

Network Working Group  
Internet Draft  
Intended status: Informational

Sergio Belotti  
Don Fedyk  
Dimitri Papadimitriou  
Alcatel-Lucent  
Daniele Ceccarelli  
Ericsson  
Fatai Zhang  
Huawei Technologies  
Yuji Tochio  
Fujitsu

Expires: Dec 2013

June 6, 2013

Applicability Statement for Layer 1 Virtual Private Network (L1VPN)  
Enhanced Mode

draft-belotti-app-statement-l1vpn-em-02.txt

## Abstract

This document provides an applicability statement on the use of Generalized Multiprotocol Label Switching (GMPLS) protocols and mechanisms to satisfy the requirements of the Layer 1 Virtual Private Network (L1VPN) Enhanced Mode.

L1VPNs provide customer services and connectivity at layer 1 over layer 1 networks. The operation of L1VPNs is divided into the Basic Mode and the Enhanced Mode, where the Enhanced Mode of operation may also include exchange of routing information between the layer 1 network and the customer domain.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months 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/ietf/lid-abstracts.txt>

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

#### Copyright Notice and License Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction.....</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Conventions Used in This Document.....</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">Terminology.....</a>	<a href="#">4</a>
<a href="#">4.</a>	<a href="#">Existing Solutions.....</a>	<a href="#">4</a>
<a href="#">5.</a>	<a href="#">General Guidelines.....</a>	<a href="#">4</a>
<a href="#">6.</a>	<a href="#">Overlay Extension Service Model.....</a>	<a href="#">6</a>
<a href="#">6.1.</a>	<a href="#">Overview of the Service Model.....</a>	<a href="#">6</a>
<a href="#">6.2.</a>	<a href="#">Applicability of Existing Solutions.....</a>	<a href="#">6</a>
<a href="#">6.3.</a>	<a href="#">Incremental protocol extensions.....</a>	<a href="#">7</a>
<a href="#">7.</a>	<a href="#">Virtual Node Service Model.....</a>	<a href="#">7</a>
<a href="#">7.1.</a>	<a href="#">Overview of the Service Model.....</a>	<a href="#">7</a>
<a href="#">7.2.</a>	<a href="#">Applicability of Existing Solutions.....</a>	<a href="#">8</a>
<a href="#">8.</a>	<a href="#">Virtual Link Service Model.....</a>	<a href="#">8</a>
<a href="#">8.1.</a>	<a href="#">Overview of the Service Model.....</a>	<a href="#">8</a>
<a href="#">8.2.</a>	<a href="#">Applicability of Existing Solutions.....</a>	<a href="#">8</a>
<a href="#">9.</a>	<a href="#">Per-VPN Peer Service Model.....</a>	<a href="#">8</a>
<a href="#">9.1.</a>	<a href="#">Overview of the Service Model.....</a>	<a href="#">8</a>
<a href="#">9.2.</a>	<a href="#">Applicability of Existing Solutions.....</a>	<a href="#">9</a>
<a href="#">10.</a>	<a href="#">Manageability Considerations.....</a>	<a href="#">9</a>
<a href="#">11.</a>	<a href="#">Security Considerations.....</a>	<a href="#">9</a>
<a href="#">12.</a>	<a href="#">IANA Considerations.....</a>	<a href="#">9</a>
<a href="#">13.</a>	<a href="#">References.....</a>	<a href="#">10</a>
<a href="#">13.1.</a>	<a href="#">Normative References.....</a>	<a href="#">10</a>
<a href="#">13.2.</a>	<a href="#">Informative References.....</a>	<a href="#">10</a>
<a href="#">14.</a>	<a href="#">Acknowledgments.....</a>	<a href="#">12</a>
<a href="#">15.</a>	<a href="#">Author's Addresses.....</a>	<a href="#">12</a>

[1.](#) Introduction

This document provides an applicability statement on the use of existing Generalized Multiprotocol Label Switching (GMPLS) protocols and mechanisms to the Layer 1 Virtual Private Network (L1VPN) Enhanced Mode.

