

Internet Engineering Task Force (IETF)  
Request for Comments: 7436  
Category: Historic  
ISSN: 2070-1721

H. Shah  
Cinea Corp.  
E. Rosen  
Juniper Networks  
F. Le Faucheur  
G. Heron  
Cisco Systems  
January 2015

## IP-Only LAN Service (IPLS)

### Abstract

A Virtual Private LAN Service (VPLS) is used to interconnect systems across a wide-area or metropolitan-area network, making it appear that they are on a private LAN. The systems that are interconnected may themselves be LAN switches. If, however, they are IP hosts or IP routers, certain simplifications to the operation of the VPLS are possible. We call this simplified type of VPLS an "IP-only LAN Service" (IPLS). In an IPLS, as in a VPLS, LAN interfaces are run in promiscuous mode, and frames are forwarded based on their destination Media Access Control (MAC) addresses. However, the maintenance of the MAC forwarding tables is done via signaling, rather than via the MAC address learning procedures specified in the IEEE's "Media Access Control (MAC) Bridges". This document specifies the protocol extensions and procedures for support of the IPLS service.

The original intent was to provide an alternate solution to VPLS for those Provider Edge (PE) routers that were not capable of learning MAC addresses through data plane. This became a non-issue with newer hardware. The concepts put forth by this document are still valuable and are adopted in one form or other by newer work such as Ethernet VPN in L2VPN working group and possible data center applications. At this point, no further action is planned to update this document and it is published simply as a historic record of the ideas.

## Status of This Memo

This document is not an Internet Standards Track specification; it is published for the historical record.

This document defines a Historic Document for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc7436>.

## Copyright Notice

Copyright (c) 2015 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

1. Overview .....	4
1.1. Terminology .....	7
2. Topology .....	9
3. Configuration .....	10
4. Discovery .....	10
4.1. CE Discovery .....	10
4.1.1. IPv4-Based CE Discovery .....	11
4.1.2. IPv6-Based CE Discovery (RFC 4861) .....	11
5. PW Creation .....	11
5.1. Receive Unicast Multipoint-to-Point PW .....	11
5.2. Receive Multicast Multipoint-to-Point PW .....	12
5.3. Send Multicast Replication Tree .....	13

6. Signaling .....	13
6.1. IPLS PW Signaling .....	13
6.2. IPv6 Capability Advertisement .....	17
6.3. Signaling Advertisement Processing .....	18
7. IANA Considerations .....	19
7.1. LDP Status Messages .....	19
7.2. Interface Parameters .....	19
8. Forwarding .....	20
8.1. Non-IP or Non-ARP Traffic .....	20
8.2. Unicast IP Traffic .....	20
8.3. Broadcasts and Multicast IP Traffic .....	20
8.4. ARP Traffic .....	21
8.5. Discovery of IPv6 CE Devices .....	21
8.5.1. Processing of Neighbor Solicitations .....	22
8.5.2. Processing of Neighbor Advertisements .....	22
8.5.3. Processing of Inverse Neighbor Solicitations and Advertisement .....	22
8.5.4. Processing of Router Solicitations and Advertisements .....	23
8.6. Encapsulation .....	23
9. Attaching to IPLS via ATM or Frame Relay (FR) .....	24
10. VPLS vs. IPLS .....	24
11. IP Protocols .....	25
12. Dual-Homing with IPLS .....	25
13. Proxy ARP Function .....	26
13.1. ARP Proxy - Responder .....	26
13.2. ARP Proxy - Generator .....	26
14. Data Center Applicability .....	27
15. Security Considerations .....	27
15.1. Control-Plane Security .....	27
15.2. Data-Plane Security .....	28
16. References .....	29
16.1. Normative References .....	29
16.2. Informative References .....	30
Acknowledgements .....	31
Contributors .....	31
Authors' Addresses .....	32

## 1. Overview

As emphasized in [RFC4762], Ethernet has become popular as an access technology in metropolitan- and wide-area networks. [RFC4762] describes how geographically dispersed customer LANs can be interconnected over a service provider's network. The VPLS service is provided by Provider Edge (PE) devices that connect Customer Edge (CE) devices. The VPLS architecture provides this service by incorporating bridging functions such as MAC address learning in the PE devices.

PE platforms are designed primarily to be IP routers rather than LAN switches. To add VPLS capability to a PE router, one has to add MAC-address-learning capabilities, along with aging and other mechanisms native to Ethernet switches [IEEE802.1D]. This may be fairly complex to add to the forwarding-plane architecture of an IP router. As discussed in [RFC4664], in scenarios where the CE devices are NOT LAN switches, but rather are IP hosts or IP routers, it is possible to provide the VPLS service without requiring MAC address learning and aging on the PE. Instead, a PE router has to have the capability to match the destination MAC address in a packet received from a CE to an outbound pseudowire (PW). The requirements for the IPLS service are described in [RFC4665]. The purpose of this document is to specify a solution optimized for IPLS.

IPLS provides a VPLS-like service using PE routers that are not designed to perform general LAN bridging functions. One must be willing to accept the restriction that an IPLS be used for IP traffic only, and not used to interconnect CE devices that are themselves LAN switches. This is an acceptable restriction in many environments, given that IP is the predominant type of traffic in today's networks.

The original intent was to provide an alternate solution to VPLS for those PE routers that were not capable of learning MAC addresses in the data plane. This became a non-issue with newer hardware. The concepts put forth by this document are still valuable and are adopted in one form or other by newer work such as Ethernet VPN in the L2VPN working group and possible data center applications. At this point, no further action is planned to update this document and is published simply as a historic record of the ideas.

In IPLS, a PE device implements multipoint LAN connectivity for IP traffic using the following key functions:

1. **CE Address Discovery:** Each PE device discovers the MAC address of the locally attached CE IP devices, for each IPLS instance configured on the PE device. In some configurations, the PE also learns the IP address of the CE device (when performing ARP proxy functions, described later in the document).
2. **Pseudowire (PW) for Unicast Traffic:** For each locally attached CE device in a given IPLS instance, a PE device sets up a pseudowire (PW) to each of the other PEs that supports the same IPLS instance.

For instance, if PEx and PEy both support IPLS I, and PEy is locally attached to CEa and CEb, PEy will initiate the setup of two PWs between itself and PEx. One of these will be used to carry unicast traffic from any of PEx's CE devices to CEa. The other will be used to carry unicast traffic from any of PEx's CE devices to CEb.

Note that these PWs carry traffic only in one direction. Further, while the PW implicitly identifies the destination CE of the traffic, it does not identify the source CE; packets from different source CEs bound to the same destination CE are sent on a single PW.

3. **Pseudowires for Multicast Traffic:** In addition, every PE supporting a given IPLS instance will set up a special 'multicast' pseudowire to every other PE in that IPLS instance. If, in the above example, one of PEx's CE devices sends a multicast packet, PEx would forward the multicast packet to PEy on the special 'multicast' pseudowire. PEy would then send a copy of that packet to CEa and a copy to CEb.

