Generalized IPv6 Tunnel

draft-li-rtgwg-generalized-ipv6-tunnel-03

draft-li-rtgwg-gip6-for-quic-00

draft-li-rtgwg-gip6-for-mpls-00

draft-li-rtgwg-gip6-protocol-ext-requirements-01

Zhenbin (Robin) Li, Shuanglong Chen, Qiangzhou Gao, Hang Shi, Tianran Zhou, Shuping Peng (Huawei)

Shuai Zhang, Xinxin Yi (China Unicom)

Qingbang Xu (Agricultural Bank of China)

Why Need GIP6

- Currently there are many types of IP tunnels, such as VXLAN and GRE. On IPv6 networks, it is hard to define extensions for all these tunnels to support new features. On the other hand it is not recommended to extend new features based on the IPv4 data plane for these tunnels

There have been many types of IP tunnels

- GRE Tunnels: defined in [RFC2784].
- IP in IP Tunnels: defined in [RFC1853].
- L2TPv3 Tunnels: defined in [RFC3931].
- ISATAP Tunnels: defined in [RFC4214].
- IPv4/IPv6 over IPv6 (4over6) Tunnels: defined in [RFC2473].
- VXLAN Tunnels: defined in [RFC7348].
- NVGRE Tunnels: defined in [RFC7637].
- MPLS over UDP: defined in [RFC7510].
- VXLAN-GPE (Generic Protocol Extension for VXLAN) Tunnels: defined in [I-D.ietf-nvo3-vxlan-gpe].

New Features

- [I-D.dong-6man-enhanced-vpn-vtn-id] defines the IPv6 encapsulation used to determine resource isolation.
- [I-D.li-apn-ipv6-encap] defines the IPv6 encapsulation of an APN.
- [I-D.ietf-6man-ipv6-alt-mark] defines IPv6 encapsulation for Alternate Marking.
- [I-D.ietf-ippm-ioam-ipv6-options] defines IPv6 encapsulation for IOAM.

Challenges

If the existing IP tunnels need to support new features such as Alternate Marking, IOAM, resource isolation, and APN, the following problems exist:

1. **A Lot Of Standardization work:** All of the IP tunnels mentioned above need to be extended accordingly, resulting in a lot of standardization work.

2. It is **hard to keep the consistency** between IPv4 and IPv6 for these IP tunnels (except IPv4 transition tunnels) since the possible extensions are recommended to be only done over the IPv6.

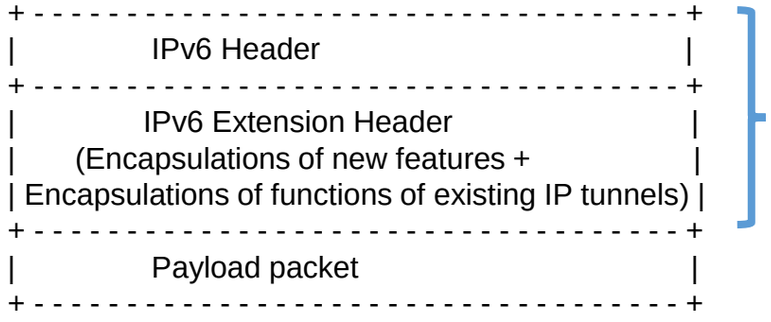
3. **Functions Redundant:** IPv6 can directly support some functions of these IP tunnels which cannot be done over the IPv4. This means such functions becomes redundant over the IPv6. For example, VXLAN takes use of the UDP to support ECMP. However for the IPv6 VXLAN, the Flow Label in the IPv6 header can also be used to support ECMP.

4. **Difficult to extend based on the existing format:** Some IP tunnels such as VXLAN and GRE have their own headers. If these tunnels need to support new features over the IPv6, there will face the challenge of the choice between reusing the exiting IPv6 encapsulations for these new features based on the IPv6 extension header and define new extensions based on their own tunnel headers.
    1) - If the tunnel header is extended, it will be redundant with the existing IPv6 encapsulation for the new features based on the IPv6 extension header.
    2) - For some existing IP tunnels (such as IP in IP) that do not have their own headers, they have to reuse the IPv6 encapsulations for these new features based the IPv6 header. extensions need to be redefined in the IPv6 extension header. As a result, their extensions may be different from that of the IP tunnels which have their own headers.