In particular, this document shows section by section (from [Section 5](#) to 8) the applicability of GMPLS protocols and mechanisms to each sub-model of the Enhanced Mode mentioned in [[RFC4847](#)].

Note that discussion in this document is limited to areas where GMPLS protocols and mechanisms are relevant.

As will be described in this document, support of the Overlay Extension service model and the Virtual Node service model are well

covered by existing protocol mechanisms already described in other documents, with only minor protocol extensions required. The Virtual Link service model and the Per-VPN Peer service model are not explicitly covered by existing documents, and would require extension of current GMPLS protocols and mechanisms

Solutions should be scalable and manageable per [RFC 4847](#). Solutions should not require L1VPN state to be maintained on the P devices as much as possible.

## [2. 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 [RFC-2119](#) [[RFC2119](#)].

## [3. Terminology](#)

The reader is assumed to be familiar with the terminology in [[RFC3031](#)], [[RFC3209](#)], [[RFC3471](#)], [[RFC3473](#)], [[RFC4202](#)], [[RFC4026](#)] and [[RFC4847](#)], [[RFC4874](#)], [[RFC5251](#)], [[RFC5253](#)], [[RFC5252](#)] and [[RFC4208](#)].

## [4. Existing Solutions](#)

This section lists existing solution documents that describe how the L1VPN Enhanced Mode may be constructed using the mechanisms of GMPLS. This document draws on those solutions and explains their applicability with respect to the framework described in [[RFC4847](#)]. Further solution documents may be listed in a future version of this document.

- [[RFC5251](#)] addresses L1VPN Basic Mode signaling.
- [[RFC4208](#)] addresses the application of GMPLS to the Overlay model.
- [[RFC5252](#)] describes OSPF based autodiscovery mechanisms.

Note that although [[RFC5251](#)] specifies signaling mechanisms for L1VPN Basic Mode, it is applicable to the L1VPN Enhanced Mode, unless otherwise specified.

## [5. General Guidelines](#)

This section provides general guidelines for L1VPN solutions. Note

that applicability to specific sub-models will be separately described in following sections. One important general design guideline is that protocol mechanisms should be re-used where possible. This means that solutions should be incremental, building on existing protocol mechanisms rather than developing wholly new protocols. Further, as service models are extended or developed resulting in the requirement for additional functionalities, deltas should be added to the protocol mechanisms rather than developing new techniques. [[RFC4847](#)] describes how the service models can be seen to provide "cascaded" functionality, and this should be leveraged to achieve re-use of protocol extensions so that, for example, it is highly desirable that the same signaling protocols and extensions are used in both the Basic Mode and the Enhanced Mode.

In addition, the following are general guidelines:

- The support of L1VPNs should not necessitate any change to core (P)devices. Therefore, any protocol extensions made to facilitate L1VPNs need to be made in a backward compatible way allowing GMPLS aware P devices to continue to function.
- Customer (C) devices not directly involved in providing L1VPN
- Services should also be protected from protocol extensions made to support L1VPNs. Again, such protocol extensions need to be backwards compatible. Note however, that some L1VPN service models allow for VPN connectivity between C devices rather than between CE devices: in this case, the C devices may need to be aware of protocol extensions.
- Solutions should aim to minimize the protocol extensions on CE devices.
- Solutions should be scalable and manageable per [RFC 4847](#). Solutions should not require L1VPN state to be maintained on the P devices as much as possible.
- Solutions should be secure. Providers should be able to screen and protect information based on their operational policies per [RFC 4847](#).
- Solutions should provide an operational view of the L1VPN for the customer and provider. There should be a common operational and management perspective in regard to other (L2 and L3) VPN services per [RFC 4847](#).