The 'multicast' pseudowire carries Ethernet frames of multicast/broadcast IP, ARP, and ICMP (Inverse) Neighbor Discovery (ND/IND) packets for IPv6. Thus, when a PE sends a multicast packet across the network, it sends one copy to each remote PE (supporting the given IPLS instance). If a particular remote PE has more than one CE device in that IPLS instance, the remote PE must replicate the packet and send one copy to each of its local CEs.

As with the pseudowires that are used for unicast traffic, packets travel in only one direction on these pseudowires, and packets from different sources may be freely intermixed.

4. Signaling: The necessary pseudowires can be set up and maintained using the signaling procedures based on the Label Distribution Protocol (LDP) described in [RFC4447].

A PE may assign the same label to each of the unicast pseudowires that lead to a given CE device, in effect creating a multipoint-to-point pseudowire.

Similarly, a PE may assign the same label to each of the 'multicast' pseudowires for a given IPLS instance, in effect creating a multipoint-to-point pseudowire. When setting up a pseudowire to be used for unicast traffic, the PE must also signal the MAC address of the corresponding CE device. It should also, optionally, advertise the IP address of the local CE device, especially when ARP proxy function is configured or simply for operational management purposes. Similarly, for IPv6 support, PE may optionally advertise the IPv6 addresses of the local CE device.

5. ARP Packet Forwarding: ARP packets [RFC826] are forwarded from the attachment circuit (AC) to 'multicast' pseudowires in the Ethernet frame format as described by [RFC4448]. The following rules are observed when processing ARP packets:
  - a. Both broadcast (request) and unicast (response) ARP packets are sent over the 'multicast' pseudowire.
  - b. When an ARP packet is received from an AC, the packet is copied to the control plane for the purpose of learning the MAC address of the CE. Optionally, an IP address is also learned to record the association of the IP and MAC address.
  - c. All Ethernet packets, including ARP packets, received from the 'multicast' pseudowire are forwarded out to all the ACs associated with the IPLS instance. These packets are not copied to the control plane.
6. ICMP IPv6 ND/IND-related Packet Forwarding: ND/IND IPv6 packets from an AC are replicated and a copy is sent to other ACs and to 'multicast' PWs associated with the IPLS instance in the native Ethernet format, unchanged. A copy is also submitted to the control plane to learn the MAC address and, optionally, corresponding IPv6 addresses.

7. Multicast IP packet forwarding: An IP Ethernet frame received from an AC is replicated to other ACs and the 'multicast' PWs associated with the IPLS instance. An IP Ethernet frame received from a 'multicast' PW is replicated to all the egress ACs associated with the IPLS instance.
8. Unicast IP packet forwarding: An IP packet received from the AC is forwarded based on the destination MAC address lookup in the forwarding table. If a match is found, the packet is forwarded to the associated egress interface. If the egress interface is unicast PW, the packet is sent without a MAC header. If the egress interface is a local AC, the Ethernet frame is forwarded as such. An IP packet received from the unicast PW is forwarded to the egress AC with the MAC header prepended. The destination MAC address is derived from the forwarding table while the source MAC address is the MAC address of the PE.

Both VPLS [RFC4762] and IPLS require the ingress PE to forward a frame based on its destination MAC address. However, two key differences between VPLS and IPLS can be noted from the above description:

- In VPLS, MAC entries are placed in the Forwarding Information Base (FIB) of the ingress PE as a result of MAC address learning (which occurs in the data plane); whereas, in IPLS, MAC entries are placed in the FIB as a result of PW signaling operations (control plane).
- In VPLS, the egress PE looks up a frame's destination MAC address to determine the egress AC; in IPLS, the egress AC is determined entirely by the ingress PW label.

The following sections describe the details of the IPLS scheme.

### 1.1. Terminology

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].

**IPLS** IPLS stands for IP-only LAN service (a type of Virtual Private LAN Service that is restricted to IP traffic only).

**MP2P PW** A Multipoint-to-Point Pseudowire is a PW that carries traffic from remote PE devices to a PE device that signals the PW. The signaling PE device advertises the same PW label to all remote PE devices that

participate in the IPLS service instance. In IPLS, for a given IPLS instance, an MP2P PW used for IP unicast traffic is established by a PE for each CE device locally attached to that PE. It is a unidirectional tree whose leaves consist of the remote PE peers (which connect at least one AC associated with the same IPLS instance) and whose root is the signaling PE. Traffic flows from the leaves towards the root.

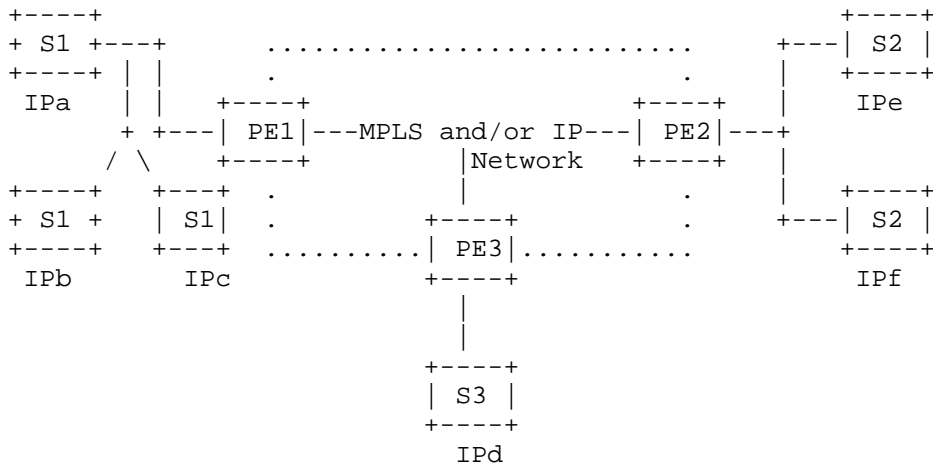
- Multicast PW** A Multicast/broadcast Pseudowire is a special kind of MP2P PW that carries IP multicast/broadcast traffic, all ARP frames and ICMP (I)ND frames for IPv6. In the IPLS architecture, for each IPLS instance supported by a PE, that PE device establishes exactly one multicast PW. Multicast PW uses Ethernet encapsulation.
- Unicast PW** A Unicast pseudowire carries IP unicast packets. A PE creates unicast PW for each locally attached CE. The unicast PW uses IP Layer 2 (L2) transport encapsulation.
- CE** In this document, a Customer Edge (CE) is any IP node (host or router) connected to the IPLS LAN service.
- Send Multicast Replication Tree** The collection of all multicast PWs and ACs that are members of an IPLS service instance on a given PE. When a PE receives a multicast/broadcast packet from an AC, the PE device sends a copy of the packet to every multicast PW and AC of the Send Multicast Replication Tree, excluding the AC on which the packet was received. When a PE receives a packet from a multicast PW, the PE device sends a copy of the packet to all the ACs of the Send Multicast Replication Tree and never to other PWs.
- (I)ND** (Inverse) Neighbor Discovery in IPv6 uses ICMP Neighbor Solicitation (NS) and Neighbor Advertisement (NA) packets.
- RS** Router Solicitation is when hosts generate all-routers multicast ICMP packets to discover the IPv6 router on the local link.
- RA** Router Advertisement occurs when a router generates all-nodes multicast ICMP packets to advertise its presence on the link. A unicast response is also sent when RS is received.



