BESS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 10 November 2025

P. Brissette, Ed.
Cisco Systems
W. Lin
Juniper
J. Rabadan
Nokia
J. Uttaro
ATT
B. Wen
Comcast

9 May 2025

EVPN-VPWS Seamless Integration with L2VPN VPWS
draft-ietf-bess-evpn-vpws-seamless-02

Abstract

This document presents a solution for migrating L2VPN Virtual Private Wire Service (VPWS) to Ethernet VPN Virtual Private Wire Service (EVPN-VPWS) services. The solution allows the coexistence of EVPN and L2VPN services under the same point-to-point VPN instance. By using this seamless integration solution, a service provider can introduce EVPN into their existing L2VPN network or migrate from an existing L2VPN based network to EVPN. The migration may be done per pseudowire or per flexible-crossconnect (FXC) service basis. This document specifies control-plane and forwarding behaviors.

Requirements Language

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] and RFC 8174 [RFC8174].

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/.

Table of Contents

1. Introduction

Point-to-point L2VPN solutions are specified in [RFC8077] when LDP-based pseudowire are offered. BGP-based L2VPN service may also offer point-to-point service using [RFC6624] or by setting up auto-discovered VPN members using [RFC6074] and then the pseudowires using [RFC8077].

EVPN-VPWS leverages the latest EVPN technology and brings extra functions to Layer 2 point-to-point Ethernet service, such as all-active redundancy, load balancing and mass withdrawal. All-active redundancy also makes it easier to achieve fast convergence on an access link or node failure.

When expanding an existing L2VPN network with Ethernet encapsulation, a service provider may want to deploy EVPN-VPWS to provide additional Layer 2 point-to-point Ethernet services, and at the same time some of the customer traffic may still need to be terminated on the existing L2VPN PEs within the service provider network.

This document describes a seamless-integration solution that allows the co-existence of L2VPN point-to-point Ethernet services and EVPN-VPWS procedure per [RFC8214] under the same VPN network and over the same MPLS/IP network. Service providers may also use the seamless integration solution to migrate traditional L2VPN network to EVPN-VPWS based network.

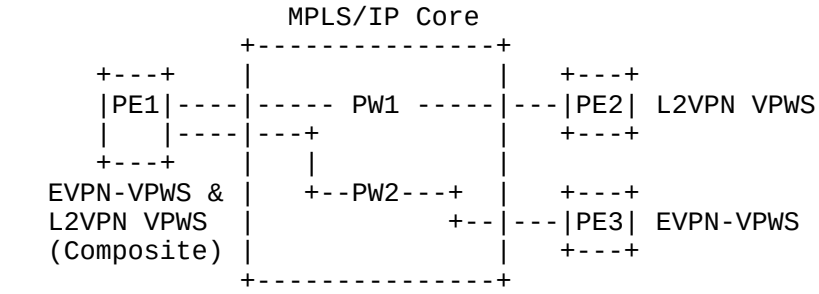

Figure 1

Seamless Integration of EVPN-VPWS.

Figure 1 shows a network where PE1 runs in hybrid mode (EVPN-VPWS and legacy L2VPN VPWS). PE1 has established a pseudowire (PW1) with PE2 running L2VPN VPWS. Also, it has initiated another pseudowire (PW2) with PE3 running EVPN-VPWS. In the future, PE2 may be upgraded to EVPN-VPWS seamlessly. The seamless integration solution described in this document has the following attributes:

- It is backward compatible with [RFC8214] and EVPN Flexible crossconnect service [RFC9744] documents.

