Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 18, 2020

M. McBride
Futurewei
J. Xie
S. Dhanaraj
Huawei
R. Asati
Cisco
Y. Zhu
China Telecom

January 15, 2020

BIER IPv6 Requirements
draft-ietf-bier-ipv6-requirements-04

Abstract

The BIER WG includes, in its charter, work on developing mechanisms to transport BIER natively in IPv6. This document is intended to help the WG with this effort by specifying requirements for transporting packets, with Bit Index Explicit Replication (BIER) headers, in an IPv6 environment. There will be a need to send IPv6 payloads, to multiple IPv6 destinations, using BIER. There have been several proposed solutions in this area. But there hasn't been a document which describes the problem and lists the requirements. The goal of this document is to describe the BIER IPv6 requirements, summarize the proposed solutions, and guide the working group in understanding the benefits, and drawbacks, of the various solutions and to help in the development of acceptable solutions.

Status of This Memo

Table of Contents

1. Introduction

Bit Index Explicit Replication (BIER) [RFC8279] is an architecture that provides optimal multicast forwarding, without requiring intermediate routers to maintain per-flow state, through the use of a multicast-specific BIER header. [RFC8296] defines two types of BIER encapsulation to run on physical links: one is BIER MPLS encapsulation to run on various physical links that support MPLS, the other is non-MPLS BIER Ethernet encapsulation to run on ethernet links, with an ethertype 0xAB37. This document describes using BIER in non-MPLS IPv6 environments. We explain the requirements of transporting IPv4/IPv6 multicast payloads, from an IPv6 router (BFIR) to multicast IPv6 destinations (BFERs), using BIER. This can include native IPv6 encapsulation and generic tunneling. Native IPv6, in this document, is defined as BIER not encapsulated in mpls or ethernet. The goal of this document is to help the BIER WG evaluate the BIER v6 requirements and solutions in order to begin adopting solution drafts.

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 RFC 2119 [RFC2119].

1.2. Terminology

- o BIER: Bit Index Explicit Replication. Provides optimal multicast forwarding through adding a BIER header and removing state in intermediate routers.

- o BUM: Broadcast, Unknown Unicast, Multicast. Term used to describe the three types of Ethernet modes that will be forwarded to multiple destinations

2. Problem Statement

The problem is the ability of the network to transport BUM packets, with BIER headers, in an IPv6 environment. In IPv6 networks, many deployments use non-MPLS encapsulation for unicast as the data-plane. In such case, it may be expected to have a BIER IPv6 encapsulation which is compliant with various kinds of physical links, perhaps in a hop-by-hop manner, and maintain the benefit of "fast reroute" of an IPv6 tunnel. Evaluating the BIER IPv6 requirements will help determine the best solutions to address these problems.

3. BIER IPv6 Scenario's

```
         +---------------------------------------------+
         |                                             |
         |                                          +-------+
         |                                          | BFER  |
     +-------+              IPv6                    +-------+
     | BFIR  |                                         |
     +-------+             Network                  +-------+
         |                                          | BFER  |
         |                                          +-------+
         |                                             |
         +---------------------------------------------+
```

This basic scenario depicts the need to replicate bier packets from a BFIR to BFERs across an IPv6 core. The IPv6 environment may include a variety of link types, may be entirely IPv6, may be dual stack or any type of combination which includes IPv6. Regardless of the environment, there are times when a BIER header, including the BIER bitstring used to determine the set of BIER forwarding egress routers, will need to traverse a IPv6 domain. The ways in which BIER will function in an IPv6 environment is the problem that needs to be solved. [RFC8354] lists some good IPv6 related use cases which we will similarly reference in this document.

3.1. BIERv6 for Access Network

Access networks deliver a variety of types of multicast video traffic from the service provider's network to the home (or Enterprise) environment and from the home towards the service provider's network.

There will be a need to send traffic from the IPv4 access towards the service provider's IPv6 network and vice versa. A packet could be mapped into a providers IPv6 network through the use of a BIERv6 header. The access devices would not need to know specific details about the packet to perform this mapping; instead the access device would only need to know how to process a BIER header unless there is end to end IPv6.

3.2. BIERv6 for Data Center

Some Data Center operators are transitioning their Data Center infrastructure from IPv4 to native IPv6 only, in order to cope with IPv4 address depletion and to achieve larger scale. In such environment, BIERv6, can be used to natively steer multicast data across an IPv6 data center.

