Abstract

Bit Index Explicit Replication (BIER) can be used as provider tunnel for Multicast Virtual Private Network (MVPN) [RFC6514], Global Table Multicast [RFC7716] or Ethernet Virtual Private Network (EVPN) [RFC7432]. It is possible that not all routers in the provider network support BIER and there are various methods to handle BIER incapable transit routers. However those methods assume the MVPN/EVPN Provider Edges (PEs) are BIER capable. This document specifies a method to allow BIER incapable routers to act as MVPN/EVPN PEs with BIER as the transport, by having the upstream BIER Forwarding Router (BFR) that is connected directly or indirectly via a tunnel to a BIER incapable PE remove the BIER header and send the payload to the PE.

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.

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 April 5, 2020.
1. Introduction

The BIER architecture includes three layers: the "routing underlay", the "BIER layer", and the "multicast flow overlay". The multicast flow overlay is responsible for the BIER Forwarding Egress Routers (BFERs) to signal to BIER Forwarding Ingress Routers (BFIRs) that they are interested in receiving certain multicast flows so that BFIRs can encode the correct bitstring for BIER forwarding by the BIER layer.

MVPN and EVPN are two similar overlays where BGP Auto-Discovery routes for MVPN/EVPN are exchanged among all PEs to signal which PEs need to receive multicast traffic for all or certain flows. Typically the same provider tunnel type is used for traffic to reach all receiving PEs.

Consider an MVPN/EVPN deployment where enough provider routers are BIER capable for BIER to become the preferred choice of provider tunnel. However, some PEs cannot be upgraded to support BIER forwarding. While there are ways to allow an ingress PE to send traffic to some PEs with one type of tunnel and send traffic to some
other PEs with a different type of tunnel, the procedure becomes complicated and forwarding is not optimized.

One way to solve this problem is to use Penultimate Hop Popping (PHP) so that the upstream BFR can pop the BIER header and send the payload "natively" (note that the upstream BFR can be connected directly or indirectly via any type of tunnel to the PE). This is similar to Multi-Protocol Label Switching (MPLS) PHP though it is the BIER header that is popped.

The transition of an existing MVPN/EVPN deployment with traditional provider tunnels to using BIER with some PEs not capable of receiving BIER packets can be incremental. All PEs are first upgraded to support BIER at least in the control plane, with those not capable of BIER forwarding requesting PHP. Then BIER capable ingress PEs independently and incrementally switch to BIER transport.

While the above text uses MVPN/EVPN as example, BIER PHP is applicable to any scenario where the multicast flow overlay edge router does not support BIER, as long as the edge router does not need to know the transmitting BFR.

This works well if a BIER incapable PE only needs to receive multicast traffic. If it needs to send multicast traffic as well, then it must Ingress Replicate to a BIER capable helper PE, who will in turn relay the packet to other PEs. The helper PE is either a Virtual Hub as specified in [RFC7024] for MVPN and [I-D.keyupate-bess-evpn-virtual-hub] for EVPN, or an AR-Replicator as specified in [I-D.ietf-bess-evpn-optimized-ir] for EVPN.

2. Specifications

The procedures in this section apply only if, by means outside the scope of this document, it is known that the payload after BIER header is one of the following:

- MPLS packets with downstream-assigned label at top of stack (i.e., the Proto field in the BIER header is 1). For example, a label from a Domain-wide Common Block (DCB) is used as specified in [I-D.ietf-bess-mvpn-evpn-aggregation-label].

- Packets with VXLAN/NVGRE/GENEVE header [I-D.ietf-bier-evpn] (i.e. the Proto field in the BIER header specifies VXLAN/NVGRE/GENEVE per IANA assignments to be done for [I-D.ietf-bier-evpn]).

A BIER incapable router, if acting as a multicast flow overlay router, MUST signal its BIER information as specified in [RFC8401] or [RFC8444] or [I-D.ietf-bier-idr-extensions], with a PHP sub-sub-TLV
included in the BIER sub-TLV attached to the BIER incapable router’s BIER prefix to request BIER PHP from other BFRs. The sub-sub-TLV’s type is TBD, and the length is 0.

With MPLS encapsulation, the BIER incapable multicast flow overlay router MAY omit the BIER MPLS Encapsulation sub-sub-TLV, or MUST set the Label field in BIER MPLS Encapsulation sub-sub-TLV to Implicit Null Label [RFC3032].

With MPLS encapsulation, if a BFER does not support certain BSL, it MAY still advertise a corresponding BIER MPLS Encapsulation sub-TLV but set the Label field to Implicit Null Label.

If a BFR follows section 6.9 of [RFC8279] to handle BIER incapable routers, it must treat a router as BIER incapable if the label advertised by the router is Implicit Null, or if the router advertises a PHP sub-sub-TLV, so that the router is not used as a transit BFR.

If the downstream neighbor for a BIER prefix is the one advertising the prefix with a PHP sub-sub-TLV or with an Implicit Null Label in the Label field in its BIER MPLS Encapsulation sub-sub-TLV, then when the corresponding BIRT or BIFT entry is created/updated, the forwarding behavior MUST be that the BIER header is removed and the payload be sent to the downstream router without the BIER header, either directly or over any type of tunnel.

3. Security Considerations

This specification does not introduce additional security concerns beyond those already discussed in BIER architecture and OSPF/ISIS/BGP extensions for BIER signaling.

4. IANA Considerations

This document requests a new sub-sub-TLV type value from the "Sub-sub-TLVs for BIER Info Sub-TLV" registry in the "IS-IS TLV Codepoints" registry:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>BIER PHP Request</td>
</tr>
</tbody>
</table>

This document also requests a new sub-TLV type value from the OSPFv2 Extended Prefix TLV Sub-TLV registry:
5. Acknowledgements

The author wants to thank Eric Rosen and Antonie Przygienda for their review, comments and suggestions. The author also wants to thank Senthil Dhanaraj for his suggestion of requesting PHP if a BFER does not support certain BSL.

6. References

6.1. Normative References

[I-D.ietf-bess-mvpn-evpn-aggregation-label]

[I-D.ietf-bier-evpn]

[I-D.ietf-bier-idr-extensions]


6.2. Informative References

[I-D.ietf-bess-evpn-optimized-ir]

[I-D.keyupate-bess-evpn-virtual-hub]


Author’s Address

Zhaohui Zhang
Juniper Networks

EMail: zzhang@juniper.net