Network Working Group
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

X. Yi
China Unicom
Z. Li
Q. Gao
B. Liu
T. Zhou
S. Peng
Huawei

3 March 2025

Scenarios and Protocol Extension Requirements of a Generalized IPv6 Tunnel
draft-li-rtgwg-gip6-protocol-ext-requirements-03

Abstract

IPv6 provides extension header mechanism for additional functions. There are emerging features based on the extension headers, such as SRv6, Network Slicing, Alternate Marking, iOAM, DetNet etc. In some networks, the operators might want to leverage these new features but since the network system still using some lagecy encapsulations other than IPv6 (e.g. VxLAN, GRE etc.), these features are just not applicable for them.

This document introduces some cases of such scenarios, and discusses the potential requirement of defining a new Generalized IPv6 Tunnel (GIP6). With GIP6, all the additional functions defined as IPv6 extension headers could be easily supported, so that the legacy encapsulations could migrate to a unified solution rather than sccaterred upgrade in each legacy technologies, which is heavy burden for the industry.

Considering network devices have different capabilities of IPv6 extension header processing, this document also analyses the issues found during the deployment of the above new features using IPv6 extension headers and the protocol extension requirements for IPv6 capability advertisement are defined.

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].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

IPv6 provides extension header mechanism for additional functions. There are emerging features based on the extension headers, such as:

- [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.

There are some scenarios that the network operators want to leverage these new features but since the network system still using some lagecy encapsulations other than IPv6 (e.g. VxLAN, GRE etc.), so these features are not applicable. GIP6 [I-D.li-rtgwg-generalized-ipv6-tunnel] defines a generalized IPv6 tunnel to unify the IP tunnels to support the new features. With GIP6, all the additional functions defined as IPv6 extension headers could be easily supported, so that the legacy encapsulations could migarate to a unified solution, rather than extending all the legacy IP tunnels individually.

However, network devices have different capabilities of IPv6 extension header processing, which hugely impact the deployment of these features, even causes the packet loss. Thus, this document also analyses the issues found during the deployment of the above new features using IPv6 extension headers. In order to solve the issues, the capabilities of IPv6 extension header process can be advertised among network devices and reported from network devices to the controller. Based on these IPv6 capability information, the new features can be deployed properly.

2. Terminology

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

iOAM: In-situ Operations, Administration, and Maintenance

SRv6: Segment Routing over IPv6

VxLAN: Virtual Extensible LAN

GRE: Generic Routing Encapsulation

GTP: GPRS Tunnelling Protocol

GPRS: General Packet Radio Service

3. Scenarios and Gaps

3.1. Private line E2E Measurement/Troubleshooting

Operators might want to leverage iOAM technologies to provide users with performance measurement and troubleshooting capabilities across the entire private line, which requires end-to-end iOAM implementation might across the WAN (Wide Area Network) and the DCN (Data Center Network). Especially in the SFC (Service Function Chain) scenario, the path of data flow may enter and exit the cloud multiple times, making fault localization extremely complex. The current issue is that the WAN and DCN might use different VPN technologies, for example, SRv6 for WAN and VxLAN for DCN. In the DCN segment (as well as the access segment in some cases), the lack of support for iOAM in VxLAN results in an inability to have end-to-end iOAM functionality across the path. This limits the ability to have unified performance measurement and troubleshooting across the entire private line.

3.2. V2X Experience Guaranting

In Vehicle-to-Everything (V2X) communications, the network usually needs to distinguish different types of data flows (for example: media flows and remote driving signaling flows). And one common choice is to utilizing network slicing technology, so as to meet the performance and priority requirements of different services. Moreover, it is also necessary to provide high-precision performance monitoring and fault localization capabilities for critical services (e.g., remote driving). This requires end-to-end iOAM features

throughout the entire path from the RAN to the WAN. In current V2X networks, GTP is the standard encapsulation protocol in Radio Access Network (RAN), and IPv6 or SRv6 is the mainstream encapsulation protocol in WAN. The GTP tunnel itself lacks support for advanced features such as network slicing and iOAM, making it impossible to achieve end-to-end performance detection and slice-based flow differentiation and management.

3.3. SD-WAN E2E Slicing/iOAM

Similarly as the V2X case described above, in SD-WAN scenario, due to the widely used GRE protocol does not support iOAM and slicing features, it is also impossible to achieve end-to-end performance detection and slice-based flow differentiation and management.

3.4. Data sharing/exchagne between Enterprises

Users such as enterprises or hospitals may have demand for data sharing or exchange. Since these data often involve sensitive information, it is necessary to protect the data packets accordingly. One good way is to use an identifier encapsulated into IPv6 header to classify and identify the sensitivity level of data, so that the circulation scope of sensitive data can be controlled and a credible network path can be ensured throughout the entire process. Besides, when the data reaches the receiver, the receiver can also determine whether the data is credible and whether it can be received based on the ID.

