INTERNET-DRAFT   L. Fang, Ed.
Intended Status: Informational   Cisco
Expires: July 20, 2013   B. Niven-Jenkins, Ed.
                                                          Velocix
                                                S. Mansfield, Ed.
                                                         Ericsson
                                                R. Graveman, Ed.
                                                     RFG Security

                                                January 20, 2013

                      MPLS-TP Security Framework
                  draft-ietf-mpls-tp-security-framework-07

Abstract

   This document provides a security framework for Multiprotocol Label
   Switching Transport Profile (MPLS-TP). MPLS-TP extends MPLS
   technologies and introduces new 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, security
   requirements for MPLS-TP, and mitigation procedures for MPLS-TP
   networks and MPLS-TP interconnection to other MPLS and GMPLS
   networks. This document is built on RFC5920 "MPLS and GMPLS MPLS and
   GMPLS security framework" by providing additional security
   considerations which are applicable to the MPLS-TP extensions. All
   the security considerations from RFC5920 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 PWE3 architectures to support the
   capabilities and functionality of a packet transport network.

Status of this Memo

and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1. Introduction

This document provides a security framework for Multiprotocol Label Switching Transport Profile (MPLS-TP).

As defined in MPLS-TP Requirements [RFC5654] and MPLS-TP Framework [RFC5921], MPLS-TP uses a subset of MPLS features and introduces extensions to reflect the characteristics of the transport technology. The additional functionalities include in-band OAM, transport-oriented path protection and recovery mechanisms, and new OAM capabilities developed for MPLS-TP but apply to general MPLS and GMPLS. There is strong emphasis in MPLS-TP on static provisioning support through network management systems (NMS) or Operation Support Systems (OSS).

This document is built on RFC 5920 by providing additional security considerations which are applicable to the MPLS-TP extensions. The security models, threats, requirements, and defense techniques previously defined in [RFC5920] are assumed to apply to general aspect 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 [RFC5920] for security terminologies which are relevant to MPLS and GMPLS.

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 defined in [RFC5921]. The placement of Service Provider (SP) boundaries plays 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) An MPLS-TP network with Single Segment Pseudowire (SS-PW) from PE to PE. The trusted zone is PE1 to PE2 as illustrated in Figure 1.

```
         |<------------- Emulated Service --------------->|
         |                                                |
         |              |<------- Pseudo Wire ------>|    |
         |              |                            |    |
         |              |    |<-- PSN Tunnel -->|    |    |
         |              v    v                  v    v    |
         v    AC     +----+                  +----+   AC  v
   +-----+    |      | PE1|==================| PE2|   |   +-----+
   |     |----------|...........PW1..............|----------|   |
   | CE1 |    |      |    |                  |    |   |   | CE2 |
   |     |----------|...........PW2..............|----------|   |
   +-----+  ^ |     |    |==================|    |   | ^ +-----+
        ^   |       +----+                  +----+   | | ^
        |   |    Provider Edge 1      Provider Edge 2 | |
        |   |                                         | |
     Customer |                                  |Customer
     Edge 1   |                                  |Edge 2
              |                                  |
        Native service                     Native service

   ---Untrusted--- >|<------- Trusted Zone ----->|<---Untrusted----
```
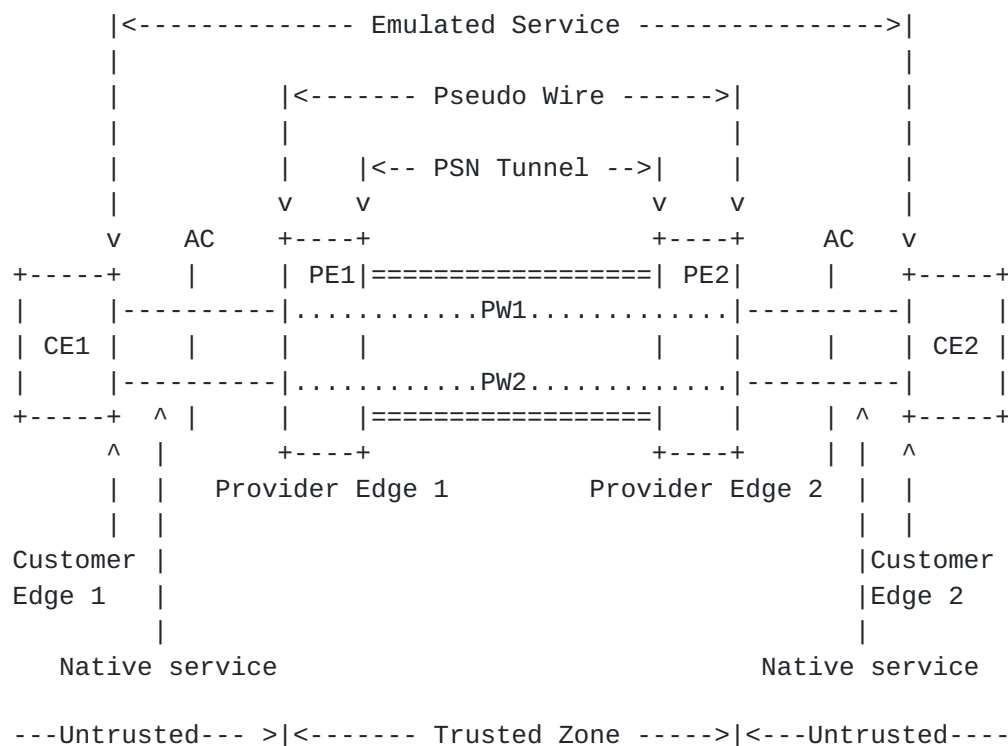
                   Figure 1. MPLS-TP Security Model 1(a)

