E-VPN Ping Mechanism for Virtual eXtensible Local Area Network (VXLAN)
draft-vji-evpn-ping-vxlan-02.txt

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on December 30, 2018.

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 (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
Internet-Draft       E-VPN Ping Mechanism for VXLAN           June 2018

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.

Abstract

Ping is a widely deployed Operation, Administration, and Maintenance
(OAM) mechanism in networks. This document describes a mechanism
for detecting data-plane failures using Ping in RFC7348 VXLAN based
EVPN networks.

Table of Contents

1. Introduction...................................................2
2. Conventions used in this document..............................3
3. Acronyms and Definitions....................................3
4. IP ping and trace route extension for VXLAN....................4
5. VXLAN OAM header format.......................................4
   5.1. VXLAN EVPN OAM Header:....................................5
   5.2. EVPN MAC/IP TLV...........................................7
   5.3. EVPN Inclusive Multicast TLV............................8
   5.4. EVPN Auto-Discovery TLV................................9
   5.5. EVPN IP Prefix TLV....................................10
6. E-VPN Context Validation procedure............................10
7. Security Considerations......................................11
8. IANA Considerations..........................................11
9. References....................................................11
   9.1. Normative References....................................11
   9.2. Informative References.................................13
10. Acknowledgments.............................................13

1. Introduction

RFC7348 Virtual eXtensible Local Area Network (VXLAN): A Framework
for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks
defines means to support data center layer 2 E-VPN over an IP core
network.

draft-jain-bess-evpn-lsp-ping defines procedures to detect data-
plane failures using LSP Ping in MPLS networks deploying EVPN and
PBB-EVPN, which is an extension of RFC6426.

This document outlines how OAM data fields are encapsulated and how
connectivity check and fault isolation is performed from edge to
edge for VXLAN networks using RFC792 ICMP based ping and traceroute solution.

2. Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119.

In this document, the characters ">>" preceding an indented line(s) indicates a statement using the key words listed above. This convention aids reviewers in quickly identifying or finding the portions of this RFC covered by these keywords.

3. Acronyms and Definitions

AD             Auto Discovery
CE             Customer Edge Device
ECMP           Equal-Cost Multipath
ESI            Ethernet Segment Identifier
EVPN           Ethernet Virtual Private Network
OAM            Operations, Administration and Maintenance
PE             Provider Edge Device
VLAN           Virtual Local Area Network
VNI            VXLAN Network Identifier (or VXLAN Segment ID)
VTEP           VXLAN Tunnel End Point. An entity that originates and/or terminates VXLAN tunnels
VXLAN          Virtual eXtensible Local Area Network
VXLAN Segment  VXLAN Layer 2 overlay network over which VMs communicate

VXLAN Gateway  an entity that forwards traffic between VXLANs

4. IP ping and trace route extension for VXLAN

In IP network ICMP, UDP or HTTP based ping and traceroute provide ways to perform reachability check and fault isolation, this can be used for OAM purpose for the IP underlay network. E-VPN extension for the existing ping and traceroute operations make it control-plane aware and add additional capability to validate the E-VPN forwarding context, detect data-plane errors and measure PE to PE performance.

5. VXLAN OAM header format

IPv4 underlay OAM information is encoded in the VXLAN header as below.

VXLAN Header

0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R|R|R|O|I|R|R|R|            Reserved                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                VXLAN Network Identifier (VNI) |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

RFC7348 VXLAN header OAM extension

New O bit is selected for OAM purpose, value 1 for OAM packets, 0 for regular VXLAN traffic. This bit is temporarily declared as bit3, subject to be changed.
5.1. VXLAN EVPN OAM Header:

```
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Option Class = OAM_ECHO | Type   |R|R|R| Length |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Return Code       | Return Subcode   | Must Be Zero      |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Sender’s Handle   |                   |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Sequence Number   |                   |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Time Stamp Sent (seconds) |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Time Stamp Sent (seconds fraction) |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Time Stamp Received (seconds) |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| Time Stamp Received (seconds fraction) |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
|                   |                   |
.                   |
|                   | TLVs              |
.                   |
|                   |                   |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
```

VXLAN EVPN OAM header

Type: 0 for echo request; 1 for echo reply.

Return Code and Return sub-code must be zero for the ping or traceroute request. For ping or traceroute reply, the value is defined as:

<table>
<thead>
<tr>
<th>Return Code #</th>
<th>Value Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
</tr>
<tr>
<td>1</td>
<td>Context Not Found</td>
</tr>
<tr>
<td>2</td>
<td>Context Found but IP address Mis-Match</td>
</tr>
</tbody>
</table>

Return sub-code is reserved for future use.

The Sender’s Handle is filled in by the sender and returned unchanged by the receiver in the echo reply (if any). There are no
semantics associated with this handle, although a sender may find this useful for matching up requests with replies.

The Sequence Number is assigned by the sender of the echo request and can be (for example) used to detect missed replies.

The TimeStamp Sent is the time of day (according to the sender’s clock) in 64-bit NTP timestamp format [RFC5905] when the echo request is sent. The TimeStamp Received in an echo reply is the time of day (according to the receiver’s clock) in 64-bit NTP timestamp format in which the corresponding echo request was received. TimeStamp Received must be zero for the request. Value 0 means the time is not measured or available, shall be ignored.