- New PEs can leverage the multi-homing mechanisms and provisioning simplifications of EVPN Ethernet-Segment framework:

a. Auto-sensing of MHN / MHD

b. Auto-discovery of redundancy groups

c. Auto-election of Designated Forwarder and VLAN carving

d. Support of various load-balancing modes such as port-active, single-active and all-active

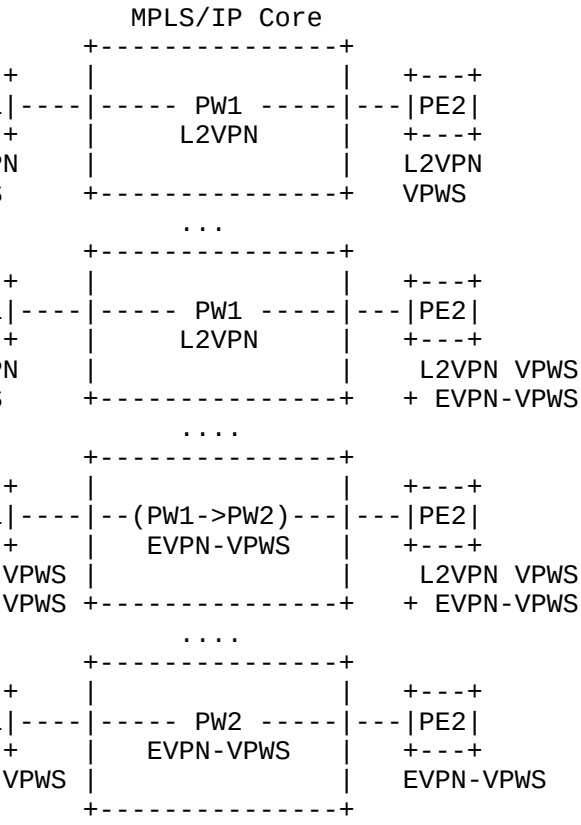

Figure 2

Migration from L2VPN to EVPN-VPWS.

Figure 2 illustrates the migration of a L2VPN VPWS brownfield network to EVPN-VPWS. Initially PE1 and PE2 have a L2VPN PW established between them. First, a network operator may upgrade PE2 to enable EVPN-VPWS. Once upgraded, PE2 which now has the EVPN-VPWS capability still runs L2VPN PW with PE1. Later on, a network operator may decide to upgrade PE1 to support EVPN-VPWS. As soon as the upgrade is completed, PE1 and PE2 auto-discover their respective EVPN routes and the corresponding point-to-point service. That EVPN-VPWS service takes higher precedence over existing legacy L2VPN pseudowire. Finally, the network operator may safely remove any legacy configurations from PE1 and PE2 nodes while PW remains established using EVPN-VPWS.

2. Terms and Abbreviations

* CE: A Customer Edge device, e.g., a host, router, or switch.

* DF: EVPN Ethernet Segment Designated Forwarder.

* NDF: EVPN Ethernet Segment Non-Designated Forwarder.

* Ethernet Segment (ES): Refers to a set of Ethernet links connecting a customer site (device or network of devices) to one or more PEs.

* Virtual Ethernet Segment (vES): Refers to a subset of Ethernet links connecting customer site (device or network of devices) to one or more PEs. All procedures listed in all-active and single-active mutli-homing apply; but not port-active.

* Ethernet Tag: An Ethernet Tag identifies a particular pseudowire, e.g. a PW-ID as per [RFC8214].

* FEC: Forwarding Equivalence Class.

* homogeneous PEs: Refers to PEs that are of the same types.

* LDP-LM: LDP Label Mapping Message.

* LDP-LW: LDP Label Withdraw Message.

* LSP: Label Switched Path.

* MHD: Multi-Homed Device.

* MHN: Multi-Homed Network.

* P2P: Point to Point - a P2P LSP typically refers to a LSP for Layer2 pseudowire.

* PE: Provider Edge device.

* VPWS: Virtual Private Wire Service. It refers to L2VPN VPWS circuit where pseudowires are signaled using LDP or BGP-AD protocol. The latter is referred as VPWS A-D.

* EVPN-VPWS: Ethernet-VPN Virtual Private Wire Service. It refers to EVPN-VPWS circuit where pseudowires are signaled via BGP-EVPN. It can also refer to [RFC9744].