Security reference model 1(b)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE to
T-PE. The trusted zone is T-PE1 to T-PE2 in Figure 2.

```
         Native  |<------------Pseudowire---------->| Native
         Service |                                  | Service
          (AC)   |    |<- PSN ->|    |<- PSN ->|     |   (AC)
             |   v    v         v    v         v    v    |
             |   +----+         +----+         +----+    |
     +----+  |   |TPE1|=========|SPE1|=========|TPE2|    | +----+
     |    |------|.....PW.Seg't1......PW.Seg't3.....|-------|    |
     | CE1|  |   |    |         |    |         |    |    |   |CE2 |
     |    |------|.....PW.Seg't2......PW.Seg't4.....|-------|    |
     +----+  |   |    |=========|    |=========|    |    | +----+
         ^       +----+    ^    +----+    ^    +----+        ^
         |                 |              |                  |
         |              TP LSP         TP LSP                |
         |                                                   |
         |<---------------- Emulated Service -------------->|

     -- Untrusted->|<--------- Trusted Zone --------->|<-Untrusted--
```
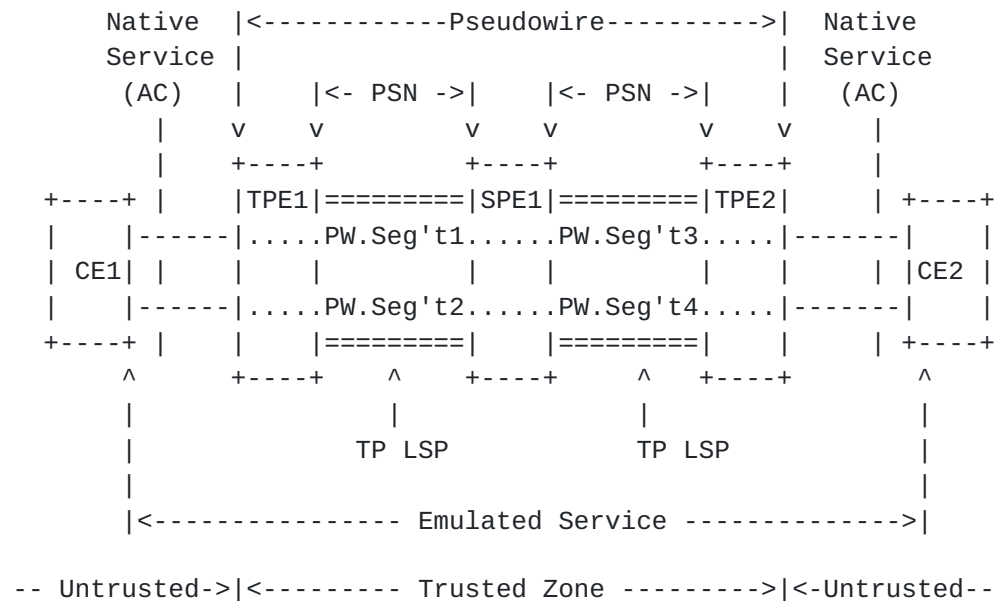
                   Figure 2. MPLS-TP Security Model 1(b)

2.2. Security Reference Model 2

In reference model 2, a single SP does not have total control of the
PE/T-PE to PE/T-PE part of the MPLS-TP network. S-PE and T-PE may be
under the control of different SPs, or their customers or may not be
trusted for some other reason. The MPLS-TP network is not contained
within a single trusted zone.