In this scenario, there are two situations:

1) Data transmission between users that across cities

   In this situation, the tunnel encapsulation methods may be different in different metropolitan area networks, and the methods for metropolitan area networks and backbone networks may also differ.

2) User data entering into the cloud

   Clouds are generally connected to backbone networks, the methods for metropolitan area networks and backbone networks may be different.

The differentiated tunnel encapsulation methods may result in the loss of the encapsulated ID on the packet. For example, when packets enter MPLS tunnels from IPv6 domain, information encapsulated in IPv6 header is lost. As a result, the credibility and controllability of data circulation service cannot be guaranteed.

4. Protocol Extensions of Capability Advertisement

4.1. Problems of Extention Header Processing

As described in Section 1, many new features are emerging and the corresponding encapsulations over the IPv6 are defined. There features uses the IPv6 extension headers including HbH (Hop-by-Hop Options Header), DoH (Destination Options Header) and SRH (Segment Routing Header).

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.

4.2. Protocol Extensions

To solve the above issues, there are requirements for protocol extensions to advertise the capability of IPv6 extension header processing so as to identify the unavailable nodes and facilitate the deployment of new features successfully.

4.2.1. Capability Advertisement

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.

4.2.2. Inter-Domain Operation

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.

4.2.3. Capabilities about IPv6 Extension Header

Network devices need to advertise its capability information about what IPv6 extension header can be supported. These capabilities may include:

* 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

4.2.4. Capability about Options of IPv6 Extension Header

Network devices need to advertise its capability information about process options in the IPv6 extension headers. These capabilities may include:

* 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

4.2.5. Capability about Specific Features

In addition to the common capabilities described above, network devices may support some specific features only. These capabilities may include:

* 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.

5. IANA Considerations

This document makes no request of IANA.

6. Security Considerations

TBD

7. Normative References

[I-D.ietf-6man-enhanced-vpn-vtn-id]
Dong, J., Li, Z., Xie, C., Ma, C., and G. S. Mishra, "Carrying Network Resource (NR) related Information in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-ietf-6man-enhanced-vpn-vtn-id-09, 3 November 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-enhanced-vpn-vtn-id-09>.

[I-D.ietf-6man-ipv6-alt-mark]
Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate-Marking Method", Work in Progress, Internet-Draft, draft-ietf-6man-ipv6-alt-mark-17, 27 September 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-ipv6-alt-mark-17>.

[I-D.ietf-ippm-ioam-ipv6-options]
Bhandari, S. and F. Brockners, "In-situ OAM IPv6 Options", Work in Progress, Internet-Draft, draft-ietf-ippm-ioam-ipv6-options-12, 7 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-ioam-ipv6-options-12>.

[I-D.li-apn-ipv6-encap]
Li, Z., Peng, S., and C. Xie, "Application-aware IPv6 Networking (APN6) Encapsulation", Work in Progress, Internet-Draft, draft-li-apn-ipv6-encap-07, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-li-apn-ipv6-encap-07>.

[I-D.li-rtgwg-generalized-ipv6-tunnel]
Li, Z., Chen, S., Gao, Q., Zhang, S., and Q. Xu, "Generalized IPv6 Tunnel (GIP6)", Work in Progress, Internet-Draft, draft-li-rtgwg-generalized-ipv6-tunnel-04, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-li-rtgwg-generalized-ipv6-tunnel-04>.

[I-D.yzz-detnet-enhanced-data-plane]
Geng, X., Zhou, T., Zhang, L., and Z. Du, "DetNet Enhanced Data Plane", Work in Progress, Internet-Draft, draft-yzz-detnet-enhanced-data-plane-03, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-yzz-detnet-enhanced-data-plane-03>.

[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>.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

Authors' Addresses

Xinxin Yi
China Unicom
Beijing,100048
China
Email: yixx3@chinaunicom.cn

Zhenbin Li
Huawei
156 Beiqing Road
Beijing,100095
China
Email: lizhenbin@huawei.com

Qiangzhou Gao
Huawei
156 Beiqing Road
Beijing,100095
China
Email: gaoqiangzhou@huawei.com

Bing Liu
Huawei
156 Beiqing Road
Beijing,100095
China
Email: leo.liubing@huawei.com

Tianran Zhou
Huawei
156 Beiqing Road
Beijing,100095
China
Email: zhoutianran@huawei.com

Shuping Peng
Huawei
156 Beiqing Road
Beijing,100095
China
Email: pengshuping@huawei.com