* EVPN-FXC: Ethernet-VPN Flexible Cross-connect Service [RFC9744].

* Port-Active Redundancy Mode: When only a single PE, among all the PEs attached to an Ethernet segment, is allowed to forward traffic to/from that Ethernet segment for a given interface, then the Ethernet Segment is defined to be operating in Port-Active redundancy mode.

* Single-Active Redundancy Mode: When only a single PE, among all the PEs attached to an Ethernet segment, is allowed to forward traffic to/from that Ethernet segment for a given VLAN, then the Ethernet Segment is defined to be operating in Single-Active redundancy mode.

* All-Active Redundancy Mode: When all PEs attached to an Ethernet Segment are allowed to forward traffic to/from that Ethernet segment for a given VLAN, then the Ethernet segment is defined to be operating in All-Active redundancy mode.

* VPWS A-D: Refers to Virtual Private Wire Services with BGP-based Auto Discovery as in [RFC6074].

* PW: Pseudowire

3. L2VPN PE, EVPN-VPWS PE and Composite PE

There are three types of PEs defined in the seamless integration solution: L2VPN PE, EVPN-VPWS PE and composite PE. Under a given Layer 2 Ethernet VPN, the type of PE is categorized by the technology it is provisioned for. For instance, a PE that is provisioned to use L2VPN and EVPN-VPWS on the same VPN service is considered a composite PE.

Also in this document, in the context of a given Layer 2 Ethernet VPN, an EVPN-VPWS PE is a PE that is provisioned to provide only the EVPN solution per [RFC8214] or [RFC9744] but not a seamless integration solution. It is irrelevant whether an EVPN-VPWS PE is capable to support a seamless integration solution.

For example, for a non-L2VPN PE, a network administrator may know a priori that the PE does not need to establish any P2P Ethernet service that involves L2VPN PE under a given Layer 2 Ethernet VPN instance. In this case, the PE can be provisioned to act only as an EVPN-VPWS PE for that VPN even though it is capable of providing seamless integration procedure. If such prior knowledge is unavailable, then a PE SHALL be provisioned to act as a composite PE if it is capable of. Otherwise, it is unable to establish a P2P Ethernet service with a L2VPN PE.

Unless explicitly specified in this specification, a PE’s type applies to a given Layer 2 Ethernet VPN instance. A PE may act as an EVPN-VPWS PE for one VPN, but as a composite PE for another VPN.

4. Solution Requirements

The seamless integration solution for point-to-point Ethernet VPN meets the following requirements:

* It must allow L2VPN, EVPN-VPWS and composite PEs to participate in the same Layer 2 Ethernet VPN instance.

* The solution MUST allow for staged migration towards EVPN-VPWS on a site-by-site basis - e.g., new EVPN-VPWS sites to be provisioned on EVPN-VPWS Provider Edge devices (PEs). Migration SHOULD be possible on a per-pseudowire basis.

* The solution MUST NOT require any changes to existing L2VPN PEs running Legacy VPWS, unless it is to upgrade them to EVPN-VPWS and make them composite PE.

* The solution MUST allow for the co-existence of composite PE devices running EVPN-VPWS and L2VPN VPWS for the same single-homed and/or multi-homed segments.

* The solution MUST support port-active redundancy of multi-homed networks and multi-homed devices for L2VPN, EVPN-VPWS and composite PEs.

* The solution MUST support single-active redundancy of multi-homed networks and multi-homed devices for L2VPN, EVPN-VPWS and composite PEs.

* The solution SHOULD support all-active redundancy of multi-homed Ethernet Segments for L2VPN, EVPN-VPWS and composite PEs.

* Composite PEs provisioned for all-active multihoming for their multihomed CE(s) MAY work with L2VPN PE(s) working in single home or active-standby multihoming.

These requirements collectively allow for the seamless insertion of the EVPN-VPWS technology into brownfield L2VPN VPWS deployments.

