EVPN-VPWS Seamless Integration with Legacy VPWS
draft-brissette-bess-evpn-vpws-seamless-01

Abstract

This document specifies mechanisms for backward compatibility of Ethernet VPN Virtual Private Wire Service (EVPN-VPWS) solutions with legacy Virtual Private Wire Service (VPWS). It provides mechanisms for seamless integration in the same MPLS/IP network on a per-pseudowire or per flexible-crossconnect service basis. Implementation of this document enables service providers to introduce EVPN-VPWS PEs in their brown-field deployments of legacy VPWS networks. This document specifies control-plane and forwarding behaviour needed for auto-discovery of a pseudowire in order to enable seamless integration between EVPN-VPWS and VPWS PEs.

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 May 21, 2020.
1. Introduction

Virtual Private Wire Service (VPWS) is a widely-deployed Layer-2 VPN (L2VPN) technology. Many service providers, who are looking at adopting Ethernet VPN Virtual Private Wire Service (EVPN-VPWS), want to preserve their investment in the VPWS networks. Hence, they require mechanisms by which EVPN-VPWS can be introduced into their brown-field legacy VPWS networks without requiring any upgrades (software or hardware) to these networks. This document specifies control-plane and forwarding behaviour needed for auto-discovery of a
pseudowire in order to enable seamless integration between EVPN-VPWS Provider Edge (PE) devices and PEs running legacy VPWS services in the same MPLS/IP network.

Seamless Integration of EVPN-VPWS.

Figure 1

Figure 1 shows a simple network where PE1 runs in hybrid mode (EVPN-VPWS and legacy VPWS). It provides a pseudowire (PW1) with PE2 running legacy VPWS. It also provides a pseudowire (PW2) with PE3 running EVPN-VPWS. PE2 may be upgraded to EVPN-VPWS seamlessly.

Legacy PEs may be setting up PWs per [RFC8077] or may be setting up a VPWS service by first auto-discovering VPN members using [RFC6074] and then setting up the PWs using [RFC8077] or [RFC6624].

The seamless integration solution described in this document has the following attributes:

- It is backward compatible with [RFC8214] and EVPN Flexible crossconnect Service [evpn_fxc] document.

- New PEs can leverage the multi-homing mechanisms and provisioning simplifications of EVPN Ethernet-Segment:
  a. Auto-sensing of MHN / MHD
  b. Auto-discovery of redundancy group
  c. Auto-election of Designated Forwarder and VLAN carving
  d. Support of various load-balancing mode such as port-active, single-active and all-active

One of the objective of this document is to describe how a legacy VPWS brown-field network can be migrated seamless to EVPN-VPWS.
Usually, it is achieved in few steps. For example, let say PE1 and PE2 from Figure 1 have a legacy PW established between them. First, network operator may upgrade PE1 to support EVPN-VPWS. Once upgraded, PE1 which now have the EVPN-VPWS capability still runs legacy VPWS PW with PE2. Later on, network operator may decide to upgrade PE2 to support EVPN-VPWS. As soon as the upgrade is completed, EVPN-VPWS service takes high-precedence over legacy VPWS network. The network operator can safely remove any legacy configuration related to that PW from PE1 and PE2 nodes. PW remains established as an EVPN-VPWS service.

1.1. 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 [RFC2119].

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 the set of Ethernet links that connects a customer site (device or network) to one or more PEs.
- **Ethernet Tag**: An Ethernet Tag identifies a particular pseudowire, e.g. a PW-ID as per [RFC8214].
- **FEC**: Forwarding Equivalence Class.
- **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.
o VPWS: Virtual Private Wire Service. It refers to legacy VPWS circuit where pseudowires are signalled using LDP or BGP-AD protocol. The latter is referred as VPWS A-D.

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

o EVPN-FXC: Ethernet-VPN Flexible Cross-connect Service [evpn_fxc].

o 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.

o 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.

o 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.

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

o PW: Pseudowire

3. Solution Requirements

Following are the key requirements for backward compatibility between EVPN-VPWS and VPWS:

o 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.

o The solution MUST NOT require any changes to existing Legacy VPWS or PEs, unless it is to upgrade them to EVPN-VPWS.

o The solution MUST allow for the co-existence of PE devices running EVPN-VPWS and VPWS for the same single-homed and/or multi-homed segments.
o The solution MUST support port-active redundancy of multi-homed networks and multi-homed devices for EVPN-VPWS PEs.

o The solution MUST support single-active redundancy of multi-homed networks and multi-homed devices for EVPN-VPWS PEs.

o The solution SHOULD support all-active redundancy of multi-homed Ethernet Segments for EVPN-VPWS PEs.

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

4. Seamless Integration

In order to support seamless integration with Legacy PEs, this document may require Legacy PEs to setup PWs per [RFC8077] or may require Legacy PEs to setup VPWS service by auto-discovering VPN members using [RFC6074] and then setting up the PWs using [RFC8077] or [RFC6624]. Furthermore, EVPN-VPWS PEs must support BGP EVPN routes per [RFC8214] and one of method of legacy VPWS technologies. All the logic for seamless integration SHALL reside on the EVPN-VPWS PEs.

5. 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.