Security Reference Model 2(a)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE to
T-PE. The trusted zone is T-PE1 to S-PE, as illustrated in Figure 3.

```
        Native  |<------------Pseudowire---------->| Native
        Service |                                  | Service
         (AC)   |    |<--PSN-->|     |<--PSN-->|    |  (AC)
          |     V    V         V     V         V    V   |
          |     +----+         +----+         +----+    |
   +----+ |     |TPE1|=========|SPE1|=========|TPE2|    | +----+
   |    |-------|.....PW.Seg't1......PW.Seg't3.....|------|    |
   | CE1| |     |    |         |    |         |    |      | |CE2 |
   |    |-------|.....PW.Seg't2......PW.Seg't4.....|------|    |
   +----+ |     |    |=========|     |=========|    |     | +----+
       ^       +----+    ^     +----+    ^    +----+       ^
       |                 |               |                |
       |               TP LSP          TP LSP             |
       |                 |               |                |
       |<--------------- Emulated Service ------------->|

   -- Untrusted-->|<-- Trusted Zone-->|<---------Untrusted--------
```
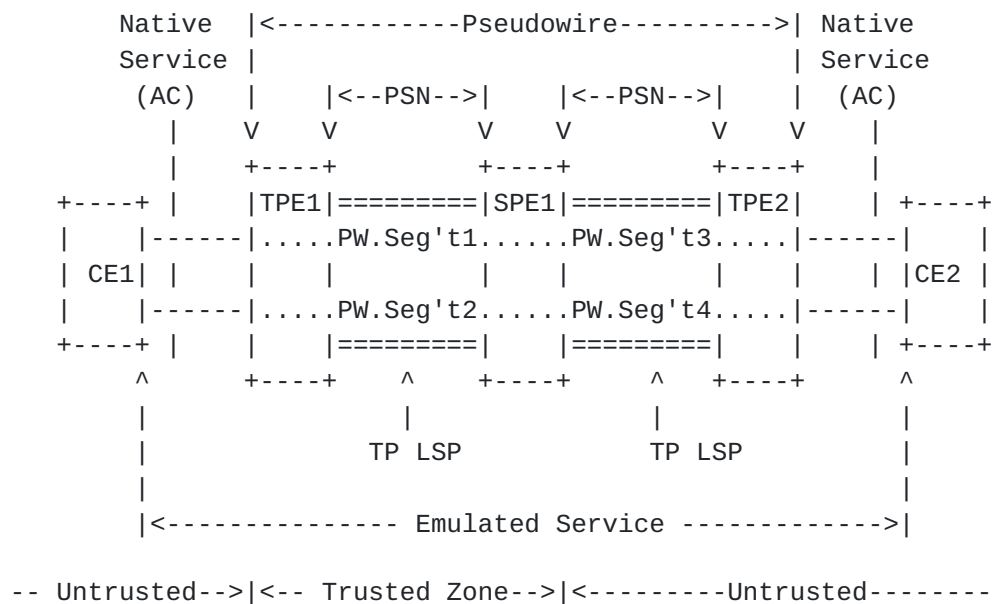
                Figure 3. MPLS-TP Security Model 2(a)