5. Seamless Integration Solution

To support seamless integration, the solution may require L2VPN PEs to setup PWs per [RFC8077] or [RFC6624] or may require L2VPN PEs to setup VPWS service by auto-discovering VPN members using [RFC6074] and then setting up the PWs using [RFC8077]. Furthermore, composite PEs must support BGP EVPN routes per [RFC8214] and as per [RFC9744] and one of a method of legacy VPWS technologies. All the logic for seamless integration SHALL reside on the composite PEs.

A PE participating in a point-to-point Ethernet VPN offers P2P Ethernet services with different remote PEs. By nature of point-to-point service, there is no requirement for full-mesh among all the PEs participating in the same point-to-point Ethernet VPN instance.

The seamless integration solution allows the coexistence of composite PE, L2VPN PE and EVPN-VPWS PE under the same VPN instance. It allows the establishment of P2P Ethernet services over the same MPLS/IP core: (a) between two homogenous PEs, or (b) between a composite PE and a L2VPN PE, or (c) between a composite PE and a EVPN-VPWS PE.

A composite PE can establish a P2P Ethernet service with a L2VPN PE and different a P2P service with the same or a different EVPN-VPWS PE. It is the sole responsibility of a composite PE to seamless integrate with L2VPN PEs and EVPN-VPWS PEs.

There will be no P2P service between an EVPN-VPWS PE and a L2VPN PE in the same L2 Ethernet VPN as an EVPN-VPWS PE is provisioned only to provide the procedure/function per EVPN-VPWS.

6. Capability Discovery

The EVPN-VPWS PEs MUST advertise both BGP VPWS Auto-Discovery (VPWS A-D) route or LDP-LM message as well as the BGP EVPN Ethernet AD per EVI route for a given pseudowire. Auto-discovery is only meaningful to PEs participating in the same VPN.

In the case of L2VPN PEs running VPWS A-D, they may advertise the BGP VPWS A-D route, per the procedures specified in [RFC4664] and [RFC6074] or [RFC6624]. The operator may decide to use the same BGP Route Target (RT) to identify a pseudowire on both EVPN-VPWS and L2VPN networks. In this case, when a L2VPN PE receives the EVPN Ethernet AD per EVI route, it MUST ignore it on the basis that it belongs to an unknown SAFI. However, the operator may choose to use two RTs - one to identify the pseudowire on L2VPN network and another for EVPN-VPWS network and employ RT-constrained route distribution [RFC4684] in order to prevent BGP EVPN routes from reaching the L2VPN PEs.

When an EVPN-VPWS PE receives both a VPWS A-D route or a LDP-LM message as well as an EVPN-VPWS Ethernet AD per EVI route from a given remote PE for the same pseudowire, it MUST give preference to the EVPN-VPWS route for discovery. This ensures that, at the end of the route exchange, all EVPN-VPWS capable PEs discover other EVPN-VPWS capable PEs.

When the discovery phase is completed, the composite PEs have discovered the remote PE per pseudowire along with their associated capability (EVPN-VPWS or L2VPN), whereas the L2VPN PE have discovered the remote PE per pseudowire as if they are L2VPN-only PEs. Basically, a L2VPN PE discovers all L2VPN PEs and all composite PEs participating in the same VPN. However, a L2VPN cannot distinguish a L2VPN from a composite PE. From a point of L2VPN PE, all composite PEs are L2VPN PEs.

Also, an EVPN-VPWS PE discovers all EVPN PEs and all composite PEs participating in the same VPN. Similarly, an EVPN-VPWS PE cannot distinguish an EVPN-VPWS PE from a composite PE. From a point of EVPN-VPWS PE, all composite PEs are EVPN-VPWS PEs.

7. Data Plane Operations

When a packet arrives at an ingress composite PE, the composite PE adds a VPN service label based on the AC that packet arrives at, and it encapsulates the packet and sends it through a pseudowire to the egress PE.

* A composite PE will not forward customer traffic to the L2VPN PE playing a non-DF role

* If a composite PE detects that two or more EVPN-VPWS PEs are attached to the same ES and they are working in all-active mode, it will load balance the traffic among the EVPN-VPWS PEs.