- NS Neighbor Solicitation in IPv6 uses (multicast) ICMP packets to resolve the association of the IPv6 interface address to the MAC address.
- NA Neighbor Advertisement in IPv6 uses (unicast) ICMP packets to respond to NS.

2. Topology

The CE devices are IP nodes (hosts or routers) that are connected to PE devices either directly or via an Ethernet network. We assume that the PE/CE connection may be regarded by the PE as an "interface" to which one or more CEs are attached. This interface may be a physical LAN interface or a VLAN. The PE routers are MPLS Label Edge Routers (LERs) that serve as PW endpoints.



In the above diagram, an IPLS instance is shown with three sites: site S1, site S2, and site S3. In site S3, the CE device is directly connected to its PE. In the other two sites, there are multiple CEs connected to a single PE. More precisely, the CEs at these sites are on an Ethernet (switched at site 1 and shared at site 2) network (or VLAN), and the PE is attached to that same Ethernet network or VLAN). We impose the following restriction: if one or more CEs attach to a PE by virtue of being on a common LAN or VLAN, there MUST NOT be more than one PE on that LAN or VLAN.

PE1, PE2, and PE3 are shown as connected via an MPLS network; however, other tunneling technologies, such as Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol version 3 (L2TPv3), etc., could also be used to carry the PWs.

An IPLS instance is a single broadcast domain, such that each IP end station (e.g., IPa) appears to be co-located with other IP end stations (e.g., IPb through IPf) on the same subnet. The IPLS service is transparent to the CE devices and requires no changes to them.

### 3. Configuration

Each PE router is configured with one or more IPLS service instances, and each IPLS service instance is associated with a unique VPN-ID. For a given IPLS service instance, a set of ACs is identified. Each AC can be associated with only one IPLS instance. An AC, in this document, is either a customer-facing Ethernet port, or a particular VLAN (identified by an IEEE 802.1Q VLAN ID) on a customer-facing Ethernet port.

The PE router can optionally be configured with a local MAC address to be used as a source MAC address when IP packets are forwarded from a PW to an AC. By default, a PE uses the MAC address of the customer-facing Ethernet interface for this purpose.

### 4. Discovery

The discovery process includes:

- Remote PE discovery
- VPN (i.e., IPLS) membership discovery
- IP CE end station discovery

This document does not discuss the remote PE discovery or VPN membership discovery. This information can either be user configured or can be obtained using auto-discovery techniques described in [RFC6074] or other methods. However, the discovery of the CE is an important operational step in the IPLS model and is described below.

#### 4.1. CE Discovery

Each PE actively detects the presence of local CEs by snooping IP and ARP frames received over the ACs. When an AC configured in an IPLS instance becomes operational, it enters the CE discovery phase. In this phase, the PE examines each multicast/broadcast Ethernet frame. For link-local IP broadcast/multicast frames (e.g., IPv4 packets with destination addresses within 224.0.0/24 [RFC5771]), the CE's (source) MAC address is extracted from the Ethernet header and the (source) IP address is obtained from the IP header.

For each CE, the PE maintains the following tuple: <Attachment Circuit identification info, VPN-ID, MAC address, IP address (optional)>.

#### 4.1.1. IPv4-Based CE Discovery

As indicated earlier, a copy of each ARP frame received over the AC is submitted to the control plane. The PE learns the MAC address and optionally the IP address of the CE from the source address fields of the ARP PDU.

Once a CE is discovered, its status is monitored continuously by examining the received ARP frames and by periodically generating ARP requests. The absence of an ARP response from a CE after a configurable number of ARP requests is interpreted as loss of connectivity with the CE.

#### 4.1.2. IPv6-Based CE Discovery (RFC 4861)

A copy of Neighbor and Router Discovery frames received over the AC are submitted to the control plane in the PE.

If the PE receives an NS message, and the source IP address of the message is not the unspecified address, the PE learns the MAC address and optionally the IP address of the CE.

If the PE receives an unsolicited NA message, the PE learns the source MAC address and optionally the IP address of the CE.

If the PE receives an RS, and the source IP address of the message is not the unspecified address, the PE learns source MAC address and optionally the IP address of the CE.

If the PE receives an RA, it learns the source MAC address and optionally the IP address of the CE.

The PE will periodically generate NS messages for the IP address of the CE as a means of verifying the continued existence of the address and its MAC address binding. The absence of a response from the CE device for a given number of retries could be interpreted as a loss of connectivity with the CE.

### 5. PW Creation

#### 5.1. Receive Unicast Multipoint-to-Point PW

As the PE discovers each locally attached CE, a unicast multipoint-to-point pseudowire (MP2P PW) associated exclusively with that CE is created by distributing the MAC address and optionally the IP address of the CE along with a PW label to all the remote PE peers that participate in the same IPLS instance. Note that the same value of a

PW label SHOULD be distributed to all the remote PE peers for a given CE. The MP2P PW thus created is used by remote PEs to send unicast IP traffic to a specific CE.

(The same functionality can be provided by a set of point-to-point PWs, and the PE is not required to send the same PW label to all the other PEs. For convenience, however, we will use the term MP2P PWs, which may be implemented using a set of point-to-point PWs.)

The PE forwards a frame received over this MP2P PW to the associated AC.

The unicast PW uses IP Layer 2 Transport encapsulation as defined in [RFC4447].

## 5.2. Receive Multicast Multipoint-to-Point PW

When a PE is configured to participate in an IPLS instance, it advertises a 'multicast' PW label to every other PE that is a member of the same IPLS. The advertised PW label value is the same for each PE, which creates an MP2P PW. There is only one such multicast MP2P PW per PE for each IPLS instance, and this PW is used exclusively to carry IP multicast/broadcast, ARP traffic, and (inverse) Neighbor Discovery packets for IPv6 from the remote PEs to this PE for this IPLS instance.

Note that no special functionality is expected from this PW. We call it a 'multicast' PW because we use it to carry multicast and broadcast IP, ARP, and IPv6 Neighbor Discovery traffic. The PW itself need not provide any different service than any of the unicast PWs.

In particular, the Receive multicast MP2P PW does not perform any replication of frames itself. Rather, it is there to signify to the PE that the PE may need to replicate a copy of a frame received over this MP2P PW onto all the ACs that are associated with the IPLS instance of the MP2P PW.

