intarea
Internet-Draft
Intended status: Standards Track
Expires: July 16, 2021

Z. Zhang
R. Bonica
K. Kompella
Juniper Networks

January 12, 2021

Generic Delivery Functions
draft-zzhang-intarea-generic-delivery-functions-00

Abstract

Some functionalities (e.g. fragmentation/reassembly and Encapsulating Security Payload) provided by IPv6 can be viewed as delivery functions independent of IPv6 or even IP entirely. This document proposes to provide those functionalities at different layers (e.g., MPLS, BIER or even Ethernet) independent of IP.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Consider an operator providing Ethernet services such as pseudowires, VPLS or EVPN. The Ethernet frames that a Provider Edge (PE) device receives from a Customer Edge (CE) device may have a larger size than the PE-PE path MTU (pMTU) in the provider network. This could be because

1. the provider network is built upon virtual connections (e.g. pseudowires) provided by another infrastructure provider, or

2. the customer network uses jumbo frames while the provider network does not, or

3. the provider-side overhead for transporting customers packets across the network pushes past the pMTU.

In any case, the provider cannot simply require its customers to change their MTU.

To get those large frames across the provider network, currently the only workaround is to encapsulate the frames in IP (with or without GRE) and then fragment the IP packets. Even if MPLS is used for service delimiting, IP is used for transporation (MPLS over IP/GRE). This may not be desirable in certain deployment scenarios, where MPLS

is the preferred transport or IP encapsulation overhead is deemed excessive.

IPv6 fragmentation and reassembly are based on the IPv6 Fragmentation header below [RFC8200]:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Next Header  |   Reserved    |      Fragment Offset    |Res|M|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Identification                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: IPv6 Fragmentation Header

This document proposes adapting this header for use in non-IP contexts, since the fragmentation/reassembly function is actually independent of IPv6 except the following aspects:

- The fragment header is identified as such by the "previous" header.
- The "Next Header" value is from the "Internet Protocol Numbers" registry.
- The "Identification" value is unique in the (source, destination) context provided by the IPv6 header

The "Identification" field, in conjunction with the IPv6 source and destination identifies fragments of the original packet, for the purpose of reassembly.

Therefore, the fragmentation/reassembly function can be applied at other layers as long as a) the fragment header is identified as such; and b) the context for packet identification is provided. Examples of such layers include MPLS, BIER, and Ethernet (if IEEE determines it is so desired).

For the same consideration, the IP Encapsulating Security Payload (ESP) [RFC4303] could also be applied at other layers if ESP is desired there. For example, if for whatever reason the Ethernet service provider wants to provide ESP between its PEs, it could do so without requiring IP encapsulation if ESP is applied at non-IP layers.

We refer to these as Generic Delivery Functions (GDFs), which could be achieved at a shim layer between a source and destination delivery points, for example:

- o Source and destination IP/Ethernet nodes

- o Ingress and egress nodes of MPLS Label Switch Paths (LSPs)

- o BIER Forwarding Ingress Routers (BFIRs) and BIER Forwarding Egress Routers (BFERs)

It is not the intention to apply the GDFs hop by hop between the source and destination delivery points.

The possibility of applying some other IP functions (e.g. Authentication Header [RFC4302]) is for further study.

2. Specifications

2.1. Generic Delivery Function Header

The following Generic Delivery Function Header (GDFH) is defined:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0| Rsved |  This Header  | Header Length |  Next Header  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~              Variable field per "This header"                 ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Generic Delivery Function Header

0000 nibble: Prevents the GDFH from being mistaken as an IP header by a router doing deep packet inspection for ECMP hashing purpose.

This Header: The type of this GDFH header. For example, TBD1 for generic fragmentation, TBD2 for generic ESP. The values are from a space independent of the "Next Header".

Header Length: The number of octets of the entire header.

Next Header: The type of next header. For functions that IETF is concerned with, the "Next Header" values are from the "Internet Protocol Numbers" registry. A next header could be another GDFH, so a value is to be assigned for GDFH from the registry.

The outer header MUST identify that a GDFH follows. Encoding "This Header" in the GDFH allows that a single outer header encoding can be used for different GDFHs.