* If a composite PE detects that two or more EVPN-VPWS PEs are attached to the same ES and they are working in single-active mode, it will only forward the traffic to the EVPN-VPWS PE playing a DF role. Similar logic is followed with port-active mode.

* If a set of composites PEs work in all-active multihoming mode for the same multihomed CE, then regardless of DF or Non-DF role each composite PE plays, it may forward the packet received from its multihomed CE to the remote L2VPN DF PE. Detailed description is done in Section 9.3.

* If a composite PE receives both L2VPN and EVPN A-D routes from a remote PE for the same p2p Ethernet service, the composite should install forwarding routes in a make-before-break fashion:

  a. For the traffic coming from the remote PE to its local access interface direction, to achieve a fast failover, the composite may install forwarding routes based on both L2VPN and EVPN A-D routes. However, to save system resources in a scaled setup, the composite may choose to install only the forwarding route for the EVPN A-D route and it should do so before it deletes the forwarding route for the L2VPN A-D route if it was installed beforehand.

  b. For traffic coming from its local access interface to the remote PE direction, only one route can be installed for the same local access interface. Forwarding should be based on the EVPN A-D route. The composite PE should update the forwarding route in a make-before-break fashion if the forwarding route for L2VPN A-D route has already been installed before the processing of the incoming EVPN A-D route.

* If a composite PE receives both L2VPN and EVPN A-D routes from a remote PE for the same p2p Ethernet service, and later on the remote PE has reverted back to a L2VPN only PE and withdraws its EVPN A-D route, the composite PE should also update the forwarding route accordingly in a make-before-break fashion:

  a. For the traffic coming from the remote PE to its local access interface direction, if the forwarding route for the L2VPN A-D route is not there, the composite PE should install the forwarding route for the L2VPN A-D route before it tears down the forwarding route for the EVPN A-D route.

b. For the traffic coming from its local access interface to the remote PE direction, only one route can be installed for the same local access interface. The composite PE should update the forwarding route based on the L2VPN A-D route in a make-before-break fashion.

8. Control Plane Operations

Figure 3 demonstrates a typical brown-field deployment where PE1 is a composite PE and PE2 is a L2VPN PE.

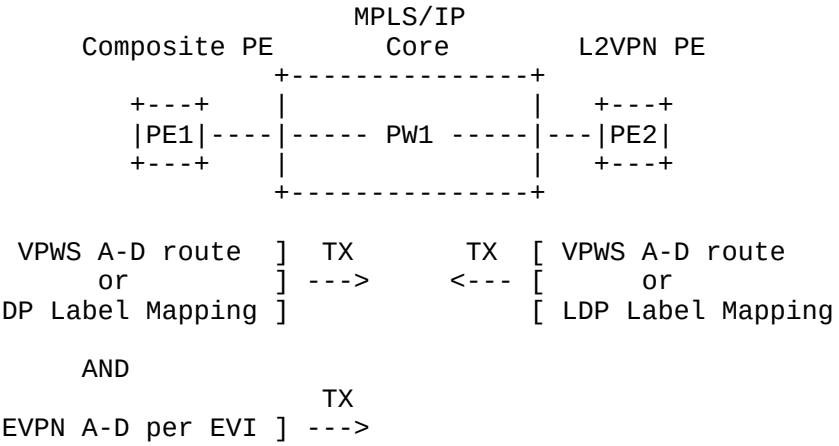

Figure 3

EVPN-VPWS Single-Homed

The control plane procedures of L2VPN PEs are per [RFC8077], [RFC8214] and [RFC4762].

The EVPN-VPWS PE procedures are as follows:

* The composite PE MUST establish a PW to each remote PE from which it has received only a VPWS A-D route or a LDP-LM message for the corresponding pseudowire, and MUST set up the label stack corresponding to the PW FEC.