The multicast MP2P PW is considered the principal PW in the bundle of MP2P PWs that consists of one multicast MP2P PW and a variable number of unicast MP2P PWs for a given IPLS instance. In a principal role, multicast PW represents the IPLS instance. The life of all unicast PWs in the IPLS instance depends on the existence of the multicast PW. If, for some reason, multicast PWs cease to exist, all the associated unicast PWs in the bundle would be removed.

The multicast PW uses Ethernet encapsulation as defined in [RFC4448].

The use of PWs that are specially optimized for multicast is for further study.

### 5.3. Send Multicast Replication Tree

The PE creates a Send Multicast Replication Tree for each IPLS instance, which consists of the collection of all ACs and all the 'multicast' PWs of the IPLS instance.

Any ARP, Neighbor Discovery, or broadcast/multicast IP Ethernet frame received over an AC is replicated to the other ACs and to the MP2P multicast PW of the Send Multicast Replication Tree. The Send Multicast Replication Tree deals mostly with broadcast/multicast Ethernet MAC frames. One exception to this is unicast ARP and IPv6 Neighbor Discovery frame, the processing of which is described in the following section.

Any Ethernet frame received over the multicast PW is replicated to all the ACs of the Send Multicast Replication Tree of the IPLS instance associated with the incoming PW label: one exception is unicast ARP and Neighbor Discovery frames used for IPv6, the processing of which is described in the following section.

## 6. Signaling

[RFC4447] uses LDP to exchange PW FECs in the Label Mapping message in a downstream unsolicited mode. The PW FEC comes in two forms; PWid and Generalized PWid FEC elements. These FEC elements define some fields that are common between them. The discussions below refer to these common fields for IPLS-related extensions. Note that the use of multipoint-to-point and unidirectional characteristics of the PW makes BGP the ideal candidate for PW FEC signaling. The use of BGP for such purposes is for future study.

### 6.1. IPLS PW Signaling

An IPLS carries IP packets as payload over its unicast PWs and Ethernet frames as payload over its multicast PW. The PW type to be used for unicast PW is the IP PW, defined in [RFC4447] as IP Layer 2 Transport. The PW type to be used for multicast PW is the Ethernet PW as defined in [RFC4448]. The PW type values for these encapsulations are defined in [RFC4446].

When processing a received PW FEC, the PE matches the PW Id with the locally configured PW Id for the IPLS instance. If the PW type is Ethernet, the PW FEC is for multicast PWs. If the PW type is 'IP Layer 2 transport', the PW FEC is for unicast PWs.

For unicast PWs, the PE must check the presence of a MAC Address TLV in the optional parameter fields of the Label Mapping message. If this parameter is absent, a Label Release message must be issued with a status code meaning "MAC Address of the CE is absent" (note: status code 0x000000XX is pending IANA allocation (see Section 7)), to reject the establishment of the unicast PW with the remote PE.

The PE may optionally include an IP address TLV based on the user configuration for the advertising of the IP addresses of the local CE.

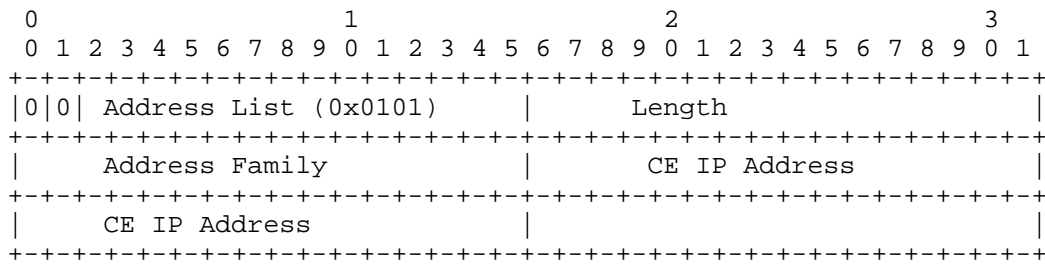
The processing of the Address List TLV is as follows.

- o If a PW is configured for ACs with IPv4 CEs only, the PE should advertise an Address List TLV with an Address Family type of an IPv4 address. The PE should process the IPv4 address list TLV as described in this document.
- o If a PW is configured for ACs with both IPv4 and IPv6 CEs, the PE should advertise IPv6 capability using the procedures described in the section below.
- o If a PE does not receive any IP Address List TLV or IPv6 capability advertisement, it MAY assume IPv4 behavior.

The IPLS uses the Address List TLV as defined in [RFC5036] to signal the MAC (and optionally IP) address of the local CE. There are two TLVs defined below: the IP Address TLV and MAC Address TLV. The MAC Address TLV must be included in the optional parameter field of the Label Mapping message when establishing the unicast IP PW for IPLS.

When configured to support a specific type of IP traffic (IPv4 or IPv6), the PE verifies the type of IP traffic the PW will carry. If there is a mismatch between the received Address Family value and the expectation of an IPLS instance to which the PW belongs, the PE must issue a Label Release message with a status code meaning "IP Address type mismatch" (status code 0x0000004A) to reject the PW establishment.

The encoding of the IP Address TLV is as follows:



Length

When an Address Family is IPv4, the Length is equal to 6 bytes; 2 bytes for the Address Family and 4 bytes of IP address. The Length is 18 bytes when the Address Family is IPv6; 2 bytes for the Address Family and 16 bytes of IP address.

Address Family

Two-octet quantity containing a value from the "Address Family Numbers" registry [ADDR-IANA] that encodes the addresses contained in the Addresses field.

CE IP Address

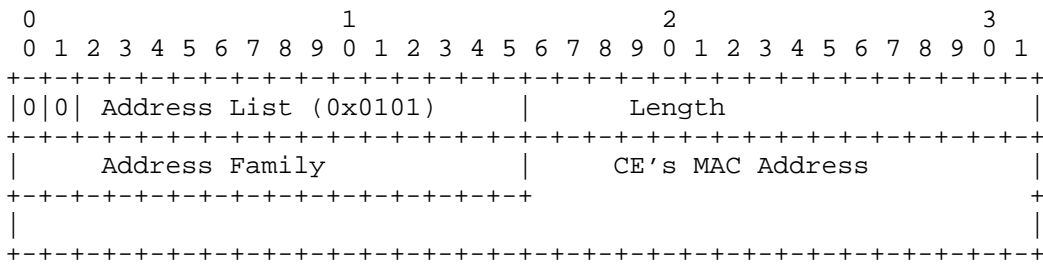
IP address of the CE attached to the advertising PE. The encoding of the individual address depends on the Address Family.

The following address encodings are defined by this version of the protocol:

Address Family	Address Encoding
IPv4 (1)	4-octet full IPv4 address
IPv6 (2)	16-octet full IPv6 address

Note that more than one instance of the IP address TLV may exist, especially when support for IPv6 is configured.