If the outer header is BIER, a TBD value for the "proto" field in the BIER header identifies that a GDFH follows.

If the outer header is MPLS, the label preceding the GDFH indicates that a GDFH follows (see Section 2.5).

If the outer header is Ethernet (if IEEE would decide to provide the generic delivery functions on top of Ethernet directly), then a new Ethertype would be assigned by IEEE.

2.2. Generic Fragmentation Header

For generic fragmentation/reassembly functionality, the GDFH takes the following Generic Fragmentation Header (GFH) format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0| Rsved | Header Length |     TBD1      |  Next Header  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Fragment Offset    |R|S|M| Identification (variable)     ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Identification                        |
|                           (continues)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: Generic Fragmentation Header

The "Fragment Offset" and "M" flag bit fields are as in the IPv6 Fragmentation Header.

R: The "R" flag bit is reserved. It MUST be 0 on transmitting and ignored on receiving.

Identification: at least 4-octet long. // would 2-octet be ok as minimum?

S: If the "S" flag bit is clear, the context for the Identification field is provided by the outer header, and only the source-identifying information in the outer header is used.

If the "S" flag bit is set, the variable Identification field encodes both source-identifying information (e.g. the IP address of the node adding the GFH) and an identification number unique within that source.

When a GFH is used together with other GDFHs, the GFH SHOULD be the first GDFH.

If the outer header is BIER and the "S" flag bit is clear, the "BFIR-id" field in the BIER header provides the context for the "Identification" field.

If the outer header is MPLS, the "S" flag bit MAY be clear if the the label preceeding the GFH identifies the sending node in addition to indicating that a GFH follows (see Section 2.5).

2.3. Payload Type Header

While originally it is not the intention to provide a way to identify the payload type after an MPLS label stack, it has been pointed out that the GFH now provides the payload-identifying functionality as a by product - even when fragmentation is not needed, a GFH can be inserted, with the Fragmentation Offset, the M-bit and Identification fields set to 0, and the Next Header set appropriately.

If the payload-identifying functionality is deemed as desired, a dedicated header type could be assigned for this purpose, with a smaller header compared to GFH.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0| Rsved |Header Length:4|     TBD3      |  Next Header  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: Generic Payload Type Header

2.4. Generic ESP/Authentication Header

To be specified in future revisions.

2.5. MPLS Signaling

When GDFH is used with MPLS, the preceeding label needs to indicate that a GDFH follows, and optionally identify the node that does the fragmentation. The label can be signaled via BGP or IGP as sepcified below.

2.5.1. BGP Signaling

This document defines a new transitive BGP "GDFH Labels" attribute, very similar to the "PE Distinguisher Labels" attribute defined in [RFC6514] (and the text below is adapted from Section 8 of [RFC6514]):

```
+----------------------------------+
|     Node Address                 |
+----------------------------------+
|     Label (3 octets)             |
+----------------------------------+
.......
+----------------------------------+
|     Node Address                 |
+----------------------------------+
|     Label (3 octets)             |
+----------------------------------+
```

The Label field contains an MPLS label encoded as 3 octets, where the high-order 20 bits contain the label value. The Node Address MAY be 0, meaning that the following label only indicates a GDFH follows when the label is used in the label stack of a data packet.

The Node Address MAY also be a unicast address, indicating that the following label when used in the label stack of a data packet will both indicate that a GDFH follows and identify the sending node.

If a node supports GDFH with MPLS, it attaches the attribute in the BGP routes for its local addresses. A border router SHOULD remove the attribute if no node beyond the border will use GDFH with MPLS to send traffic to the corresponding addresses.

A router that supports the attribute considers this attribute to be malformed if the Node Address field does not contain a unicast address or 0. The attribute is also considered to be malformed if: (a) the Node Address field is expected to be an IPv4 address, and the length of the attribute is not a multiple of 7 or (b) the Node Address field is expected to be an IPv6 address, and the length of the attribute is not a multiple of 19. The Address Family Indicator (AFI) of the BGP route that the attribute is attached to provides the information on whether the Node Address field contains an IPv4 or IPv6 address. Each of the Node Addresses in the attribute MUST be of the same address family as the route that is carrying the attribute.