* If an composite PE receives a VPWS A-D route or a LDP-LM message from a given PE, it sets up a L2VPN VPWS PW to that PE. If it then receives an EVPN Ethernet AD per EVI route for that PW from the same PE, then the composite PE may bring the L2VPN PW operationally down and MUST forward traffic using the label information from the EVPN Ethernet AD per EVI route.

* If an composite PE receives an EVPN Ethernet AD per EVI route followed by a VPWS A-D route or a LDP-LM message from the same PE, then the composite PE will setup the EVPN-VPWS PW. It may keep the L2VPN VPWS PW operationally down and MUST forward traffic using the reachability information from that EVPN Ethernet AD per EVI route.

* For L2VPN PEs not using VPWS A-D or LDP signaling, the composite PEs need to be provisioned manually with PWs to those remote L2VPN PEs for each pseudowire. In that case, if an composite PE receives an EVPN Ethernet AD per EVI route from a PE to which a PW exists, it may keep VPWS PW operationally down and MUST forward traffic using the reachability information from that EVPN Ethernet AD per EVI route.

In the case where a composite PE receives an EVPN Ethernet AD per EVI route for an established L2VPN PW from a different PE, the result should be directed by a local configuration. This is to avoid any security breach where a malicious user may want to steer an existing connection to a different PE.

9. Multi-homed Operations

Figure 4 demonstrates a multi-homing scenario. CE1 is connected to PE1 and PE2 where PE1 is the designated forwarder while PE2 is the non-designated forwarder.

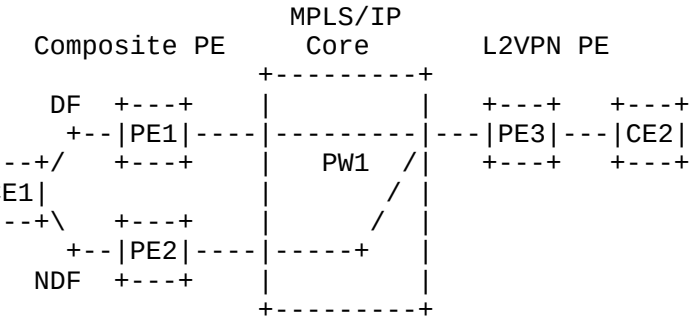

Figure 4

EVPN-VPWS Multi-homing Redundancy

9.1. Operations with Port-Active MH PEs

In Figure 4, PE1 and PE2 are configured in port-active load-balancing mode. Both PEs are advertising EVPN Ethernet AD per ES route with the single-active bit set as described in [I-D.ietf-bess-evpn-mh-pa]. In this example, PE1 is DF elected for the shared Ethernet-Segment identifier.

* Only PE1, as DF, advertises the VPWS A-D route or LDP-LM message towards remote PE3.

* PE1 advertises the EVPN Ethernet AD per EVI route for PW1 towards remote PE3. The P-bit in L2 Attributes Extended Community is set for PE1 as per [RFC8214]. The purpose is to have all required EVPN-VPWS routes on remote PE. During an upgrade from L2VPN to EVPN-VPWS, those remote nodes are immediately upgraded.

* PE2, as NDF, only advertises its EVPN Ethernet AD per EVI route corresponding to that same PW1. The B-bit in L2 Attributes Extended Community is set for PE2 as per [RFC8214]

* If PE3 is running 2-way pseudowire redundancy and PW-status is enabled, PE2 may leverage the existence of standby/backup PW with PE3. In this particular scenario, PE2 may advertise VPWS A-D route or LDP-LM message along with PW-status message

Upon link failure between CE1 and PE1, PE1 and PE2 follow EVPN Ethernet Segment DF Election procedures described in [RFC8214] for EVPN-VPWS. Furthermore, PE1 withdraws its VPWS A-D route or sends LDP-LW message to remote PE3 to teardown the L2VPN PW. Finally, PE2 advertises corresponding VPWS A-D route or LDP-LM message for that PW1 and re-establish L2VPN PW with new PE2 destination.