The encoding of the MAC Address TLV is as follows:



Length

The Length field is set to a value of 8 (2 bytes for the Address Family, 6 bytes for the MAC address)

Address Family

Two-octet quantity containing a value from the "Address Family Numbers" registry [ADDR-IANA] that encodes the addresses contained in the Addresses field.

CE's MAC Address

MAC address of the CE attached to the advertising PE. The encoding of the individual address depends on the Address Family.

The following address encodings are defined by this version of the protocol:

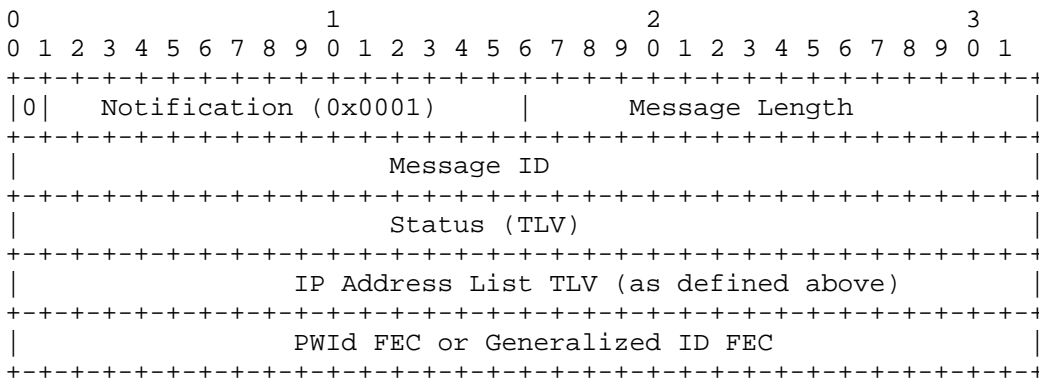
Address Family	Address Encoding
MAC (6)	6-octet full Ethernet MAC address

The IPv4 address of the CE is also supplied in the optional parameters field of the LDP Notification message along with the PW FEC. The LDP Notification message is used to signal any change in the status of the CE's IPv4 address.

Note that Notification message does not apply to the MAC Address TLV since an update to the MAC address of the CE should result in label withdrawal followed by establishment of a new PW with a new MAC address of the CE. However, advertisement of IP address(es) of the CE is optional, and changes may become known after the establishment of unicast PW.



The encoding of the LDP Notification message is as follows.



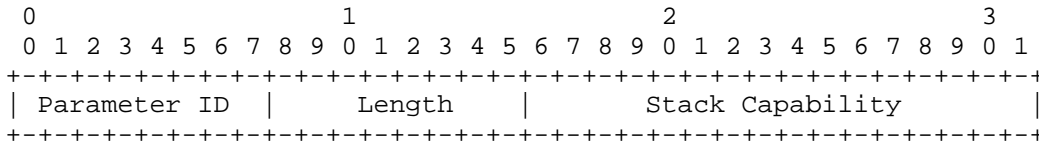
The Status TLV status code is set to 0x0000002C "IP address of CE", to indicate that an IP address update follows. Since this notification does not refer to any particular message, the Message ID and Message Type fields are set to 0.

The PW FEC TLV SHOULD NOT include the interface parameters as they are ignored in the context of this message.

### 6.2. IPv6 Capability Advertisement

A 'Stack Capability' Interface Parameter sub-TLV is signaled by the two PEs so that they can agree which stack(s) they should be using. It is assumed, by default, that the IP PW will always be capable of carrying IPv4 packets. Thus, this capability sub-TLV is used to indicate if other stacks need to be supported concurrently with IPv4.

The 'Stack Capability' sub-TLV is part of the interface parameters of the PW FEC. The proposed format for the 'Stack Capability' Interface Parameter sub-TLV is as follows:



Parameter ID = 0x16

Length = 4

Stack Capability = 0x000X to indicate IPv6 stack capability

The value of Stack Capability is dependent on the PW type context. For IP PW type, a setting of 0x000X indicates IPv6 stack capability.

A PE that supports IPv6 on an IP PW MUST signal the 'Stack Capability' sub-TLV in the initial Label Mapping message for the PW. The PE nodes compare the value advertised by the remote PE with the local configuration and only use a capability that is advertised by both. If a PE that supports IPv6 does not receive a 'Stack Capability' sub-TLV from the far-end PE in the initial Label Mapping message, or one is received but it is set to a reserved value, the PE MUST send an unsolicited release for the PW label with the LDP status code meaning "IP Address type mismatch" (status code 0x0000004A).

The behavior of a PE that does not understand an interface parameter sub-TLV is specified in RFC 4447 [RFC4447].

### 6.3. Signaling Advertisement Processing

A PE should process a received [RFC4447] advertisement with a PW type of IP Layer 2 Transport for IPLS as follows:

- Verify the IPLS VPN membership by matching the VPN-ID signaled in the Attachment Group Identifier (AGI) field or the Pwid field with all the VPN-IDs configured in the PE. Discard and release the PW label if VPN-ID is not found.
- Program the FIB such that when a unicast IP packet is received from an AC with its destination MAC address matching the advertised MAC address, the packet is forwarded out over the tunnel to the advertising PE with the advertised PW label as the inner label.

A PE should process a received [RFC4447] advertisement with the PW type of Ethernet for IPLS as follows:

- Verify the IPLS VPN membership by matching the VPN-ID signaled in the AGI field or the Pwid field with all the VPN-IDs configured in the PE. Discard and release the PW label if VPN-ID is not found.
- Add the PW label to the send broadcast replication tree for the VPN-ID. This enables the sending of a copy of a multicast/broadcast IP Ethernet frame, ARP Ethernet frame, or Neighbor Discovery frame from the AC to this PW.

## 7. IANA Considerations

Since this document is being published as Historic, no registration of IANA code points is necessary. However, in the future, if interest to pursue this proposal arises, the following IANA code registrations would become necessary.

### 7.1. LDP Status Messages

This document uses a new LDP status code. IANA already maintains the "Status Code Name Space" registry defined by [RFC5036]. The following allocation would be needed from the LDP Status Code Name Space.

0x000000XX "MAC Address of CE is absent"

### 7.2. Interface Parameters

This document proposes a new Interface Parameters sub-TLV, to be assigned from the "Pseudowire Interface Parameters Sub-TLV type Registry". The following allocation would be needed for the Parameter ID:

0xXX "Stack Capability"

IANA would also be requested to set up an "L2VPN PE Stack Capabilities" registry. This is a 16-bit field. The Stack Capability value (0x000X) is specified in Section 6.2 of this document. The remaining bit field values (0x0002,..,0x8000) would be assigned by IANA using the "IETF Consensus" policy defined in [RFC5226].

L2VPN PE Stack Capabilities:

Bit (Value)	Description
=====	=====
Bit 0 (0x000X)	IPv6 stack capability
Bit 1 (0x000X)	Reserved
Bit 2 (0x000X)	Reserved
.	.
.	.
Bit 14 (0xX000)	Reserved
Bit 15 (0xX000)	Reserved

## 8. Forwarding

### 8.1. Non-IP or Non-ARP Traffic

In an IPLS VPN, a PE forwards only IP and ARP traffic. All other frames are dropped silently. If the CEs must pass non-IP traffic to each other, they must do so through IP tunnels that terminate at the CEs themselves.

