Encapsulation for BIER in Non-MPLS IPv6 Networks

draft-xie-bier-ipv6-encapsulation-00

IETF104 2019-03-25 Prague

Jingrong Xie
Liang Geng
Mike McBride
Senthil Dhanaraj
Gang Yan
Yang Xia
Status update

• 00 version posted at April 2018, and updated to 02 ever since.

• Renamed from [draft-xie-bier-6man-encapsulation-02] to [draft-xie-bier-ipv6-encapsulation-00]
  
  • Re-arranged & Updated Sections to make it more readable.

  • Removed the problem-statement part. Spawned new draft [draft-mcbride-bier-ipv6-problem-statement] to detail the problem statement and use cases of BIER in IPv6 environment as suggested IETF103 BIER WG discussion.

• Removed the dependency on SRH, and use Unicast IPv6 destination address instead.

• Detailed each field of the encapsulation, notably the IPv6 SA/DA and BIER Proto fields.

• Detailed the procedures, notably the IPv6-specific forwarding procedures.
The proposed encapsulation

<table>
<thead>
<tr>
<th>Ver</th>
<th>TC</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Payload Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Hdr = 4/41</td>
</tr>
<tr>
<td>BIFT-Id</td>
</tr>
<tr>
<td>Nibble</td>
</tr>
<tr>
<td>OAM</td>
</tr>
<tr>
<td>BitString (first 32 bits)</td>
</tr>
<tr>
<td>BitString (last 32 bits)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv4/IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original User multicast data packet</td>
</tr>
</tbody>
</table>

- Standard BIER header (RFC8296) in standard IPv6 Extension Header (RFC8200).
- New IPv6 option defined, change type 1 -- “Option Data may change en route”.
- IPv6 DA is well-known multicast in general case, and is unicast in special cases.
- IPv6 SA is routable IPv6 unicast, and used to identify a VPN/GTM.
Next Header values cover current BIER

- ‘Proto’ field in BIER Header ---- replaced by ‘Next Header’ in IPv6 Dest Option Header.
  - BIER Proto=1, indicating downstream-assigned MPLS payload, use Next Header value 137
  - BIER Proto=2, indicating upstream-assigned MPLS payload,
    - use IPv6 SA to identify the MVPN.
    - use Next Header value 4 or 41 to indicate IPv4/IPv6 payload.
  - BIER Proto=3, indicating Ethernet payload, use Next Header value TBD.
    - Value 97 can be used but it has an extra 2 octets.
    - A new value is better since Ethernet in IPv6 is common in SRv6-L2VPN too.
  - BIER Proto=4, indicating IPv4 payload, use Next Header value 4
  - BIER Proto=5, indicating BIER-OAM, use Next Header value 58
    - BIER-PING need some adaption to IPv6.
  - BIER Proto=6, indicating IPv6 payload, use Next Header value 41
Forwarding Procedure

- Normal BIER forwarding as required by RFC8279.
  - All steps (from step 1 to step 8) defined in section 6.5 of RFC8279 apply.
  - Walk through the BitString to determine the BFR-NBR(s) to copy packets to.
  - May change the BitString when copy packet to a BFR-NBR.
    - BIER option type have chg flag 1 for this purpose.
- Some “IPv6-specific” forwarding procedures required for this encapsulation.
  - IPv6 SA - Routable unicast IPv6 address (normally BFIR IPv6 Prefix).
  - IPv6 DA – BIER multicast address (FF0X::AB37) or Unicast address (BFR-Prefix).
    - BIERv6 packet (IPv6 header with BIER Option type) is dropped if the DA is not one of the above.
  - Nodes which support BIERv6, obtain the standard non-MPLS BIER header in the BIER Option type and perform the BIER forwarding as specified by RFC8279.
The General case: Use Multicast DA

Use multicast address FF0X::AB37 as DA while forwarding the BIER packets. (To be allocated by IANA – reserved by this draft)
Unicast DA Case 1: To bypass non-capable node

Use unicast address to bypass non-bier capable nodes. (No need for special tunneling - 😊)

IPv4/6 Hdr:
SA: X, DA: mcX
Payload

Outer IPv6 Header with BIER Header in Destination Options extension header

Inner IPv4/IPv6 multicast packet

IPv6 Hdr(Outer):
SA: A::1, DA: FF0X::AB37
Dest Opt Hdr:
BIER BitString: 0010
IPv4/6 Hdr(inner):
SA: X, DA: mcX
Payload

IPv6 Hdr(Outer):
SA: A::1, DA: FF0X::AB37
Dest Opt Hdr:
BIER BitString: 0100
IPv4/6 Hdr(inner):
SA: X, DA: mcX
Payload

IPv4/6 Hdr:
SA: X, DA: mcX
Payload
Unicast DA case-2:

This is an Unicast-Unicast case.
Why is the encapsulation

- Why use IPv6 Destination Option Header?
  - [RFC8200] Defining new IPv6 extension headers is not recommended, unless there are no existing IPv6 extension headers that can be used by specifying a new option for that IPv6 extension header.
  - [RFC8200] it is recommended that the Destination Options header is used to carry optional information that must be examined only by a packet’s destination node(s), because they provide better handling and backward compatibility.
  - IPv6 Destination Option Header is not only feasible, but also the recommended one in RFC8200.

- Why use well-known multicast address as IPv6 DA for general case?
  - [RFC8200] Extension headers are not processed 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.
  - This can not only simplify the forwarding, but also match the general concept of Replication.

- Why use Next Header instead of BIER Proto in IPv6 encapsulation?
  - Use of Next Header to indicate the format of the payload is more general IPv6 usage.
  - Better backward compatibility, e.g., enable offline tools to know the payload type.
BIERv6(L3) and BIER-ETH(L2.5) Brief Comparison

- Hop-by-hop replication
  - L3 BIER uses L3 multicast DA/MAC, and doesn't change hop-by-hop.
  - L2.5 BIER uses unicast MAC, and change hop-by-hop.

- Multi-hop replication
  - L3 BIER uses L3 unicast DA, without introducing tunnel handling.
    - Consider unicast-multicast, multicast-unicast, unicast-unicast replication.
  - L2.5 BIER uses L3 unicast tunnel (in Non-MPLS network).
    - May need more cost on tunnel endpoint encapsulation/decapsulation.
    - May need more filtering of L2.5 packets, since tunnel allows L2.5 packet, various L2.5 packets may come from the tunnel.
    - May need more control-plane to advertise the tunnel endpoint info like <draft-ietf-isis-encapsulation-cap>.
    - May need more packet length and header cascading using GRE/UDP.
    - May not be able to use the IPv6 SA to identify a VPN, while having to use IPv6 for tunneling.
Request to the WG

• Please join us

• Adoption Request
Thank you !