Once PE3 is upgraded and support EVPN-VPWS, seamless integration procedures are applied. Higher precedence of EVPN-VPWS over L2VPN VPWS allow all PEs to avoid the usage of legacy circuit. Then, non-preferred L2VPN VPWS protocols and configuration may be removed from all PEs.

9.2. Operation with Single-Active MH PEs

Single-active operation is similar to Port-active load-balancing mode described above. The main difference resides in the Designated Forwarder election where the carving is performed at the circuit level instead being of at the port/interface level.

9.3. Operation with All-Active MH PEs

In EVPN-VPWS all-active load-balancing mode, all PEs participating in a redundancy group forward traffic bidirectionally, reducing the importance of DF and NDF PE. However, L2VPN PEs do NOT support all-active peering PEs as remote endpoints.

9.3.1. Falling back to port-active

Composite PE discovering remote L2VPN PE MAY fallback into port-active load-balancing mode. That can be achieved dynamically or by enforcing network operators to configure port-active instead of all-active load-balacing mode. In both cases, port-active multi-homing operations, as described before, apply here

9.3.2. Asymmetric forwarding

As per Figure 4, peering PEs run in all-active load-balancing mode while PE3 behaves as single-homed PE. Asymmetric forwarding consists of transmitting traffic in an all-active manner from peering PEs to PE3 while the reverse direction is done in port-active or single-active manner.

Traffic from CE1 going to PE1 is forwarded to PE3 using the VPN label learned from VPWS AD route or LDP-LM message received from PE3. Traffic from CE1 going to PE2 is forwarded to PE3 using that same VPN label. Traffic coming from CE2 to PE3 gets forwarded only over the primary PW towards PE1; the DF PE. Supporting asymmetric forwarding with L2VPN PE requires extensions to EVPN-VPWS MH procedures.

For BGP VPWS, PE1 and PE2 naturally receive the same label from PE3 via BGP. They can use the same label when sending to PE3. There is no direct need for alias label signaling. For LDP VPWS, since the LDP sessions are targeted, PE1 and PE2 always receive different labels, hence the alias label procedure is needed.

Following rules are applied to achieve expected behavior:

* Peering PEs advertise EVPN Ethernet AD per ES route with the single-active bit unset. That is to get the network ready when remote L2VPN PE are upgraded to composite PE.

* DF PE advertises VPWS AD routes or LDP-LM message and EVPN Ethernet AD per EVI route per PW.

* NDF PE advertises only EVPN Ethernet AD per EVI route per PW.

* If PE3 is running 2-ways pseudowire redundancy, PE2 may leverage the existence of standby/backup PW with PE3. PE2 may advertise VPWS AD route or LDP-LM message with proper PW-status message.

* If PE3 is not running pseudowire redundancy, the tunnel encapsulation attribute [RFC9012] is used to synchronize alias PW label between peering PEs. The tunnel encapsulation attribute, specifying the alias PW label and tunnel endpoint (nexthop) of the remote PE (PE3), is transmitted along with EVPN Ethernet AD per EVI route. The NDF PEs uses that alias VPN label per L2VPN PW as DF PE when transmitting traffic coming from CE (CE1) towards remote PE(PE3).

* Composite PE1 and PE2 do not need similar mechanism for EVPN-VPWS since the same route advertised by PW is received on both PEs.

10. Route Optimization

If a composite PE does not know at priori whether the remote PE for a given P2P service is a L2VPN PE or an EVPN PE, the composite needs to participate in the auto-discovery and signaling procedures for both L2VPN and EVPN-VPWS. This works well as it allows a composite PE to establish a P2P service with different types of PEs, and to switch from using a L2VPN PW to EVPN-VPWS dynamically during the migration process.

A composite PE originates twice as many A-D routes as they are required to establish the number of P2P services it is provisioned to. Therefore in some scenarios, a composite PE should be optimized to perform either L2VPN or EVPN-VPWS procedure for a given P2P service, but not both.