In the case of VPWS PEs running VPWS A-D, they may advertise the BGP VPWS A-D route, per the procedures specified in [RFC4664] and [RFC6074]. The operator may decide to use the same BGP Route Target (RT) to identify a pseudowire on both EVPN-VPWS and VPWS networks. In this case, when a VPWS 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 VPWS network and another for EVPN-VPWS network and employ RT-constrained [RFC4684] in order to prevent BGP EVPN routes from reaching the VPWS 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 the purpose of discovery. This ensures that, at the end of the route exchange, all EVPN-VPWS capable PEs discover other EVPN-VPWS capable PEs. Furthermore, all the VPWS-only PEs discover the EVPN-VPWS PEs as if they are standard VPWS PEs. In other words, when the discovery phase is completed, the EVPN-VPWS PEs
have discovered the remote PE per pseudowire along with their associated capability (EVPN-VPWS or VPWS-only), whereas the VPWS PE have discovered the remote PE per pseudowire as if it is VPWS-only PEs.

6. Forwarding and Control Plane Operations

Figure 2 demonstrates a typical brown-field deployment where PE2 is a legacy PE and PE1 is an EVPN-VPWS PE.

```
+---------------+    |               |   +---+
|PE1|----|----- PW1 -----|---|PE2|
+---------------+    |               |   +---+
```

Figure 2

The forwarding state setup procedures on the VPWS PE are per [RFC8077], [RFC4761] and [RFC4762].

The EVPN-VPWS PE procedures are as follow:

- The EVPN-VPWS 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 EVPN-VPWS PE receives a VPWS A-D route or a LDP-LM message from a given PE, it sets up a Legacy 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 EVPN-VPWS PE may bring the Legacy PW operationally down and MUST forward traffic using the label information from the EVPN Ethernet-AD per EVI route.
o If an EVPN-VPWS 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 EVPN-VPWS PE will setup the EVPN-VPWS PW. It may keep the Legacy VPWS PW operationally down and MUST forward traffic using the label information from that EVPN Ethernet-AD per EVI route.

o For VPWS PE not using VPWS A-D or LDP signalling, the EVPN-VPWS PEs need to be provisioned manually with PWs to those remote VPWS PEs for each pseudowire. In that case, if an EVPN-VPWS 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 label information from that EVPN Ethernet-AD per EVI route.

6.1. Multi-homed Operations

Figure 3 below demonstrates multi-homing scenarios. CE1 is connected to PE1 and PE2 where PE1 is the designated forwarder while PE2 is the non designated forwarder.

```
+---------+
|DF   +---+    |         |   +---+   +---+
+--|PE1|----|---------|---|PE3|---|CE2|
|CE1|             |       / |
|CE1|             / |
|CE1|             / |
+---+
```

EVPN-VPWS Port-Active Redundancy

Figure 3

6.1.1. Operations with Port-Active MH PEs

In Figure 3, 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 EVPN port-active document [evpn_pa]. In this example PE1 is DF elected for the shared Ethernet Segment identifier.
o Only PE1, as DF, advertises the VPWS A-D route or LDP-LM message towards remote PE3.

o 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 so during an upgrade from Legacy VPWS to EVPN-VPWS, those remote nodes are immediately upgraded.

o 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]

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

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.

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

6.1.2. Operation with Single-Active MH PEs

Single-active operation is similar to Port-active load-balancing mode described above but at the VLAN level instead being of at the port/interface level.

The main difference resides on the support of Legacy PW VC-type 4 vs PW VC-Type 5 mode on the EVPN-VPWS PE as per [RFC4448]. While services running in port-active load-balancing mode require raw mode, services running single-active load-balancing mode use tagged mode.

6.1.3. 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 PEs running Legacy VPWS do NOT support all-active peering PEs as remote endpoint.
6.1.3.1. Falling back to port-active

EVPN-VPWS PE discovering remote PE running VPWS PW MAY fallback into port-active load-balancing mode. In that case, following rules are applied:

- Peering PEs advertise EVPN Ethernet-AD per ES route with the single-active bit set. They also advertise EVPN Ethernet-AD per EVI route towards PE3 with P/B bit set accordingly as per [RFC8214].
- 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.

6.1.3.2. Asymmetric forwarding

One privilege option is the asymmetric forwarding while peering PEs run in all-active load-balancing mode. In the example of Figure 3, 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 should get forwarded to PE3 using that same VPN label. Traffic coming from CE3 to PE3 gets forwarded only over the primary PW towards PE1; the DF PE.

Supporting asymmetric forwarding with purely LDP as per [RFC8077] requires extensions to EVPN-VPWS MH procedures. These procedures are NOT restricted only to LDP and may be applied to VPWS A-D.

Following rules are applied to achieve expected behaviour:

- Peering PEs advertise EVPN Ethernet-AD per ES route with the single-active bit unset. That is to get the network ready when remote legacy PE are upgraded to EVPN-VPWS.
- 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.
The tunnel encapsulation attribute [tun_encap] 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 the same VPN label per Legacy PW as DF PE when transmitting traffic coming from CE (CE1) towards remote PE(PE3).

7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

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

9. Acknowledgements

The authors would like to acknowledge Sylvain Masse for his feedback and contribution to this document.

10. References

10.1. Normative References


10.2. Informative References


Authors’ Addresses

Patrice Brissette (editor)
Cisco Systems
Ottawa, ON
Canada

Email: pbrisset@cisco.com

Ali Sajassi
Cisco Systems
USA

Email: sajassi@cisco.com

Luc Andre Burdet
Cisco Systems
Ottawa, ON
Canada

Email: lburdet@cisco.com

James Uttaro
ATT
USA

Email: uttar@att.com

Daniel Voyer
Bell Canada
Montreal, QC
Canada

Email: daniel.voyer@bell.ca

Iman Ghamari
Telus
Canada

Email: Iman.Ghamari@telus.com