TLVs (Type-Length-Value tuples) have the following format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Value                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TLV format
TLV type values use the same value of corresponding BGP route type when advertised the route, defined in [RFC7432], [draft-ietf-bess-evpn-prefix-advertisement] and [draft-ietf-bess-evpn-igmp-mld-proxy].

<table>
<thead>
<tr>
<th>Type #</th>
<th>Value Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet Auto-Discovery (A-D) TLV</td>
</tr>
<tr>
<td>2</td>
<td>MAC/IP TLV</td>
</tr>
<tr>
<td>3</td>
<td>Inclusive Multicast TLV</td>
</tr>
<tr>
<td>4</td>
<td>Ethernet Segment TLV (format to be defined)</td>
</tr>
<tr>
<td>5</td>
<td>IP Prefix TLV</td>
</tr>
<tr>
<td>6</td>
<td>Selective Multicast Ethernet Tag TLV (format to be defined)</td>
</tr>
</tbody>
</table>

5.2. EVPN MAC/IP TLV

The EVPN MAC/IP TLV is used to identify the MAC for an EVI under test at a peer PE.

The EVPN MAC TLV fields are derived from the MAC/IP advertisement route defined in [RFC7432] Section 7.2 and has the format as shown in Figure 4. This TLV is included in the Echo Request sent to the Peer PE by the PE that is the originator of the request.
The ping echo request is sent using the EVPN VNI(s) associated with the MAC route announced by a remote PE to reach the remote PE.

5.3. EVPN Inclusive Multicast TLV

The EVPN Inclusive Multicast sub-TLV fields are based on the EVPN Inclusive Multicast route defined in [RFC7432] Section 7.3. The EVPN Inclusive Multicast TLV has the format as shown in Figure 5. This TLV is included in the echo request sent to the EVPN peer PE by the originator of request to verify the multicast connectivity state on the peer PE(s) in EVPN and PBB-EVPN.
5.4. EVPN Auto-Discovery TLV

The EVPN Auto-Discovery (AD) TLV fields are based on the Ethernet AD route advertisement defined in [RFC7432] Section 7.1. EVPN AD TLV applies to only EVPN. The EVPN AD sub-TLV has the format shown in Figure 1.

Broadcast, multicast and unknown unicast traffic can be sent using ingress replication or P2MP P-tree in EVPN network.
5.5. EVPN IP Prefix TLV

The EVPN IP Prefix TLV is used to identify the IP Prefix for an EVI under test at a peer PE. The EVPN IP Prefix sub-TLV fields are derived from the IP Prefix Route (RT-5) advertisement defined in [I-D.ietf-bess-evpn-prefix-advertisement] and has the format as shown in Figure 7. This TLV is included in the Echo Request sent to the Peer PE by the PE that is the originator of the request.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Route Distinguisher                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      (8 octets)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Ethernet Tag ID                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Ethernet Segment Identifier           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       | must be zero | IP Prefix Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     IP Prefix (4 or 16 Octets)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     GW IP Address (4 or 16 Octets)     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     L3VNI (3 Octets)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Reserved                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

EVPN IP Prefix TLV format

6. E-VPN Context Validation procedure

The TLVs in the EVPN OAM header is collect from the control-plane of the ping or traceroute initiator PE, and to be validated by control-plane of the peer PE, mid-node transmit routers may ignore it. For traceroute, when the packet is punted to OAM for each TTL expiry event, transmitter router may update the TimeStamp field in the header to provide performance measurement.

This procedure do not have preference of protocol selection of ping or trace route. Typically, ICMP echo request and ICMP echo reply is used for ping; while ICMP echo request, UDP, HTTP or other protocols may be used for traceroute. There is no change to these upper level protocols.
7. Security Considerations

The proposal introduced in this document does not introduce any new security considerations beyond that already apply to [RFC7432], [RFC7348], [RFC7623] and [RFC6425] and draft-jain-bess-evpn-lsp-ping.

8. IANA Considerations

8.1. Sub-TLV Type

This document defines 6 new TLV types, which is intend to use the same value as RT types defined in [RFC7432], [draft-ietf-bess-evpn-prefix-advertisement] and [draft-ietf-bess-evpn-igmp-mld-proxy].

IANA is requested to assign a sub-TLV type value to the following

8.2. Proposed new Return Codes

[RFC8029] defines values for the Return Code field of Echo Reply. This document proposes two new Return Codes, which SHOULD be included in the Echo Reply message by a PE in response to LSP Ping Echo Request message:

1. The FEC exists on the PE and the behavior is to drop the packet because of not DF.

2. The FEC exists on the PE and the behavior is to drop the packet because of Split Horizon Filtering.

9. References

9.1. Normative References


9.2. Informative References


10. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors’ Addresses

Victor Ji
Cisco Systems, Inc.
Email: vji@cisco.com

Jaganbabu Rajamanickam
Cisco Systems, Inc.
Email: jrajaman@cisco.com

Hicham Ouahid
Cisco Systems, Inc.
Email: houahid@cisco.com

Chuanfa Wang
Cisco Systems, Inc.
Email: chuanwan@cisco.com

Xianlei Du
Cisco Systems, Inc.
Email: xiandu@cisco.com