Individual Submission
Internet-Draft
Intended status: Standards Track
Expires: 16 October 2026

Abhishek Garg
Ciena

14 April 2026

Method to enable signaling of L2VPN services using SRv6 extensions
draft-garg-l2vpn-over-srv6-00

Abstract

This document describes a mechanism to provide L2VPN services using Segment Routing over IPv6 (SRv6), eliminating the need for a separate signaling protocol for VPN label distribution.

In current deployments, L2VPN services rely on dedicated protocols such as Label Distribution Protocol (LDP) or Border Gateway Protocol (BGP) for service label signaling, which adds control-plane complexity.

The proposed mechanism introduces an SRv6-based extension that enables L2VPN service identification within the SRv6 framework.

This approach reduces control-plane overhead and provides a simplified and efficient solution for L2VPN service delivery.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 16 October 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Problem Statement 3
3. Proposed Solution 3
4. Detailed Mechanism 3
4.1. End.L2VPN SID Generation 4
4.2. Signaling of L2VPN 4
5. Example 4
5.1. Control Plane 5
5.2. Data Plane 6
6. Security Considerations 6
7. IANA Considerations 6
7.1. L2VPN SRv6 Service TLV 7
8. References 7
8.1. Normative References 7
8.2. Informative References 8
Author's Address 8

1. Introduction

Layer 2 Virtual Private Network (L2VPN) services are widely deployed across service provider and data center networks to provide connectivity between geographically distributed sites.

These services typically rely on two protocols for transport and service signaling.

With the evolution of networking technologies, Segment Routing over IPv6 (SRv6) has emerged as a flexible and scalable approach for traffic engineering and service delivery, as described in [RFC8402] and [RFC8986].

In parallel, network environments continue to include a mix of modern and legacy devices, with varying capabilities and scalability constraints.

This document focuses on improving L2VPN services with the help of an SRv6 extension.

2. Problem Statement

L2VPN services are widely deployed across service provider (SP) and data center (DC) networks. Existing solutions typically require separate mechanisms for transport and service identification, resulting in additional label overhead and dependency on multiple control-plane protocols. These protocols must remain synchronized for correct operation, which increases operational complexity and may lead to service issues in case of inconsistency.

Current approaches, such as Ethernet VPN (EVPN) over SRv6, reduce data-plane complexity but rely heavily on BGP, which can introduce scalability challenges, particularly on resource-constrained devices.

In many deployments, lightweight L2VPN services are required for use cases such as management traffic or small-scale data center interconnect (DCI), where existing solutions may be overly complex.

Therefore, there is a need for a simplified and scalable L2VPN mechanism with reduced control-plane overhead and improved operational efficiency.

3. Proposed Solution

This document proposes a simplified L2VPN mechanism based on Segment Routing over SRv6, eliminating the need for separate signaling protocols for transport and service identification.

In the proposed approach, SRv6 is used for both transport and pseudowire (PW) signaling, thereby reducing the dependency on multiple control-plane protocols. This unification simplifies service provisioning and reduces operational overhead.

In a typical SRv6 deployment, an Endpoint SID (End SID) derived from an SRv6 locator is used to provide end-to-end transport connectivity.

This document extends the same concept to L2VPN services by introducing an SRv6 endpoint function that represents the L2VPN service. This function, referred to as End.L2VPN, enables both service identification and forwarding behavior within the SRv6 framework.

By leveraging SRv6 for both transport and service layers, the proposed mechanism reduces control-plane complexity and avoids the need for maintaining separate label spaces or signaling protocols.

4. Detailed Mechanism

4.1. End.L2VPN SID Generation

A PW-ID that is unique in an L2VPN instance can be used to generate an End.L2VPN SID. One implementation model is to derive the service-specific portion of the SID from the PW-ID.

For example, if a PE has PW 11 configured, the decimal value 11 can be converted to hexadecimal B and combined with the local End SID structure to form an End.L2VPN SID.

4.2. Signaling of L2VPN

To signal L2VPN services, this document introduces a new IGP advertisement that carries L2VPN pseudowire information. In the example described here, the signaling is carried in IS-IS. Equivalent advertisement in other IGPs is outside the scope of this document.

An IS-IS LSP carries the L2VPN information in a new TLV. The TLV includes at least the following information:

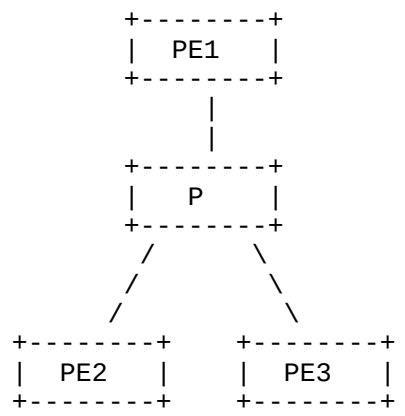
* PW-ID
* End.L2VPN SID
* Neighbor IP address
* MTU
* Control word

This list includes the key parameters associated with an L2VPN PW from both the control-plane and data-plane perspective.

