or T-PE1 in the trusted zone may be reduced by using non-IP-based communication paths, so that the paths in the trusted zone cannot be reached from the outside via IP.

- Verification of connectivity

To protect against deliberate or accidental misconnection, mechanisms can be put in place to verify both end-to-end connectivity and segment-by-segment resources. These mechanisms can trace the routes of LSPs in both the control plane and the data plane. Note that the connectivity verification tools are now developed for general MPLS networks as well.

The defense techniques that apply generally to MPLS/GMPLS are not detailed here; see [RFC5920] for details regarding these techniques. For example:

1) Authentication, including management system authentication, peer-to-peer authentication, and cryptographic techniques for authenticating identity

2) Access control techniques

3) Use of aggregated infrastructure

4) Mitigation of denial-of-service attacks

5) Monitoring, detection, and reporting of security attacks

It is important to point out the following security defense techniques, as they are particularly critical for NMSs, due to the strong emphasis on static provisioning supported by NMSs in MPLS-TP deployments. These techniques include the following:

- entity authentication for identity verification

- encryption for confidentiality

- message integrity and replay detection to ensure the validity of message streams

- user access control and event logging, which must be applied for NMSs and provisioning applications

5. Security Considerations

Security considerations constitute the sole subject of this document and hence are discussed throughout.

This document evaluates security risks specific to MPLS-TP, as well as mitigation mechanisms that may be used to counter potential threats. All of the techniques presented here involve mature and widely implemented technologies that are practical to implement. It is meant to assist equipment vendors and service providers who must ultimately decide what threats to protect against in any given configuration or service offering, from a customer’s perspective as well as from a service provider’s perspective.

6. Acknowledgements

The authors wish to thank the following people: Joel Halpern and Gregory Mirsky for their review comments and contributions to this document, Mach Chen for his review and suggestions, Adrian Farrel for his Routing Area Director review and detailed comments, Loa Andersson for his continued support and guidance as the MPLS WG co-chair, and Dan Romascanu and Barry Leiba for their helpful comments during IESG review.

7. References

7.1. Normative References

[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.

7.2. 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.

Contributors

Raymond Zhang
Alcatel-Lucent
750D Chai Chee Road
Singapore 469004

EMail: raymond.zhang@alcatel-lucent.com

Nabil Bitar
Verizon
40 Sylvan Road
Waltham, MA 02145
US

EMail: nabil.bitar@verizon.com

Masahiro Daikoku
KDDI Corporation
3-11-11 Iidabashi, Chiyodaku, Tokyo
Japan

EMail: ms-daikoku@kddi.com

Lei Wang
Lime Networks
Strandveien 30, 1366 Lysaker
Norway

EMail: lei.wang@limenetworks.no

Henry Yu
TW Telecom
10475 Park Meadow Drive
Littleton, CO 80124
US

EMail: henry.yu@twtelecom.com

Authors' Addresses

Luyuan Fang (editor)
Cisco Systems
111 Wood Ave. South
Iselin, NJ 08830
US

EMail: lufang@cisco.com

Ben Niven-Jenkins (editor)
Velocix
326 Cambridge Science Park
Milton Road
Cambridge CB4 0WG
UK

EMail: ben@niven-jenkins.co.uk

Scott Mansfield (editor)
Ericsson
300 Holger Way
San Jose, CA 95134
US

EMail: scott.mansfield@ericsson.com

Richard F. Graveman (editor)
RFG Security, LLC
15 Park Avenue
Morristown, NJ 07960
US

EMail: rfg@acm.org