### 8.2. Unicast IP Traffic

In IPLS, IP traffic is forwarded from the AC to the PW based on the destination MAC address of the L2 frame (and not based on the IP header).

The PE identifies the FIB associated with an IPLS instance based on the AC or the PW label. When a frame is received from an AC, the PE uses the destination MAC address as the lookup key. When a frame is received from a PW, the PE uses the PW label as the lookup key. The frame is dropped if the lookup fails.

For IPv6 support, the unicast IP ICMP frame of Neighbor Discovery Protocol [RFC4861] is bi-casted; one copy is submitted to the control plane and other copy to the PW, based on the destination MAC address.

### 8.3. Broadcasts and Multicast IP Traffic

When the destination MAC address is either broadcast or multicast, a copy of the frame is sent to the control plane for CE discovery purposes (see Section 4.1). It is important to note that stricter rate-limiting criteria is applied to frames sent to the control plane, in order to avoid overwhelming it under adverse conditions such as DoS attacks. The service provider should also provide a configurable limitation to prevent the overflowing of the learned source addresses in a given IPLS instance. Also, caution must be used such that only link-local multicasts and broadcast IP packets are sent to the control plane.

When a multicast/broadcast IP packet is received from an AC, the PE replicates it onto the Send Multicast Replication Tree (see Section 5.3). When a multicast/broadcast IP Ethernet frame is received from a PW, the PE forwards a copy of the frame to all the ACs associated with the respective IPLS VPN instance. Note that 'multicast' PW uses Ethernet encapsulation; hence, it does not require additional header manipulations.

#### 8.4. ARP Traffic

When a broadcast ARP frame is received over the AC, a copy of the frame is sent to the control plane for CE discovery purposes. The PE replicates the frame onto the Send Multicast Replication Tree (see Section 5.3), which results in a copy to be delivered to all the remote PEs on the 'multicast' PW and other local CEs through the egress ACs.

When a broadcast Ethernet ARP frame is received over the 'multicast' PW, a copy of the Ethernet ARP frame is sent to all the ACs associated with the IPLS instance.

When a unicast Ethernet ARP frame is received over the AC, a copy of the frame is sent to the control plane for CE discovery purposes. The PE may optionally do destination MAC address lookup in the forwarding table and send the ARP frame to a specific egress interface (AC or 'multicast' PW to a remote PE) or replicate the frame onto the Send Multicast Replication Tree (see Section 5.3).

When a unicast ARP Ethernet frame is received over the 'multicast' PW, the PE may optionally do destination MAC address lookup in the forwarding table and forward it to the AC where the CE is located. If the CE is not accessible through any local AC, the frame is dropped. Conversely, the PE may simply forward the frame to all the ACs associated with that IPLS instance without any lookup in the forwarding table.

#### 8.5. Discovery of IPv6 CE Devices

A PE device that supports IPv6 MUST be capable of:

- Intercepting ICMPv6 Neighbor Discovery [RFC4861] packets received over the AC.
- Recording the IPv6 interface addresses and CE link-layer addresses present in these packets
- Forwarding them towards the original destination. A PE device may also intercept Router Discovery packets in order to discover the link-layer address and IPv6 interface address(es) of the CE. The following sections describe the details.

The PE device MUST learn the link-layer address of the local CE and be able to use it when forwarding traffic between CEs. The PE MAY also wish to monitor the source link-layer address of data packets

received from the CE and discard packets not matching its learned CE link-layer address. The PE device may also optionally learn a list of CE IPv6 interface addresses for its directly attached CE.

#### 8.5.1. Processing of Neighbor Solicitations

When a multicast NS frame is received over the AC, a copy of the frame is sent to the control plane for CE discovery purposes. The PE replicates the frame onto the Send Multicast Replication Tree (see Section 5.3), which results in a copy to be delivered to all the remote PEs on the 'multicast' PW and other local CEs through the egress ACs. The PE may optionally learn an IPv6 interface address (If provided -- this will not be the case for Duplicate Address Detection) when present.

When a multicast Ethernet NS frame is received over the 'multicast' PW, a copy is sent to all the ACs associated with the IPLS instance.

#### 8.5.2. Processing of Neighbor Advertisements

When a unicast NA is received over the AC, a copy of the frame is sent to the control plane for the CE discovery purposes. The PE may optionally do destination MAC address lookup in the forwarding table and send the NA frame to a specific egress interface (AC or 'multicast' PW to a remote PE) or replicate the frame onto the Send Multicast Replication Tree (see Section 5.3).

Optionally, the PE could learn the IPv6 Interface address of the CE.

When a unicast NA frame is received over the 'multicast' PW, the PE may optionally do destination MAC address lookup in the forwarding table and forward it to the AC where the CE is located. If the CE is not accessible through any local AC, the frame is dropped. Conversely, the PE may simply forward the frame to all the ACs associated with that IPLS instance without any lookup in the forwarding table.

#### 8.5.3. Processing of Inverse Neighbor Solicitations and Advertisement

Inverse Neighbor Discovery is typically used on non-broadcast links, but is allowed on broadcast links as well [RFC3122]. A PE may optionally intercept Inverse Neighbor Solicitation and Advertisement and learn the MAC and IPv6 interface address list of the attached CE from the copy of the frame sent to the control plane. The PE may optionally do destination MAC address lookup in the forwarding table and send another copy of the frame to a specific egress interface (AC or 'multicast' PW to a remote PE) or replicate the frame onto the Send Multicast Replication Tree (see Section 5.3).

#### 8.5.4. Processing of Router Solicitations and Advertisements

RSs are multicast while RAs can be unicast or multicast Ethernet frames. The PE could optionally intercept RS and RA frames and send a copy to the control plane. The PE may learn the MAC address and a list of interface addresses for the attached CE.

For unicast RA, the PE may optionally do destination MAC address lookup in the forwarding table and send the RA frame to a specific egress interface (AC or 'multicast' PW to a remote PE) or replicate the frame onto the Send Multicast Replication Tree (see Section 5.3). The multicast RA and RS Ethernet frames are replicated using the Send Multicast Replication Tree as described in Section 5.3.

#### 8.6. Encapsulation

The Ethernet MAC header of a unicast IP packet received from an AC is stripped before forwarding the frame to the unicast PW. However, the MAC header is retained for the following cases,

- when a frame is a unicast IP packet that is directed to a local AC.
- when a frame is a broadcast/multicast IP packet
- when a frame is an ARP packet
- when a frame is Neighbor/Router Solicitation/Advertisement

An IP frame received over a unicast PW is prepended with a MAC header before transmitting it on the appropriate AC(s). The fields in the MAC header are filled in as follows:

- The destination MAC address is the MAC address associated with the PW label in the FIB.
- The source MAC address is the PE's own local MAC address or a MAC address that has been specially configured on the PE for this use.
- The Ethernet Type field is 0x0800 if IPv4 or 0x86DD if IPv6 [RFC2464].
- The frame may be IEEE 802.1Q tagged based on the VLAN information associated with the AC.