3.3. BIERv6 for Core Networks

While the overall amount of traffic offered to the network continues to grow and considering that multiple types of traffic with different characteristics and requirements are quickly converging over single network architecture, the network operators are starting to face new challenges.

Some operators are currently building, or plan to build in the near future, an IPv6 only native infrastructure for their core network. Having a native BIERv6 infrastructure will help maintain simplicity of the network and reduce state versus traditional IP Multicast.

4. Requirements

There have been several suggested requirements, on the BIER email list and in meetings, which have been used to form BIER IPv6 requirements used to help the wg evaluate against the proposed solutions:

4.1. L2 Agnostic

The solution should be agnostic to the underlying L2 data link type.

4.2. Hop by hop SA or DA modification

The solution should not require hop-by-hop modification of the IP source address field.

Solutions that do not require Hop-by-hop SA modification are preferred. Solutions which maintain the SA will help fast-path forwarding (req 4.9 in this doc), are beneficial for receiving notices from the BFIR for functions like BIER PING, TRACE and MTU notification, are beneficial for identifying an MVPN instance to help remove more encapsulation such as Service Label, are beneficial for SA filtering (req 4.6 in this doc), and are beneficial for data origin authentication if IPSEC is desired (req 4.12 in this doc).

The solution should use a IPv6 unicast address in the DA to satisfy the BIER architecture without introducing additional tunnel encapsulation, and thus may require DA modification by each BFR hop.

It is commonly thought that BIERv6 could use a multicast address, as BIER is one-hop replication on each BFR in normal cases. However, as described in section 6.9 of [RFC8279], it is useful to support non-BIER routers within a BIER domain. From the wg discussion about this document, focus is on the advantages of using unicast addresses that otherwise could not be possible by using a multicast address or

anycast address for two cases: replication from a BFR to other BFR(s) connected by Layer-3 Non-BFR router(s) without using tunneling techniques, and replication from a BFR to other BFR(s) connected by Layer-2 switch(es) without broadcasting or snooping on Layer-2 switch(es) in between. Based on the natural reachability of an IPv6 unicast address, it can support the multi-hop replication cases as well as the one-hop replication case using one encapsulation.

4.3. L4 Inspection

The solution should not require the BFRs to inspect layer 4 or require any changes to layer 4.

The proposals requiring BIER header encapsulated as part of the payload may conflict with the layers of IP protocol stack. On the one hand, fast-path BIER forwarding has to be based on the L4 inspection of the BIER header within the payload, and on the other hand, the BIER forwarding needs to change the BitString in the BIER header of the payload, which in turn conflicts with other L3 functions. Following are some examples.

One example is in IP fragmentation case, where a packet may need to be fragmented by a BFIR, according to the BIER-MTU defined in RFC8296, into one packet with BIER header and 1500 bytes of payload, and another packet with the remaining 500 bytes of payload. When BFR B receives the second fragmentation packet from BFR A, BFR B can't forward this packet because BFR B doesn't have the BIER header in the second fragmentation packet. Section 4.11 describes the fragmentation requirements.

The second example is in IPSEC case, where the BIER header is part of the payload for confidentiality or integrity. The need to change the BitString in the BIER Header, when forwarding BIER packets, makes it incompatible with IPSEC. Section 4.12 describes the IPSEC requirements.

4.4. Multicast address in SA field

The solution should not allow a multicast address to be put in the IP source address field. According to [RFC1112] "A host group address must never be placed in the source address field or anywhere in a source route or record route option of an outgoing IP datagram."

4.5. Incorrect bits

The solution should not assume that bits never get set incorrectly.

If a packet with incorrect bits is set, it should not damage BIERv6 functionality or any other functions such as Unicast Reverse Path Forwarding (URPF), nor should it cause loops or duplicates as described in section 6.8 of [RFC8279].

4.6. SA filtering

The solution should not require changes in source address filtering procedures. For instance if a host uses a "BIER address" as its source address in a given packet, and the packet doesn't get dropped according to existing SA filtering procedures, the packet may elicit responses that put the BIER address in their destination address fields. This could be a security issue, as it creates an attack vector that can create 64 responses to a single probe.