2.5.2. IGP Signaling

This document defines an OSPFv2 "GDFH Labels" sub-TLV of OSPFv2 Extended Prefix TLV [RFC7684], with the value part being the same as BGP "GDFH Labels" attribute above. If an OSPFv2 router surports GDFH with MPLS, it includes the GDFH Labels sub-TLV in the Extended Prefix TLV that is attached to its local addresses advertised in its OSPFv2 Extended Prefix Opaque LSA.

Similary, This document defines an OSPFv3 "GDFH Labels" sub-TLV of OSPFv3 Intra/Inter-Area-Prefix TLVs [RFC8362], with the value part being the same as BGP "GDFH Labels" attribute above. If an OSPFv3 router surports GDFH with MPLS, it includes the GDFH Labels sub-TLV in the Intra-Area-Prefix TLV for its local addresses.

This document also defines an ISIS "GDFH Labels" sub-TLV of ISIS prefix-reachability TLV [RFC5120] [RFC5305] [RFC5308], with the value part being the same as BGP "GDFH Labels" attribute above. If an ISIS router surports GDFH with MPLS, it includes the sub-TLV to the prefix-reachability TLV for its local addresses.

For both OSPF and ISIS, when advertising a prefix from one area/level to another, if there is a "GDFH Labels TLV" attached in the source area/level, the TLV SHOULD be attached in the target area/level and the prefix SHOULD NOT be summarized.

3. Security Considerations

To be provided.

4. IANA Considerations

This document makes the following IANA requests:

o A new BGP Attribute type for "GDFH Labels" from the BGP Path Attributes registry

o A new OSPFv2 sub-TLV type for "GDFH Labels" from the OSPFv2 Extended Prefix TLV Sub-TLVs registry

o A new OSPFv3 sub-TLV type for "GDFH Labels" from the OSPFv3 Extended-LSA sub-TLV registry

o A new BIER Next Protocol Identifier value for GDFH from BIER Next Protocol Identifiers registry

o A new Internect Protocol Number for GDFH from the Internet Protocol Numbers registry

This document requests IANA to set up a "Generic Deliver Function Header Types" registry with the following initial assigements:

0: Reserved

1: Generic Fragmentation

2: Generic ESP

5. Acknowledgements

The authors thank Stewart Bryant and Tony Przygienda for their valuable comments and suggestions.

6. References

6.1. Normative References

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <https://www.rfc-editor.org/info/rfc5305>.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI 10.17487/RFC5308, October 2008, <https://www.rfc-editor.org/info/rfc5308>.

[RFC7684] Psenak, P., Gredler, H., Shakir, R., Henderickx, W., Tantsura, J., and A. Lindem, "OSPFv2 Prefix/Link Attribute Advertisement", RFC 7684, DOI 10.17487/RFC7684, November 2015, <https://www.rfc-editor.org/info/rfc7684>.

[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>.

[RFC8362] Lindem, A., Roy, A., Goethals, D., Reddy Vallem, V., and F. Baker, "OSPFv3 Link State Advertisement (LSA) Extensibility", RFC 8362, DOI 10.17487/RFC8362, April 2018, <https://www.rfc-editor.org/info/rfc8362>.

6.2. Informative References

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC6514] Aggarwal, R., Rosen, E., Morin, T., and Y. Rekhter, "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", RFC 6514, DOI 10.17487/RFC6514, February 2012, <https://www.rfc-editor.org/info/rfc6514>.

Authors' Addresses

Zhaohui Zhang
Juniper Networks
1133 Innovation Way
Sunnyvale 94089
USA

Phone: +1 408 745 2000
Email: zzhang@juniper.net

Ron Bonica
Juniper Networks
1133 Innovation Way
Sunnyvale 94089
USA

Phone: +1 408 745 2000
Email: rbonica@juniper.net

Kireeti Kompella
Juniper Networks
1133 Innovation Way
Sunnyvale 94089
USA

Phone: +1 408 745 2000
Email: kireeti@juniper.net