GIP6 Technical Description

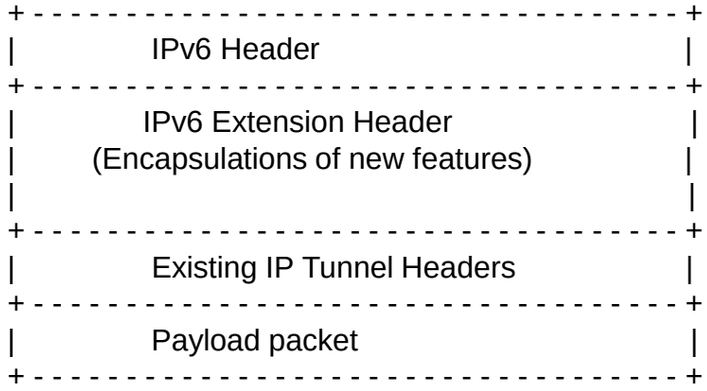
- The Generalized IPv6 (GIP6) tunnel is defined to use the IPv6 header and IPv6 extension header to support both existing IP tunnels functions and new features.
- A GIP6 encapsulated packet has the following format:

Option 1 (Recommended)



GIP6 Encapsulation

Option 2



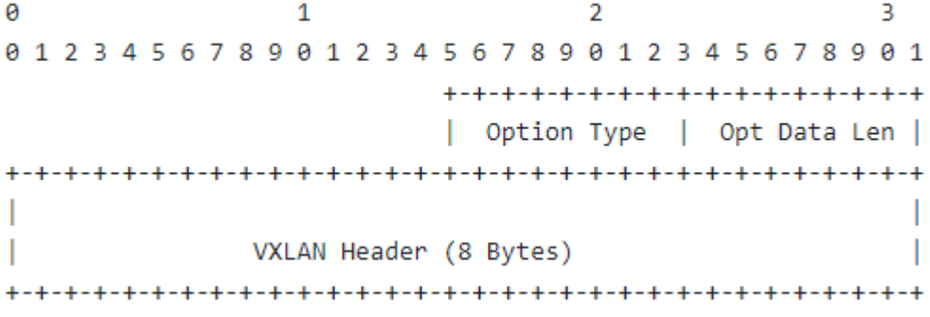
GIP6 Encapsulation

GIP6 for VXLAN

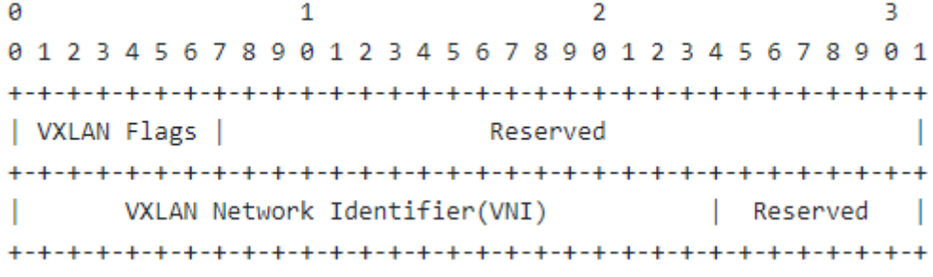
- 1. The function of the UDP is replaced by the flow label of the IPv6 header in the GIP6 tunnel. To ensure compatibility, the value of the flow label calculated for the purpose of ECMP SHOULD be the same as that of the source port of the UDP.
- 2. Definition of the VN Option

A new option called VN Option is defined to carry the VXLAN header information. The VN Option MUST only be encapsulated in the Destination Options Header (DOH).