## [6.](#) Overlay Extension Service Model

### [6.1.](#) Overview of the Service Model

This service model complements the Basic Mode and may assume all of the requirements, solutions and work items for that model.

In this service model, a CE receives from its attached PEs a list of TE link addresses to which it can request a VPN connection (i.e., membership information).

The CE may also receive some TE information concerning these CE-PE links within the VPN (e.g., switching type).

Further information may be found in [[draft-fedyk-ccamp-l1vpn-extnd-overlay](#)].

The CE does not receive any of the following from the PE:

- Routing information about the core provider network.
- Information about P device addresses.
- Information about P-P, PE-P or PE-PE TE links.
- Routing information about other customer sites. The CE may have access to routing information about the remainder of the VPN (C-C and CE-C links), but this is exchanged by control plane tunneling on the CE-CE connections and is not passed to the CE in the control plane exchange between PE and CE.

### [6.2.](#) Applicability of Existing Solutions

The following are required in this service model (in addition to requirements in the L1VPN Basic Mode:

- Interactions between an edge node (CE) and it's adjacent (at the data plane) core-node (PE).
- VPN membership information exchange between a CE and PE.
- CE-PE TE link information exchange between a CE and a PE.

[RFC 4208](#) addresses RSVP-TE procedures between an edge-node and a core-node in the overlay model. [RFC5252](#) enables PE devices using OSPF to dynamically learn about the existence of each other, and

attributes of configured CE links and their association with L1VPNs. Furthermore, [\[RFC5252\]](#) allows the exchange of CE-PE TE link information between a CE and a PE.

### [6.3](#). Incremental protocol extensions

It can be useful for the ingress node to be able to convey TE metrics (e.g., IGP metric, TE metric, hop counts, latency, etc.) that the path computation algorithm (at the remote node performing route computation or expansion) can optimize for. Similarly, it can be useful for the ingress node to be able to indicate a TE metric bound for the loose segment being expanded by the remote node, (e.g., [\[DRAFT-TE-METRIC-BOUND\]](#)).

In a similar manner, as described in [\[DRAFT-TE-METRIC-RECORD\]](#), there are RSVP-TE requirements for the support of the automatic discovery of cost, latency and latency variation attributes of an LSP. These requirements are very similar to the requirement for discovering the Shared Risk Link Groups (SRLGs) associated with the route taken by an LSP (e.g., [\[DRAFT-SRLG-RECORDING\]](#)).

It is also possible to improve route diversity for single-homed and dual-homed customer LSPs, which is a common requirement. This may be achieved via signaling extensions that provide shared constraint information for path diversity. Specifically, mechanisms that enable communication to the node computing/expanding the LSP signaled, information to exclude the route taken by a particular LSP or the route taken by all LSPs belonging to a single tunnel (e.g., [\[DRAFT-DIV-LATENCY-EXT\]](#)).

## [7](#). Virtual Node Service Model

### [7.1](#). Overview of the Service Model

In this service model, there is a private routing exchange between the CE and the PE, or to be more precise between the CE routing protocol instance and the VPN routing protocol instance running on the PE. The provider network is considered as one private node from the customer's perspective. The routing information exchanged between the CE and the PE includes CE-PE TE link information, customer network (i.e., remote CE sites), and may include TE links (Forwarding Adjacencies) connecting CEs (or Cs) across the provider network as well as control plane topology information from the customer network (i.e., CE sites).



## [7.2.](#) Applicability of Existing Solutions

The following are required in this service model:

- VPN routing
- CE-CE Label Switching Path (LSP) setup, deletion, and modification signaling.

It is possible to use IGP-based auto-discovery (based on [[RFC5252](#)]).

Signaling mechanisms are covered by [[RFC5251](#)].