4.7. BIER architecture support

It should be possible to use the solution to support the entire BIER architecture. The ability to bypass Non-BIER routers and L2 switches is part of the BIER architecture and having this ability is a mandatory requirement.

Multiple sub-domains bound to one or many topologies or algorithms, multiple sets for more BFERs, multiple Bit String Length for different forwarding capability, and multiple BIFTs for ECMP should be supported.

4.8. Simple Encapsulation

The solution should avoid requiring different encapsulation types, or complex tunneling techniques, to support BIER as an E2E multicast transport.

A single encapsulation should support Layer-2 switches within BFRs, or non-BFR within a BIER domain, or inter-domain deployment of BIER.

4.9. Hardware fast path

The solution should enable the processing and forwarding of BIER packets in hardware fast path.

4.10. Conform to existing IPv6 Spec

The proposed encapsulation must conform to the IPv6 specification and guidelines as described in RFC8200. It should not require any new modifications to the IPv6 specification aside from extensions to existing mechanisms such as IPv6 Options.

4.11. Support Fragmentation

The proposed encapsulation must support fragmentation. It shouldn't require fragmentation and re-assembly at each hop.

4.12. Support IPv6 Security

The proposed encapsulation should support IPv6 security including AH/ESP extension headers. It shouldn't require hop-by-hop encryption/decryption.

5. IANA Considerations

Some BIERv6 encapsulation proposals do not require any action from IANA while other proposals require new BIER Destination Option codepoints from IPv6 sub-registries, new "Next header" values, or require new IP Protocol codes. This document, however, does not require anything from IANA.

6. Security Considerations

There are no security issues introduced by this draft.

7. Acknowledgement

Thank you to Eric Rosen for his listed set of requirements on the bier wg list.

8. Normative References

[I-D.pfister-bier-over-ipv6]
Pfister, P. and I. Wijnands, "An IPv6 based BIER Encapsulation and Encoding", draft-pfister-bier-over-ipv6-01 (work in progress), October 2016.

[I-D.xie-bier-ipv6-encapsulation]
Xie, J., Geng, L., McBride, M., Asati, R., and S. Dhanaraj, "Encapsulation for BIER in Non-MPLS IPv6 Networks", draft-xie-bier-ipv6-encapsulation-04 (work in progress), December 2019.

[I-D.xu-bier-encapsulation]
Xu, X., somasundaram.s@alcatel-lucent.com, s., Jacquenet, C., Raszuk, R., and Z. Zhang, "A Transport-Independent Bit Index Explicit Replication (BIER) Encapsulation Header", draft-xu-bier-encapsulation-06 (work in progress), September 2016.

[I-D.zhang-bier-bierin6]
Zhang, Z., Przygienda, T., Wijnands, I., Bidgoli, H., and M. McBride, "BIER in IPv6 (BIERin6)", draft-zhang-bier-bierin6-04 (work in progress), January 2020.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, DOI 10.17487/RFC1112, August 1989, <https://www.rfc-editor.org/info/rfc1112>.

[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>.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, DOI 10.17487/RFC2473, December 1998, <https://www.rfc-editor.org/info/rfc2473>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8279] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast Using Bit Index Explicit Replication (BIER)", RFC 8279, DOI 10.17487/RFC8279, November 2017, <https://www.rfc-editor.org/info/rfc8279>.

[RFC8296] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Tantsura, J., Aldrin, S., and I. Meilik, "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks", RFC 8296, DOI 10.17487/RFC8296, January 2018, <https://www.rfc-editor.org/info/rfc8296>.

[RFC8354] Brzozowski, J., Leddy, J., Filsfils, C., Maglione, R., Ed., and M. Townsley, "Use Cases for IPv6 Source Packet Routing in Networking (SPRING)", RFC 8354, DOI 10.17487/RFC8354, March 2018, <https://www.rfc-editor.org/info/rfc8354>.

Appendix A. Solutions Evaluation

The following are solutions that have been proposed to solve BIER in IPv6 environments. Some solutions propose encoding while others propose encapsulation. It is recommended for the wg to evaluate these solutions against the requirements listed previously in order to make informed decisions on solution readiness.