VN Option



VXLAN headers

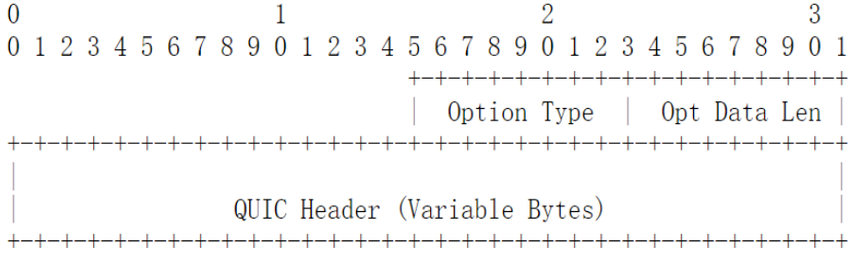


GIP6 for QUIC @ draft-li-rtgwg-gip6-for-quic-00

- 1. The function of the UDP is replaced by the flow label of the IPv6 header in the GIP6 tunnel. To ensure compatibility, the value of the flow label calculated for the purpose of ECMP SHOULD be the same as that of the source port of the UDP.
- 2. Definition of the QUIC Option

A new option called QUIC Option is defined to carry the VXLAN header information. The QUIC Option MUST only be encapsulated in the Destination Options Header (DOH).

QUIC Option



Generalized IPv6 Tunnel for MPLS

draft-li-rtgwg-gip6-for-mpls-00

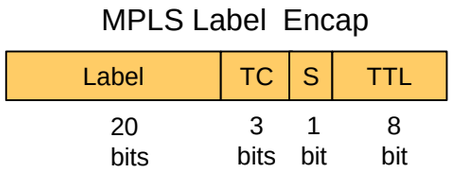
Technical Challenges to MPLS

1. MPLS is lack of the source indication and MP2P connections may occur. This causes the difficulty and complex process for OAM over MPLS. Although SFL([RFC8957]) is defined, there is few implementation.

2. The payload type (for example, L2 or L3 packets) cannot be directly determined because there is no payload indication.

3. There is no metadata extensibility and it is difficult to encapsulate new forwarding attributes for the new features such as IETF network slicing, IFIT, and APN.

4. The process of the ECMP function is complex and affects forwarding performance. Entropy labels or flow labels are placed at the bottom of the label stack for processing and the internal IP header information may have to be parsed for the purpose of ECMP.



GIP6 tunnel for MPLS

Draft-li-rtgwg-generalized-ipv6-tunnel defines the GIP6 tunnel to support both new features(iOAM/APN…) and the existing functions for the IP tunnels based on the extension of the IPv6 extension header.

If the GIP6 tunnel is used for MPLS, there can be the following advantages:

