EVPN VPWS layer 2 Attributes Extended community for Control-Word behavior
draft-gs-bess-evpn-l2-attribute-cw-00

Abstract

This document aims to define a negotiation mechanism for L2 capabilities in an EVPN scenario specific to EVPN-VPWS control word behavior.

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."

Copyright Notice

Copyright (c) 2018 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 (https://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.
1. Introduction

EVPN [RFC7432] is ambiguous about the VPWS session if the control-word (C-flag) in L2 attributes between PE devices are different.

The objective of this document is to explain the mechanism to negotiate C-flag between PE devices which helps establish EVPN-VPWS session where PE C-flags don’t align initially.

2. Specification of Requirements

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].

3. Terminology

EVPN: BGP MPLS-Based Ethernet VPN defined in [RFC7432]

EVPN ELAN: In order to distinguish EVPN VPWS, EVPN ELAN specifies

EVPN defined in [RFC7432]

CW: Control Word defined in [RFC4448]

PE: Provider Edge
4. EVPN Layer 2 Attributes Extended Community

EVPN Layer 2 Attributes Extended Community is defined in EVPN VPWS [RFC8214]. A mechanism to achieve interoperability between devices with different CW capabilities is defined in this document. EVPN Layer 2 Attributes Extended Community is advertised along with Ethernet Auto-discovery (E-AD). The definition of EVPN Layer 2 Attributes Extended Community is same with [RFC8214]. It is listed as below for convenience.

+-------------------------------------------+                        +-------------------------------------------+
|  Type (0x06) / Sub-type (0x04) (2 octets) |                        | Control Flags (2 octets)                  |
+-------------------------------------------+                        +-------------------------------------------+
|  L2 MTU (2 octets)                        |                        | Reserved (2 octets)                       |
+-------------------------------------------+                        +-------------------------------------------+

Figure 1: EVPN Layer 2 Attributes Extended Community

The definition of Control Flags is as below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-----------------------------++-----------------------------+    (MBZ = MUST Be Zero)
| MBZ | C | P | B |                |
```

Figure 2: Control Flags

The P bit and B bit operations are defined in [RFC8214].

C bit represents the control word capability of the PE. It indicates if set to C=0 that, PE is not capable of processing control-word(CW) in the data traffic. C bit SHOULD be same among PEs belonging to same Ethernet Segment (ESI).
Other bits in Control Flags are reserved for future investigation and MUST be zero.

If local PE does not support EVPN Layer 2 Attributes Extended Community, this community MUST be ignored.

5. Usage of Control Flags

The description below is based on the network topology showed in Figure 3:

```
+--------+       +--------+
|   PE1  |       |   PE2  |
|  (CW)  |-------|  (NCW) |
+--------+       +--------+
```

Figure 3: Network Topology for Control Word Interoperability

PE1 is control-word capable where as PE2 is not capable of control-word. PE2 capability for CW is either Disabled or Not supported.

With the setup mentioned in Figure 3, the current EVPN-VPWS RFC[RFC8214] does not explicitly mention the state of the VPWS session between two PEs. It also states PE2 MUST put control-word for any data to be sent to PE1 over that link. But here the problem is PE2 may not be capable of prepending control-word to traffic. Hence PE1 will receive the packets without control-word even when its expecting with CW.

This document proposes a solution for the above problem. It clearly defines the behavior for a PE in this scenario.

The solution require but does not mandate an administrative command enforce-cw. The behavior of this is explained in following statements.

```
enforce-cw enabled:

1) When PE1 receives E-AD(C-bit=0) from PE2, PE1 MUST NOT fall back to C-bit=0, but the VPWS session state will be brought DOWN.
2) When PE2 receives E-AD(C-bit=1) from PE1, PE2 will establish session in DOWN state.
```

```
enforce-cw disabled:

1) When PE1 receives E-AD(C-bit=0) from PE2, PE1 MUST fall back to C-bit=0, and initiate new E-AD message towards PE2 with C-bit=0.
   And mark VPWS session UP.
2) When PE2 receives E-AD(C-bit=1) from PE1, PE2 will establish session in DOWN state.
```

This document does not suppress any E-AD messages in any scenario. Every PE MUST be sending their E-AD message at-least once per VPWS-session.
C-bit Handling Procedures Diagram where enforce-cw is disabled.

---

<table>
<thead>
<tr>
<th>Y</th>
<th>Received E-AD message</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C=0</td>
<td>C=1</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Control Word</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capable?</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Control Word</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled?</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Control Word</th>
<th>N</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Send C=0   Send C=1   Send C=0   Send C=0   Send C=0   Send C=1

---

If receive the same as sent, VPWS setup is complete. If not:

---

Receive C=1   Receive C=0

---

Make session DOWN   Wait for the next message   Send C=0

GS Expires June 24, 2019 [Page 5]
C-bit Handling Procedures Diagram where enforce-cw is enabled.

Y | Received       |       N
-------| E-AD message   |-------------------

C=0 |                      | C=1 |
-------                      -------

Y |                            |        ----------------
|                                |        | Control Word |  N
|                            |        |  enabled?    |---
|                   |        |                Y
|                   |        |

Control Word |  N          | Control Word |  N
enabled?     |-------      | enabled?     |----

Y |                            |        |
| Send | Send | Send | Send | Send | Send
C=1 | C=0 | C=1 | C=0 | C=1 | C=0

Make VPWS | Make VPWS | Make VPWS | Make VPWS | Make VPWS |
Session DOWN | Session UP | Session UP | Session DOWN |
6. Security Considerations

There are no new security considerations due to the text of this document.

7. IANA Considerations

This document does not make any requests from IANA.

8. Normative References