Security Reference Model 2(b)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE to
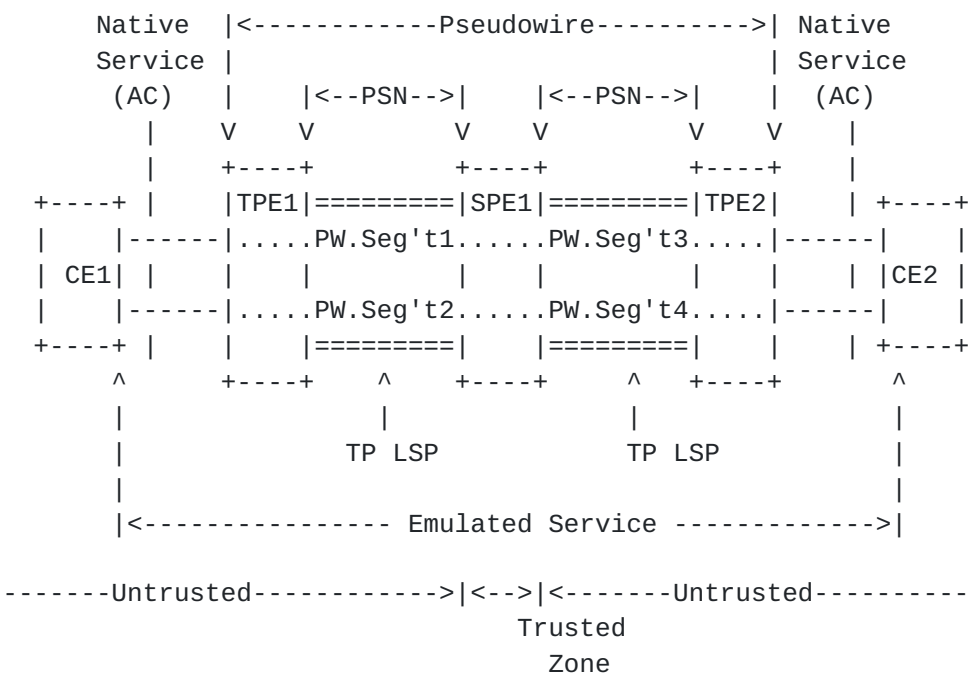T-PE. The trusted zone is the S-PE, as illustrated in Figure 4.

```
        Native  |<------------Pseudowire---------->| Native
        Service |                                  | Service
         (AC)   |    |<--PSN-->|    |<--PSN-->|     |  (AC)
           |    V    V         V    V         V     V    |
           |    +----+         +----+         +----+     |
  +----+ | |TPE1|========|SPE1|========|TPE2|    | +----+
  |    |-----|.....PW.Seg't1......PW.Seg't3.....|------|    |
  | CE1| |   |    |    |         |    |         |    |    | |CE2 |
  |    |-----|.....PW.Seg't2......PW.Seg't4.....|------|    |
  +----+ |   |    |========|    |========|    |    | +----+
         ^    +----+    ^    +----+    ^    +----+       ^
         |            |            |            |
         |           TP LSP       TP LSP           |
         |            |            |            |
         |<--------------- Emulated Service ------------->|

    -------Untrusted------------>|<-->|<-------Untrusted----------
                                Trusted
                                 Zone
```

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

   Security Reference Model 2(c)

   An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from
   different Service Providers with inter-provider PW connections. The
   trusted zone is T-PE1 to S-PE3, as illustrated in Figure 5.

```
    Native  |<-------------------- PW15 --------------------->| Native
     Layer  |                                                 | Layer
   Service  |    |<-PSN13->|    |<-PSN3X->|    |<-PSNXZ->|     | Service
     (AC1) V    V   LSP    V    V   LSP    V    V   LSP    V    V (AC2)
            +----+    +-+   +----+         +----+    +-+   +----+
   +---+    |TPE1|    | |   |SPE3|         |SPEX|    | |   |TPEZ|    +---+
   |   |    |    |========|    |========|    |========|    |    |    |   |
   |CE1|----|........PW1........|...PW3...|........PW5........|---|CE2|
   |   |    |    |========|    |========|    |========|    |    |    |   |
   +---+    | 1  |    |2|   | 3  |         | X  |    |Y|   | Z  |    +---+
            +----+    +-+   +----+         +----+    +-+   +----+
            |<- Subnetwork 123->|         |<- Subnetwork XYZ->|

   Untrusted>|<- Trusted Zone - >|<-------------Untrusted--------------
```
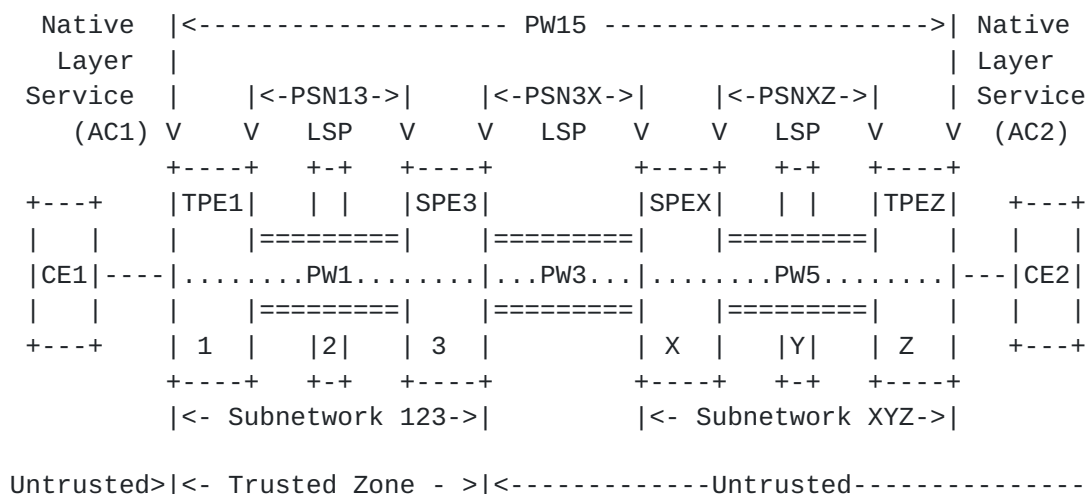
                Figure 5. MPLS-TP Security Model 2(c)