1. The IPv6 source address is used to form a source identifier.

2. The IPv6 NH can indicate the payload type.

3. IPv6 flow labels are used to implement ECMP.

4. The encapsulations for the new features have been defined well in the IPv6 and can be reused easily.

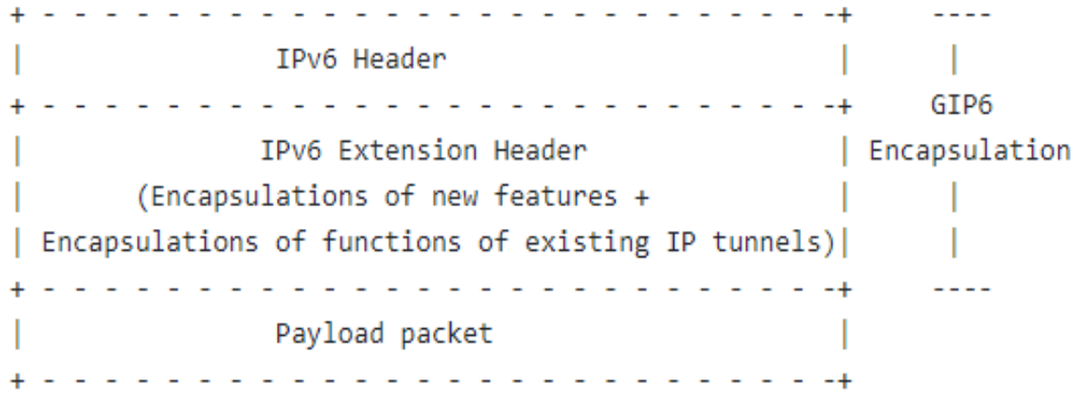
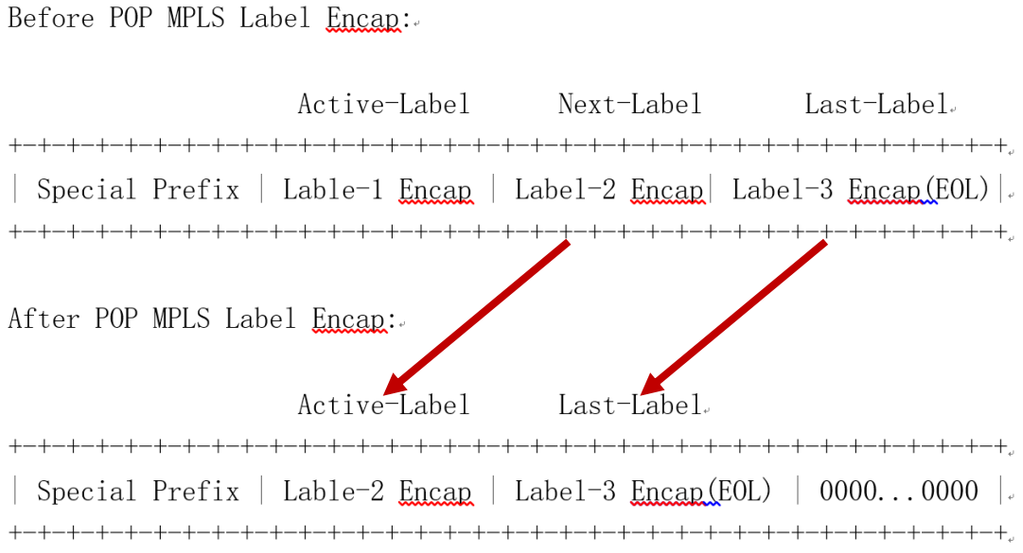


Figure 1. GIP6 Encapsulation

IPv6 MPLS SID(Type 1) can be placed in the IPv6 destination address

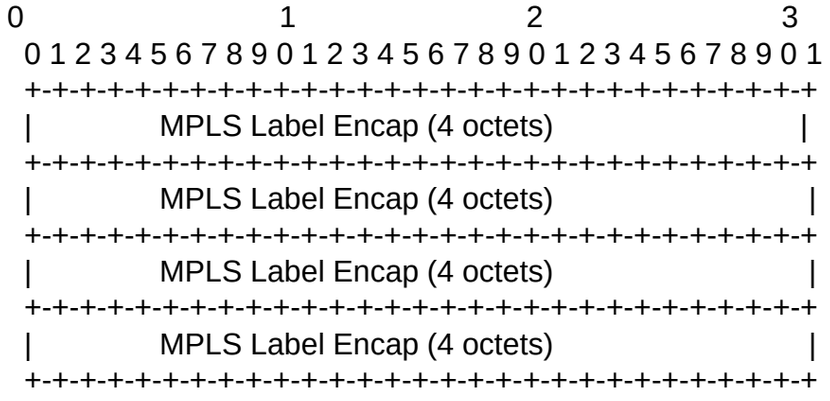
- Processing of the first label following the special prefix is as follows:
- ✓ (1) If the local action of the MPLS label is POP, the followed label encapsulations are shifted left by 32 bits after the label is popped. The following figure shows the process.



- ✓ (2) If the local action of the MPLS label is SWAP, the label encapsulation is changed to the new label after swap.

IPv6 MPLS SID(Type 2) can be placed in the IPv6 RH

- If all the MPLS label stack cannot be placed in the IPv6 destination address, IPv6 RH can be used to house the remaining MPLS label stack.
- ✓ (1) IPv6 MPLS SID (Type 2) is defined to house multiple (<= 4) label encapsulations. The format of the IPv6 MPLS SID (Type 2) is shown in the following figure.



- ✓ (2) IPv6 MPLS SID (Type 2) is used as the segment in the RH. After all of the label encapsulations in the IPv6 destination address are popped, the first label encapsulation in the segment indicated by the SL of the RH will be processed.

Control Plane Considerations

- GIP6 only provides a way to carry MPLS label encapsulations in the data plane.
- The existing MPLS control plane does not need to be changed.
- That is, MPLS labels on the control plane can still be distributed for IPv4, IPv6, L2, etc.