A Frame Check Sequence (FCS) is appended to the frame.

## 9. Attaching to IPLS via ATM or Frame Relay (FR)

In addition to (i) an Ethernet port and a (ii) combination of Ethernet port and a VLAN ID, an AC to IPLS may also be (iii) an ATM or FR Virtual Circuit (VC) carrying encapsulated bridged Ethernet frames or (iv) the combination of an ATM or FR VC and a VLAN ID.

The ATM/FR VC is just used as a way to transport Ethernet frames between a customer site and the PE. The PE terminates the ATM/FR VC and operates on the encapsulated Ethernet frames exactly as if those were received on a local Ethernet interface. When a frame is propagated from PW to an ATM or FR VC, the PE prepends the Ethernet frame with the appropriate bridged encapsulation header as defined in [RFC2684] and [RFC2427], respectively. Operation of an IPLS over ATM/FR VC is exactly as described above, with the exception that the AC is then identified via the ATM VCI/VPI or Frame Relay Data Link Connection Identifier (DLCI) (instead of via a local Ethernet port ID), or a combination of those with a VLAN ID.

## 10. VPLS vs. IPLS

The VPLS approach proposed in [RFC4762] provides VPN services for IP as well as other protocols. The IPLS approach described in this document is similar to VPLS in many respects:

- It provides a Provider-Provisioned Virtual LAN service with multipoint capability where a CE connected via a single attachment circuit can reach many remote CEs
- It appears as a broadcast domain and a single subnet
- Forwarding is based on destination MAC addresses

However, unlike VPLS, IPLS is restricted to IP traffic only. By restricting the scope of the service to the predominant type of traffic in today's environment, IPLS eliminates the need for service provider edge routers to implement some bridging functions such as MAC address learning in the data path (by, instead, distributing MAC information in the control plane). Thus, this solution offers a number of benefits:

- It facilitates Virtual LAN services in instances where PE devices cannot or cannot efficiently (or are specifically configured not to) perform MAC address learning.
- Unknown Unicast frames are never flooded as would be the case in VPLS.



- Encapsulation is more efficient (the MAC header is stripped) for unicast IP packets while traversing the backbone network.
- PE devices are not burdened with the processing overhead associated with traditional bridging (e.g., Spanning Tree Protocol (STP) processing, etc.). Note, however, that some of these overheads (e.g., STP processing) could optionally be turned off with a VPLS solution in the case where it is known that only IP devices are interconnected.
- Loops (perhaps through backdoor links) are minimized since a PE could easily reject (via label release) a duplicate IP to MAC address advertisement.
- Greater control over CE topology distribution is available.

## 11. IP Protocols

The solution described in this document offers IPLS service for IPv4 and IPv6 traffic only. For this reason, the MAC header is not carried over the unicast PW. It is reconstructed by the PE when receiving a packet from a unicast PW and the Ethertype 0x0800 or 0x86DD is used in the MAC header since IPv4 or IPv6, respectively, is assumed.

However, this solution may be extended to carry other types of important traffic such as IS-IS, which does not use Ethernet-II, an EtherType-based header. In order to permit the propagation of such packets correctly, one may create a separate set of PWs, or pass protocol information in the "control word" of a "multiprotocol" PW, or encapsulate the Ethernet MAC header in the PW. The selection of appropriate multiplexing/demultiplexing schemes is the subject of future study. The current document focuses on IPLS service for IPv4 and IPv6 traffic.

## 12. Dual-Homing with IPLS

As stated in previous sections, IPLS prohibits the connection of a common LAN or VLAN to more than one PE. However, the CE device itself can connect to more than one instance of IPLS through two separate LAN or VLAN connections to separate PEs. To the CE IP device, these separate connections appear as connections to two IP subnets. The failure of reachability through one subnet is then resolved via the other subnet using IP routing protocols.

### 13. Proxy ARP Function

The earlier version of this proposal used IP-PW to carry both the broadcast/multicast and unicast IP traffic. It also discussed how PE proxy functionality responds to the ARP requests of the local CE on behalf of remote CE. The current version of the document eliminated these functions and instead uses Ethernet PW to carry broadcast, multicast and ARP frames to remote PEs. The motivation to use Ethernet PW and propagate ARP frames in the current version is to support configuration like back-to-back IPLS (similar to Inter-AS option-A configurations in [RFC4364]).

The termination and controlled propagation of ARP frames is still a desirable option for security, DoS, and other purposes. For these reasons, we reintroduce the ARP Proxy [RFC925] function in this revision as an optional feature. The following sections describe this option.

#### 13.1. ARP Proxy - Responder

As a local configuration, a PE can enable the ARP Proxy Responder function. In this mode, the local PE responds to ARP requests received over the Attachment Circuit via learned IP and MAC address associations, which are advertised by the remote PEs. In addition, the PE may utilize local policies to determine if ARP requests should be responded based on the source of the ARP request, rate at which the ARP requests are generated, etc. In a nutshell, when this feature is enabled, ARP requests are not propagated to remote PE routers that are members of the same IPLS instance.

#### 13.2. ARP Proxy - Generator

As a local configuration, a PE can enable the ARP Proxy Generator function. In this mode, the PE generates an ARP request for each IP and MAC address association received from the remote PEs. The remote CE's IP and MAC address is used as the source information in the ARP request while the destination IP address in the request is obtained from the local configuration (that is, user needs to configure an IP address when this feature is enabled). The ARP request is sent on the ACs that have ARP Proxy Generator enabled and is associated with the given IPLS instance.

In addition, the PE may utilize local policies to determine which IP/MAC addresses are candidate for ARP request generation.

The ARP Proxy Generator feature is required to support back-to-back IPLS configuration when any member of the IPLS instance is using the ARP Proxy Responder function. An example of a back-to-back IPLS is a

configuration where PE-1 (ASBR) in an IPLS cloud in one Autonomous System (say, AS-1) is connected via an AC to another PE-2 (ASBR) in an IPLS cloud in another Autonomous System (say, AS- 2) where each PE appears as CE to each other. Such configuration is described in [RFC4364] as option-A for inter-AS connectivity. The Proxy ARP Responder feature prevents propagation of ARP requests to PE-1 (ASBR) in AS-1. This necessitates that PE-1 (ASBR) in AS-1 generates an ARP request on behalf of each CE connected to the IPLS instance in AS-1 as a mean to 'advertise' the reachability to IPLS cloud in AS-2.