As illustrated in these examples, the BIER header, or the BitString, may appear in the IPv6 Header, IPv6 Extension Header, IPv6 Payload, or IPv6 Tunnel Packet:

A.1. BIER-ETH encapsulation in IPv6 networks

```
+---------------+-----------------+-------------------
|   Ethernet    |   BIER header   | payload
|  (ethType =   | (BIFT-id, ...)  |
|    0xAB37)    |                 |
|               |  Next Header    |
+---------------+-----------------+-------------------
```

BIER-ETH encapsulation (BIER header for Non-MPLS networks as defined in [RFC8296]) can be used to transport the multicast data in the IPv6 network by encapsulating the multicast user data payload within the BIER-ETH header. However, using BIER-ETH in IPv6 networks is not considered to be a native IPv6 solution which utilizes the IPv6 header to forward the packet. Below listed are some of the properties of BIER-ETH encapsulation which could be seen as the reasons for the same,

- o BIER-ETH is not agnostic to the underlying (L2) data link type. It can be deployed only in the networks with Ethernet data link and cannot be deployed in an network which deploys any other data link types. Use of BIER-ETH in IPv6 networks might also result in using different BIER encapsulations, when BIER is used as a E2E multicast transport across a larger heterogeneous IPv6 networks with different data link types used in different layers of the network.

- o BIER-ETH in IPv6 networks is considered similar to 6PE solution where-in the multicast user data packet is encapsulated with-in the BIER-MPLS header.

    * It is worth noting that the only major difference between BIER-MPLS and BIER-Non-MPLS header is that BIER-MPLS uses downstream assigned MPLS label while BIER-Non-MPLS header uses a domain-wide-unique BIFT-id. While the use of domain-wide-unique BIFT-id in BIER-ETH header takes away the complexity of allocation and state maintenance from the network, it still requires some sort of ID (similar to label) to identify the application context after the decapsulation of BIER header (example: MVPN VRF Label). Encoding of such an ID/LABEL before encapsulating the multicast user data payload with BIER-ETH header cannot be avoided.

* The absence of an IPv6 header, and the optional IPv6 extension headers, deprives BIER of some of the useful cases (ex: Use of IPv6 address for identification of network function or service mapping) that is otherwise possible in native IPv6 encapsulation which utilizes a IPv6 header.

* Tunneling of BIER packets is one common technique used for FRR, to tunnel over BIER incapable nodes etc. While it is possible for the BIER-ETH encapsulated packet to be further encapsulated within a GRE6, etc tunnel, it might not be possible to parse and decapsulate different types of tunnel headers and forward the BIER packet completely in hardware fast path similar to the label stack processing in BIER-MPLS networks. It would be useful to select an encapsulation which could help in processing the tunnel and BIER header and make the forwarding decision completely in hardware fast path, which is lacking in BIER-ETH encapsulation if chosen to be deployed in pure IPv6 networks.

A.2. Encode Bitstring in IPv6 destination address

```
+---------------+-------------------
|  IPv6 header  | payload
| (BitString in |
| DA lower bits)|
|  Next Header  |
+---------------+-------------------
```

As described in [I-D.pfister-bier-over-ipv6], The information required by BIER is stored in the destination IPv6 address. The BIER BitString is encoded in the low-order bits of the IPv6 destination address of each packet. The high-order bits of the IPv6 destination address are used by intermediate routers for unicast forwarding, deciding whether a packet is a BIER packet, and if so, to identify the BIER Sub-Domain, Set Identifier and BitString length. No additional extension or encapsulation header is required. Instead of encapsulating the packet in IPv6, the payload is attached to the BIER IPv6 header and the IPv6 protocol number is set to the type of the payload. If the payload is UDP, the UDP checksum needs to change when the BitString in the IPv6 destination address changes.

A.3. Add BIER header into IPv6 Extension Header

```
+---------------+----------------+------------------
|  IPv6 header  | IPv6 Ext header | payload
|               | (BIER header in |
|               |  TLV Type = X)  |
| Next Header   |   Next Header   |
+---------------+----------------+------------------
```

According to [RFC8200] In IPv6, optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper- layer header in a packet. There is a small number of such extension headers, each one identified by a distinct Next Header value. An IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header. Extension headers (except for the Hop-by-Hop Options header) are not processed, inserted, or deleted by any node along a packet's delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header. The Hop-by-Hop Options header is not inserted or deleted, but may be examined or processed by any node along a packet's delivery path, until the packet reaches the node (or each of the set of nodes, in the case of multicast) identified in the Destination Address field of the IPv6 header. The Hop-by-Hop Options header, when present, must immediately follow the IPv6 header. Its presence is indicated by the value zero in the Next Header field of the IPv6 header.