Protocol Extension Requirements of Generalized IPv6 Tunnel

draft-li-rtgwg-gip6-protocol-ext-requirements-01

Problem Statement

- Currently many new features are emerging and the corresponding encapsulations over the IPv6 are defined:
  - [RFC8704] defines IPv6 encapsulation for SRv6 network programming.
  - [I-D.ietf-6man-ipv6-alt-mark] defines IPv6 encapsulation for Alternate Marking.
  - [I-D.ietf-ippm-ioam-ipv6-options] defines IPv6 encapsulation for IOAM.
  - [I-D.ietf-6man-enhanced-vpn-vtn-id] defines the IPv6 encapsulation used to determine resource isolation.
  - [I-D.yzz-detnet-enhanced-data-plane]defines the IPv6 encapsulation for implementing bounded latency.
  - [I-D.li-apn-ipv6-encap] defines the IPv6 encapsulation of an APN.

- In the process of deployment of these new features, because network devices have different capabilities of IPv6 extension header processing, the following issues are identified:
  - Some legacy network devices can only process IPv6 extension header (Hop-by-Hop Options Header) on slow path, which has negative impact on the routing jobs on the control plane. So in existing networks, packet with IPv6 extension headers are usually blocked by ACL. This will cause the packet loss on these network devices if the packet encapsulated with GIP6 tunnel and the HbH is used for the new features.
  - Network devices can only support some of the extension headers used for the new features. If the packet encapsulated with GIP6 tunnel and specific types of IPv6 extension headers used cannot be supported by these network devices, new features cannot be guaranteed along the path.
  - Network devices can only process limited number of options in an IPv6 extension header (including HbH and DoH). So when multiple options coexists to support different new features in the IPv6 extension header of the GIP6 tunnel, those devices may drop the packet.

Requirements (1)

- Way to advertise the capability
  - There are two different ways. One is to advertise the capability among network devices. So that a network device can find the right next hop with IPv6 extension header processing capabilities. In this case, IGP or BGP-SPF extensions are required for the information distribution. The other way is to report the IPv6 capabilities from network nodes to a controller. So that the network controller can calculate the right path comprised with available nodes. In this case, BGP-LS or NETCONF/YANG are considered for the extensions.

- Inter-Domain
  - A path may be across multiple network domains. The ingress node of the GIP6 tunnel need to know if all the nodes along the path can process the IPv6 extension headers properly. In this case, the capability of IPv6 extension header processing need to be distributed among multiple domains. BGP can be extended to advertise the IPv6 capability information from the egress node to the ingress node. If there is a controller collecting IPv6 capability information from multiple domains, PCEP or BGP can be extended and used by the controller to deliver information to the ingress node about the right path along which network nodes can process the IPv6 extension header properly.

Requirements (2)

- Capability about IPv6 Extension Header
  - Supporting Hop by Hop options header (HbH) or not.
  - Fast path or slow path processing of HbH.
  - Supporting Segment Routing Header (SRH) or not.
  - Supporting Destination Options header (DoH) or not.
  - Capabilities about coexistence of multiple extension headers, for example, the combination of HbH and Authentication Header (AH).
  - The maximum length of each IPv6 extension header
  - The maximum total length of IPv6 extension headers

- Capability about Options of IPv6 Extension Header
  - The maximum number of options supported in the HbH
  - The maximum number of options supported in the DoH
  - Supporting SRH TLV or not and the maximum number of TLVs supported in the SRH
  - The maximum number of segments in the SRH

Requirements (3)

- Capability about Specific Features
  - Slicing: the NRP option can be supported or not. If support, the NRP option can be placed in HbH and/or DoH.
  - Alternate Marking: the Alternate Marking option can be supported or not. If support, the Alternate Marking option can be placed in HbH and/or DoH.
  - IOAM: the IOAM option can be supported or not. If support, the IOAM option can be placed in HbH and/or DoH.
  - APN: the APN option can be supported or not. If support, the APN option can be placed in HbH, DoH and/or SRH TLV.
  - DetNet: the BLI option [I-D.yzz-detnet-enhanced-data-plane] can be supported or not. If support, the BLI option can be placed in HbH and/or DoH.

Next Steps

- Comments are welcome

Thank You