For a composite PE, if a Service Provider has prior knowledge about the types of remote PEs for some or all of its P2P Ethernet services, reducing the number of routes a composite PE originates can be achieved through the configuration. Based on the configuration, a composite may advertise EVPN route but not L2VPN A-D route for a P2P Ethernet service, or vice versa. It is up to the Service Provider to decide based on the network requirement.

11. IANA Considerations

This document has no actions for IANA.

12. Security Considerations

The same Security Considerations described in [RFC8214] are valid for this document.

13. Contributors

In addition to the authors listed on the front page, the following coauthors have also contributed to this document:

Ali Sajassi
Cisco Systems
Email: sajassi@cisco.com

Luc Andre Burdet
Cisco Systems
Email: lburdet@cisco.com

Daniel Voyer
Bell Canada
Email: daniel.voyer@bell.ca

Iman Ghamari
Linkedin
Email: iman@linkedin.com

Edward Leyton
Verizon Wireless
Email: edward.leyton@verizonwireless.com

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6074] Rosen, E., Davie, B., Radoaca, V., and W. Luo, "Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)", RFC 6074, DOI 10.17487/RFC6074, January 2011, <https://www.rfc-editor.org/info/rfc6074>.

[RFC8077] Martini, L., Ed. and G. Heron, Ed., "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", STD 84, RFC 8077, DOI 10.17487/RFC8077, February 2017, <https://www.rfc-editor.org/info/rfc8077>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8214] Boutros, S., Sajassi, A., Salam, S., Drake, J., and J. Rabadan, "Virtual Private Wire Service Support in Ethernet VPN", RFC 8214, DOI 10.17487/RFC8214, August 2017, <https://www.rfc-editor.org/info/rfc8214>.

14.2. Informative References

[I-D.ietf-bess-evpn-mh-pa] Brissette, P., Burdet, L. A., Wen, B., Leyton, E., and J. Rabadan, "EVPN Port-Active Redundancy Mode", Work in Progress, Internet-Draft, draft-ietf-bess-evpn-mh-pa-13, 5 December 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-bess-evpn-mh-pa-13>.

[RFC4664] Andersson, L., Ed. and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, DOI 10.17487/RFC4664, September 2006, <https://www.rfc-editor.org/info/rfc4664>.

[RFC4684] Marques, P., Bonica, R., Fang, L., Martini, L., Raszuk, R., Patel, K., and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)", RFC 4684, DOI 10.17487/RFC4684, November 2006, <https://www.rfc-editor.org/info/rfc4684>.

[RFC4762] Lasserre, M., Ed. and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", RFC 4762, DOI 10.17487/RFC4762, January 2007, <https://www.rfc-editor.org/info/rfc4762>.

[RFC6624] Kompella, K., Kothari, B., and R. Cherukuri, "Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling", RFC 6624, DOI 10.17487/RFC6624, May 2012, <https://www.rfc-editor.org/info/rfc6624>.

[RFC9012] Patel, K., Van de Velde, G., Sangli, S., and J. Scudder, "The BGP Tunnel Encapsulation Attribute", RFC 9012, DOI 10.17487/RFC9012, April 2021, <https://www.rfc-editor.org/info/rfc9012>.

[RFC9744] Sajassi, A., Ed., Brissette, P., Uttaro, J., Drake, J., Boutros, S., and J. Rabadan, "EVPN Virtual Private Wire Service (VPWS) Flexible Cross-Connect (FXC) Service", RFC 9744, DOI 10.17487/RFC9744, March 2025, <https://www.rfc-editor.org/info/rfc9744>.

Authors' Addresses

Patrice Brissette (editor)
Cisco Systems
Email: pbrisset@cisco.com

Wen Lin
Juniper
Email: wlin@juniper.com

J. Rabadan
Nokia
Email: jorge.rabadan@nokia.com

James Uttaro
ATT
Email: uttaro@att.com

Bin Wen
Comcast
Email: bin_wen@comcast.com