   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 given network topology.

3. Security Threats

This section discuss various network security threats which are to
MPLS-TP and may endanger MPLS-TP networks.

A successful attack on a particular MPLS-TP network or on a SP's
MPLS-TP infrastructure may cause one or more adverse effects.

Attacks to GAL or G-ACh may include:

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

   - DoS attack through in-band OAM G-ACh/GAL and BFD messages.

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

When a NMS is used for LSP setup, the attacks to NMS can cause the
above effect as well. Although this is not unique to MPLS-TP, but
MPLS-TP network can be particularly venerable as static provisioning
through NMS is a commonly used model.

Observation (including traffic pattern analysis), modification, or
deletion of a provider's or user's data, as well as 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 similar way to how they apply to
MPLS traffic regardless how the LSP is set up.

The threats may be resulting from malicious behavior or accidental
errors. For example: Users of the MPLS-TP network may attack the
network or other users; employees of the MPLS-TP operators,
especially people who operate the NMS, attackers who obtain physical
access to a MPLS-TP SP's site; Other SPs in the case of MPLS-TP
inter-provider connection.

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, which 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.

The techniques discussed here include entity authentication for
identity verification, encryption for confidentiality, 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, and event logging. Where these
techniques apply to MPLS and GMPLS in general, they are described in
Section 5.2 of [RFC5920]. The remainder of this section covers
aspects that apply particularly to MPLS-TP.

- Use of Isolated Infrastructure for MPLS-TP

Thisis one way to protect the infrastructure used for support of
MPLS-TP to separate the resources for support of MPLS-TP services
from the resources used for other purposes. For example, in security
model 2 (Section 2.2), the potential risk of attacks on the S-PE or
T-PE in the trusted zone may be reduced by using non-IP-based
communication paths.

- 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 are now developed for general MPLS networks
as well.

The defense techniques are apply generally to MPLS/GMPLS are not
detailed here, for example: 1) Authentication: including Management
System Authentication, Peer-to-Peer Authentication, Cryptographic
Techniques for Authenticating Identity; 2) Access Control Techniques;
3) Use of Aggregated Infrastructure; 4) Use of Aggregated
Infrastructure; 5) Mitigation of Denial of Service Attacks; 6)
Monitoring, Detection, and Reporting of Security Attacks. Please
refer to [RFC5920] for details.

5. Security Considerations

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

This document evaluates MPLS-TP specific security risks and

mitigation mechanisms which may be used to counter the potential
threats. All of the techniques presented 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. IANA Considerations

This document contains no new IANA considerations.

7. Acknowledgements

The authors wish to thank Joel Halpern and Gregory Mirsky for their
review comments and contributions to this document, thank Mach Chen
for his review and suggestions, thank Adrian Farrel for his Routing
AD review and detailed comments, thank Loa Andersson for his
continued support and guidance as the MPLS WG co-Chair.

8. References

8.1. 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.

8.2. 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.

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

Contributors' Addresses

    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