Two of the currently-defined extension headers are the Hop-by-Hop Options header and the Destination Options header which carry a variable number of type-length-value (TLV) encoded "options".

In [I-D.xie-bier-ipv6-encapsulation] an IPv6 BIER Destination Option is carried by the IPv6 Destination Option Header (indicated by a Next Header value 60). It is initialized in a packet sent by an IPv6 BFIR router to inform the following BFR routers in an IPv6 BIER domain to replicate to destination BFER routers hop-by-hop. BIER is generally a hop-by-hop and one-to-many architecture and it is required for a BIER IPv6 encapsulation to include the BIER Header ([RFC8296]) as an IPv6 Extension Header, to pilot the hop-by-hop BIER replication.

Hop by hop Options Headers may be considered. The Hop-by-Hop Options header is used to carry optional information that may be examined and processed by every node along a packet's delivery path. The Hop-by-Hop Options header is identified by a Next Header value of 0 in the IPv6 header.

Defining New Extension Headers and Options may also be considered, if the IPv6 Destination Option Header is not good enough and new extension headers can solve the problem better.

Such proposals may include requests to IANA to allocate a "BIER Option" code from "Destination Options and Hop-by-Hop Options", and/ or a "BIER Option Header" code from "IPv6 Extension Header Types".

A.4. Transport BIER as IPv6 payload

```
+---------------+-----------------+-------------------
|  IPv6 header  | IPv6 Ext header | BIER Hdr + payload
|               |    (optional)   | as IPv6 payload
|               |                 |
| Next Header   | Next Header = X |
+---------------+-----------------+-------------------
```

There is a proposal for a transport-independent BIER encapsulation header which is applicable regardless of the underlying transport technology. As described in [I-D.xu-bier-encapsulation] and [I-D.zhang-bier-bierin6], the BIER header, and the payload following it, can be combined as an IPv6 payload, and be indicated by a new Upper-layer IPv6 Next-Header value. A unicast IPv6 destination address is used for the replication and changes when replicating a packet out to a neighbor.

Such proposals may include a request to IANA to allocate an IPv6 Next-Header code from "Assigned Internet Protocol Numbers".

A.5. Tunneling BIER in a IPv6 tunnel

```
+---------------+-----------------+------------+----------------
|  IPv6 header  | IPv6 Ext header | GRE header |
|               |    (optional)   |            | BIER Hdr +
|               |                 |            | payload as GRE
| Next Header   |   Next Header   | Proto = X  | Payload
+---------------+-----------------+------------+----------------
```

A generic IPv6 Tunnel could be used to encapsulate the bier packet within an IPv6 domain.

GRE is a mechanism by which any ethernet payload can be carried by an IP GRE tunnel due to the 16-bits 'Protocol Type' field. Both IPv4 and IPv6 can be used to carry GRE. The Ethernet type codepoint 0xAB37, defined for BIER, can be used in a GRE header to indicate the subsequent BIER header and payload in an IPv6 network.

```
+---------------+----------------+------------+----------------
|  IPv6 header  | IPv6 Ext header | UDP header |
|               |    (optional)   |            | BIER Hdr +
|               |                 |            | payload as UDP
| Next Header   |   Next Header   | DPort = X  | Payload
+---------------+----------------+------------+----------------
```

UDP-based tunneling is another mechanism which uses a specific UDP port to indicate a UDP payload format. Both IPv4 and IPv6 can support UDP. Such UDP-based tunnels can be used for BIER in a IPv6 network by defining a new UDP port to indicate the BIER header and payload.

Authors' Addresses

Mike McBride
Futurewei

Email: michael.mcbride@futurewei.com

Jingrong Xie
Huawei

Email: xiejingrong@huawei.com

Senthil Dhanaraj
Huawei

Email: senthil.dhanaraj@huawei.com

Rajiv Asati
Cisco

Email: rajiva@cisco.com

Yongqing Zhu
China Telecom

Email: zhuyq8@chinatelecom.cn