## [8.](#) Virtual Link Service Model

### [8.1.](#) Overview of the Service Model

In this service model, virtual links are established between PEs. A virtual link is assigned to each VPN and disclosed to the corresponding CEs. The routing information exchanged between the CE and the PE includes CE-PE TE links, customer network (i.e., remote CE sites), virtual links (i.e., PE-PE links) assigned to each VPN, and may include CE-CE (or C-C) Forwarding Adjacencies as well as control plane topology from the customer network (i.e., CE sites).

NOTE - Resource management for a dedicated data plane is a mandatory requirement for the Virtual Link service model. This could be realized by assigning pre-configured FA-LSPs to each VPN routing protocol instance (no protocol extensions needed) in order to instantiate the necessary FAs.

### [8.2.](#) Applicability of Existing Solutions

Currently, there is no solution document for this type of service model.

## [9.](#) Per-VPN Peer Service Model

### [9.1.](#) Overview of the Service Model

In this service model, the provider partitions TE links within the

provider network per VPN. The routing information exchanged between the CE and the PE includes CE-PE TE links, customer network (i.e.,

remote CE sites), as well as partitioned portions of the provider network, and may include CE-CE (or C-C) Forwarding Adjacencies and control plane topology from customer network (i.e., CE sites). Note that PEs may abstract routing information about the provider network and advertise it to CEs.

Note scalability must be carefully considered for advertising provider network routing information to the CE [[RFC4726](#)].

## [9.2](#). Applicability of Existing Solutions

Currently, there is no solution document for this type of service model.

## [10](#). Manageability Considerations

[Section 11 of \[RFC4847\]](#) describes manageability considerations for L1VPNs.

This document defines a following new manageability requirement specific for the L1VPN Enhanced Mode.

MIB modules MUST be available for any protocol extensions for the L1VPN Enhanced Mode.

A future revision of this document may cover more aspects.

## [11](#). Security Considerations

[Section 12 of \[RFC4847\]](#) describes security considerations for L1VPNs. This document defines a following new security requirements specific for the L1VPN Enhanced Mode.

In the L1VPN Enhanced Mode, since there is a routing adjacency between a CE and a PE, care must be taken whether the provider network's control plane topology information is leaked to the CE. Due to security concerns, this is not recommended in general, and there must be a mechanism to prevent such operation. A future revision of this document may cover more aspects.

## [12. IANA Considerations](#)

This document requires no IANA actions.

## [13. References](#)

### [13.1. Normative References](#)

- [RFC2119]        Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4208]        Swallow, G., et al., "Generalize Multiprotocol Label Switching(GMPLS) User-Network Interface: Resource ReserVation Protocol-Traffic Engineering(RSVP-TE) Support for the Overlay Model," [RFC 4208](#), October 2005.
- [RFC4847]        Takeda, T., Editor "Framework and Requirements Layer 1 Virtual Private Networks", [RFC 4847](#),
- [RFC5251]        Fedyk, D., et al., "Layer 1 VPN Basic Mode", [RFC 5251](#), July 2008.
- [RFC5252]        Bryskin, I., Berger, L., "OSPF-Based Layer 1 VPN Auto-Discovery", [RFC 5252](#), July 2008.
- [RFC5253]        Takeda, T. et al., "Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Basic Mode", [RFC 5253](#), July 2008.

### [13.2. Informative References](#)

- [Y.1312]        Y.1312 - Layer 1 Virtual Private Network Generic requirements and architecture elements, ITU-T Recommendation, September 2003.
- [Y.1313]        Y.1313 - Layer 1 Virtual Private Network service and network architectures, ITU-T Recommendation, July 2004.

- [RFC3031] Rosen, E., Viswanathan, A. and R. Callon, "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.

Belotti and al.