A receiving PE should verify that PW-ID, peer address, MTU, and control-word related parameters are consistent with the locally configured service before installing forwarding state for the remote End.L2VPN SID.

5. Example

Suppose there is a topology with three PE devices connected through one P device. IS-IS and SRv6 are configured on all nodes, and PW configuration is present on the PE devices.



IS-IS IPv6 and SRv6 configuration are present on all nodes. PW 10 is configured between PE1 and PE2, PW 11 is configured between PE1 and PE3, and PW 12 is configured between PE3 and PE2.

* PE1 loopback: 1::1/128

* PE1 End SID: 2001:db8:bbbb:A::/64

* PE2 loopback: 2::2/128

* PE2 End SID: 2001:db8:bbbb:B::/64

* PE3 loopback: 3::3/128

* PE3 End SID: 2001:db8:bbbb:C::/64

The example below focuses on PW 11 between PE1 and PE3.

PE1 PW config

#L2VPN-srv6 pw-id 11 neighbor 3::3

PE3 PW config

#L2VPN-srv6 pw-id 11 neighbor 1::1

5.1. Control Plane

After pseudowire configuration, an IS-IS LSP advertises a new TLV carrying PW information. When PE1 receives the update from PE3, it examines the L2VPN TLV in the IS-IS LSP PDU and verifies parameters such as PW-ID, control word, MTU, and neighbor loopback address.

If PW 11 and the loopback address in the message match the locally configured service on PE1, PE1 installs the PE3 PW 11 End.L2VPN SID 2001:db8:bbbb:C::B/64 in its SRv6 forwarding table. The same process occurs on PE3 when it receives the matching advertisement from PE1, and PE3 installs 2001:db8:bbbb:A::B/64 in its SRv6 forwarding table.

5.2. Data Plane

When PE1 detects traffic on the attachment circuit for PW 11, it checks the SRv6 forwarding table, finds the remote End.L2VPN SID for PW 11, and creates an IPv6 header with destination address 2001:db8:bbbb:C::B. The L2VPN payload is then encapsulated in the IPv6 packet.

When the P device receives the IPv6 packet, it looks up the destination SID in its SRv6 forwarding table. Because the locator or End SID for PE3, 2001:db8:bbbb:C::/64, is already present in the SRv6 forwarding table, the packet is forwarded toward PE3.

When PE3 receives the packet, it looks up the destination address in its SRv6 forwarding table, finds the mapping to PW 11, decapsulates the packet, and forwards the L2VPN traffic toward the PW 11 attachment circuit.

6. Security Considerations

This document introduces a new signaling element that can influence pseudowire forwarding state. Incorrect, spoofed, or unauthorized TLV advertisements could redirect traffic, blackhole traffic, or cause unintended pseudowire bindings to be installed.

A receiving PE must validate that the advertised PW-ID, peer address, and service parameters match locally provisioned state before it installs forwarding state derived from the received advertisement.

Implementations and deployments should use the security mechanisms available for the underlying IGP carrying this information. Operators should also consider the impact of stale advertisements, replayed information, and excessive service advertisements on nodes with constrained resources.

7. IANA Considerations

This document requests one new codepoint allocation from the "IS-IS TLV Codepoints" registry for an L2VPN SRv6 Service TLV.

The registration should contain the following information:

* Value: To be assigned by IANA

* Description: L2VPN SRv6 Service TLV

* Reference: This document

The TLV carries L2VPN pseudowire service information, including PW-ID, peer address, End.L2VPN SID, Layer-2 MTU, encapsulation type, control-word capability, and optional service-status information.

This document does not request any sub-TLV codepoint assignment. Such allocations may be defined by future documents if needed.

7.1. L2VPN SRv6 Service TLV

The TLV format is summarized as follows:

* Type: TBD by IANA

* Length: Variable

* PW-ID

* Neighbor Address: IPv6 loopback address of the remote PE

* End.L2VPN SID: SRv6 service SID associated with the pseudowire

* Layer-2 MTU

* Encap-Type: PW type, for example VLAN or Ethernet

* Control-Flag: indicates whether control word is enabled

* Optional Sub-TLVs: may carry status or future extensions

If a PW status sub-TLV is present, it may indicate operational state, including whether the pseudowire is forwarding and whether attachment-circuit or PSN-facing faults have been detected.

8. References

8.1. Normative References

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

8.2. Informative References

Author’s Address

Abhishek Garg
Ciena
Email: abhishekgarg.vip@gmail.com