#### 14. Data Center Applicability

The resurgence of interest in providing an IP/MPLS-based solution for Data Center Networks (DCNs) deserves another look at the IPLS methodologies described in this document. The key requirement of a DCN to permit Virtual Machine (VM) mobility within or across a DCN necessitates extending the reachability of IP subnet over a LAN, transparently. In addition, VMs tendency to generate frequent gratuitous ARPs for location discovery necessitates a solution that curbs broadcasts closest to the source.

The IPLS solution facilitates VM mobility by the PE closest to the new location signaling the MAC address to all remote peers. In addition, control-plane-based MAC learning mechanisms prevent flooding of unknown unicast across a DCN. The optional ARP proxy mechanisms further reduce ARP broadcast floods by preventing its reach across a local PE.

#### 15. Security Considerations

A more comprehensive description of the security issues involved in L2VPNs are covered in [RFC4111]. Most of the security issues can be avoided through implementation of appropriate guards. The security aspect of this solution is addressed for two planes: the control plane and data plane.

##### 15.1. Control-Plane Security

The control-plane security pertains to establishing the LDP connection, PW establishment and CE's IP and MAC address distribution. The LDP connection between two trusted PEs can be achieved by each PE verifying the incoming connection against the configured peer's address and authenticating the LDP messages by verifying keyed digests. The PW establishments between two secure LDP peers do not pose security issue but mis-wiring could occur due to configuration error. Some checks, such as, proper PW type and other PW options may prevent mis-wiring due to configuration errors.

The learning of the appropriate CE's IP and MAC address can be a security issue. It is expected that the local attachment circuit to CE be physically secured. If this is a concern, the PE must be configured with the CE's IP and MAC address. During each ARP frame processing, the PE must verify the received information against the configuration before accepting. This prevents theft of service, denial of service to a subscriber, or DoS attacks to all subscribers by malicious use of network services.

The IPLS also provides MAC anti-spoofing by preventing the use of already known MAC address. For instance, if a PE has already learned a presence of a CE through a local connection or from another PE, and subsequently an advertisement for the same MAC and/or IP address is received from a different PE, the receiving PE can terminate service to that CE (either through label release and/or removing the ARP entry from the FIB) and raise the alarm.

The IPLS learns and distributes CE reachability through the control plane. This provides greater control over CE topology distribution through the application of local policies.

#### 15.2. Data-Plane Security

The data traffic between the CE and PE is not encrypted. In an insecure environment, it is possible that a malicious user may tap into the CE-to-PE connection and could conduct an active or passive attack. An example of an active attack would be generating traffic using the spoofed destination MAC address on the Ethernet Attachment Circuit and a passive attack could include targeted or passive monitoring between the CE and PE. In order to avoid such hijacking, the local PE may verify the source MAC address of the received frame against the MAC address of the admitted connection. The frame is forwarded to the PW only when authenticity is verified. When spoofing is detected, the PE must sever the connection with the local CE, tear down the PW, and start over.

Each IPLS instance uses its own FIB. This prevents leaking of one customer data into another.

## 16. References

## 16.1. Normative References

- [IEEE802.1D] ISO/IEC 10038, ANSI/IEEE Std 15802-3:1998, "MAC Bridges".
- [RFC826] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982, <<http://www.rfc-editor.org/info/rfc826>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998, <<http://www.rfc-editor.org/info/rfc2464>>.
- [RFC3122] Conta, A., "Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification", RFC 3122, June 2001, <<http://www.rfc-editor.org/info/rfc3122>>.
- [RFC4446] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", BCP 116, RFC 4446, April 2006, <<http://www.rfc-editor.org/info/rfc4446>>.
- [RFC4447] Martini, L., Ed., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006, <<http://www.rfc-editor.org/info/rfc4447>>.
- [RFC4448] Martini, L., Ed., Rosen, E., El-Aawar, N., and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, April 2006, <<http://www.rfc-editor.org/info/rfc4448>>.

- [RFC4762] Lasserre, M., Ed., and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", RFC 4762, January 2007, <<http://www.rfc-editor.org/info/rfc4762>>.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007, <<http://www.rfc-editor.org/info/rfc4861>>.
- [RFC5036] Andersson, L., Ed., Minei, I., Ed., and B. Thomas, Ed., "LDP Specification", RFC 5036, October 2007, <<http://www.rfc-editor.org/info/rfc5036>>.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008, <<http://www.rfc-editor.org/info/rfc5226>>.

## 16.2. Informative References

- [ADDR-IANA] IANA, "Address Family Numbers", <http://www.iana.org/assignments/address-family-numbers/>.
- [RFC925] Postel, J., "Multi-LAN address resolution", RFC 925, October 1984, <<http://www.rfc-editor.org/info/rfc925>>.
- [RFC2427] Brown, C. and A. Malis, "Multiprotocol Interconnect over Frame Relay", STD 55, RFC 2427, September 1998, <<http://www.rfc-editor.org/info/rfc2427>>.
- [RFC2684] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", RFC 2684, September 1999, <<http://www.rfc-editor.org/info/rfc2684>>.
- [RFC4111] Fang, L., Ed., "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4111, July 2005, <<http://www.rfc-editor.org/info/rfc4111>>.

- [RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006, <<http://www.rfc-editor.org/info/rfc4364>>.
- [RFC4664] Andersson, L., Ed., and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, September 2006, <<http://www.rfc-editor.org/info/rfc4664>>.
- [RFC4665] Augustyn, W., Ed., and Y. Serbest, Ed., "Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks", RFC 4665, September 2006, <<http://www.rfc-editor.org/info/rfc4665>>.
- [RFC5771] Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for IPv4 Multicast Address Assignments", BCP 51, RFC 5771, March 2010, <<http://www.rfc-editor.org/info/rfc5771>>.
- [RFC6074] Rosen, E., Davie, B., Radoaca, V., and W. Luo, "Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)", RFC 6074, January 2011, <<http://www.rfc-editor.org/info/rfc6074>>.

#### Acknowledgements

Authors would like to thank Alp Dibirdi from Alcatel, Xiaohu Xu from Huawei, and other L2VPN working group members for their valuable comments.

#### Contributors

This document is the combined effort of the following individuals and many others who have carefully reviewed this document and provided the technical clarifications.

K. Arvind	Fortress
Vach Kompella	Alcatel-Lucent
Matthew Bocci	Alcatel-Lucent
Shane Amante	Apple

## Authors' Addresses

Himanshu Shah  
Ciena Corp  
3939 North 1st Street  
San Jose, CA 95110  
United States

E-Mail: hshah@ciena.com

Eric Rosen  
Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA, 01886  
United States

E-Mail: erosen@juniper.net

Francois Le Faucheur  
Cisco Systems, Inc.  
Batiment D, 45 Allee des Ormes  
06254 Mougins  
France

E-Mail: flefauch@cisco.com

Giles Heron  
Cisco Systems  
9-11 New Square  
Bedfont Lakes  
Feltham  
Middlesex  
TW14 8HA  
United Kingdom

E-Mail: giheron@cisco.com