Expires December 6, 2013

[Page 10]

---

Internet-Draft    Applicability of L1VPN Enhanced Mode    June 2013

- [RFC3471] Berger, L., Editor, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", [RFC 3471](#), January 2003.
- [RFC3473] Berger, L., Editor "Generalized Multi-Protocol Label Switching (GMPLS) Signaling - Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", [RFC 3473](#), January 2003.
- [RFC4202] Kompella, K., et al., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", [RFC 4202](#), October 2005.
- [RFC4026] Andersson, L., and Madsen, T., "Provider Provisioned Virtual Private Network (VPN) Terminology", [RFC 4026](#), March 2005.
- [RFC4874] Lee, CY., Farrel, A., and S. De Cnodder, "Exclude Routes - Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)", [RFC 874](#), April 2007.
- [RFC4726] Farrel, A., et al., "A Framework for Inter-Domain Multiprotocol Label Switching Traffic Engineering", [RFC 4726](#), November 2006.
- [DRAFT-TE-METRIC-BOUND] Ali Z., et al., Resource ReserVation Protocol - Traffic Engineering (RSVP-TE) extension for signaling Objective Function and Metric Bound [draft-ali-ccamp-rc-objective-function-metric-bound-02](#), work in progress

[DRAFT-SRLG-RECORDING] F. Zhang, D. Li, O. Gonzalez de Dios, C. Margaria. C, " RSVP-TE Extensions for Collecting SRLG Information ", [draft-ietf-ccamp-rsvp-te-srlg-collect-02](#), work in progress.

[DRAFT-TE-METRIC-RECORD] ALI Z.,et al., "Resource ReserVation Protocol- Traffic Engineering (RSVP-TE) extension for recording TE Metric of a Label Switched Path",

Belotti and al.

Expires December 6, 2013

[Page 11]

---

Internet-Draft    Applicability of L1VPN Enhanced Mode

June 2013

[draft-ietf-ccamp-te-metric-recording-01.txt](#), work in progress.

[DRAFT-DIV-LATENCY-EXT] Fedyk D., et al., "Layer 1 VPN Enhanced Mode - Overlay Extension Service Model", [draft-fedyk-ccamp-uni-extension-01](#), work in progress.

## 14. Acknowledgments

The authors would like to thank the editor and authors of [draft-ietf-l1vpn-applicability-enhanced-mode](#) (Tomonori Takeda, Hamid Ould-Brahim, Adrian Farrel, Deborah Brungard) and the members of the L1VPN working group for their contribution, in recognition that most of the text in this draft derives from their effort.

The authors would also like to thank Dieter Beller, Lieven Levrau, and Eve Varma for their contributions to this work.

## 15. Author's Addresses

Sergio Belotti (Alcatel-Lucent)  
VIA TRENTO 30  
20059 Vimercate  
Italy  
Phone: +39 039 686 3033  
[sergio.belotti@alcatel-lucent.com](mailto:sergio.belotti@alcatel-lucent.com)

Don Fedyk (Alcatel-Lucent)  
Groton, MA 01450  
United States  
Phone: +1 978 467 5645  
Email: Donald.Fedyk@alcatel-lucent.com

Dimitri Papadimitriou (Alcatel-Lucent)  
Copernicuslaan 50  
2018 Antwerp  
Belgium  
Phone: +32 3 2408491

Belotti and al.

Expires December 6, 2013

[Page 12]

---

Internet-Draft Applicability of L1VPN Enhanced Mode

June 2013

Email: dimitri.papadimitriou@alcatel-lucent.com

Daniele Ceccarelli (Ericsson)  
Via A. Negrone 1/A  
Genova - Sestri Ponente  
Italy  
Email: daniele.ceccarelli@ericsson.com

Fatai Zhang  
Huawei Technologies  
F3-5-B R&D Center, Huawei Base  
Shenzhen 518129 P.R.China Bantian, Longgang District  
Phone: +86-755-28972912  
Email: zhangfatai@huawei.com

Yuji Tochio (Fujitsu)  
4-1-1 Kamikodanaka, Nakahara-Ku  
Kawasaki  
Japan  
Email: tochio@jp.fujitsu.com

Belotti and al.

Expires December 6, 2013

[Page 13]