6man Working Group
Internet Draft
Intended status: Informational
Expires: September 6, 2024

W. Cheng
L. Gong
China Mobile
C. Lin
H. Li
New H3C Technologies

March 6, 2024

Source IPv6 Address Programmability
draft-cheng-6man-source-address-programmability-02

Abstract

IPv6-based tunneling technologies, such as SRv6, have been deployed by provider on transport networks to provide users with services such as VPN and SD-WAN.

After the service traffic enters the provider's transport network, it will be encapsulated by tunnel (SRv6 encapsulation). In order to better meet the SLA requirements of users, some technologies need to carry relevant information along with the flow to guide the processing of packets during forwarding.

This document discusses the programmability of IPv6 source addresses to carry the necessary flow information

Table of Contents

1. Introduction

IPv6-based tunneling technologies, such as SRv6, have been deployed by provider on transport networks to provide users with services such as VPN and SD-WAN.

When the ingress node (PE) of the transport network receives user traffic, it can add IPv6 (SRv6) encapsulation to the user traffic according to VPN routes and policies, and the encapsulated service traffic is forwarded to the egress device of the transport network.

SRv6 [RFC8754] is a source routing technology. The ingress node of the transport network encapsulates the forwarding path (segment list) of user traffic in SRH. The encapsulated user traffic will be forwarded to the egress node according to the path specified by the SRH.

Meanwhile, in order to better meet user SLA requirements and provide differentiated services, it is necessary to be able to carry flow-related information with the traffic.

Although IPv6 itself provides a variety of extension headers, which can carry various flow information through extension headers, due to various considerations such as bandwidth utilization and device implementation difficulty, carrying flow information through source addresses is becoming a possible choice

This document mainly discusses the requirements for source IPv6 address programmability to support subsequent related specifications or protocol extensions.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Restrictions for IPv6 Source address programmability

The IPv6 source address programmability described in this document is limited to a limited or trusted domain, such as the SRv6 domain of a provider's transport network.

In a limited domain or trusted domain, the programmable capability of the IPv6 source address is allowed to carry flow information. That is, when the business flow enters the trust domain, it is encapsulated, and the flow information is encoded in the source address at the same time. Encapsulation is removed when business traffic leaves the trust domain. This leakage of source addresses outside the trusted domain needs to be avoided.

End-to-end IPv6 source address programmability is not recommended.

```
                       +-----+     +-----+    +-----+
   SRv6 Encapsulated   +-----+     +-----+    +-----+
    packet             |     |     |     |    |     |
            +------+   +-----+     +-----+    +-----+    +-----+
   Original |      |                                     |     |
   packet   +------+                                     +-----+
     ----------------------------------------------------------->

                +----------------------------------+
                |             SRv6  domain         |
         +----+ |  +----+   +--+    +--+    +----+ | +----+
    -----+CE1+--+---+PE1+----+P1+-----+P2+-----+PE2+--+--+CE2+----
         +----+ |  +----+   +--+    +--+    +----+ | +----+
                |                                  |
                +----------------------------------+
```

Figure 1: example topology

3. Requirement for IPv6 source address programmability

In some scenarios, flow information needs to be carried with the packet to help routers to perform special processing on the packet when forwarding. The flow information may be associated with the local resources of the router, and are used to guarantee the bandwidth of a specific flow; or identify a certain attribute of the service flow, through which the forwarding policy can be applied, and so on.

Although various extension headers have been defined in [RFC8200], information can be carried through these different types of extension headers. However, based on the current actual situation, there are some defects in carrying information through the extension header, such as

o Low bandwidth utilization

Taking SRv6 TE as an example, user traffic is encapsulated with SRH and IPv6 headers on the headend node, and the newly added encapsulation itself occupies part of the bandwidth. If flow information is carried through other extension headers such as DOH or HBH, the bandwidth utilization rate will further decrease, especially for small packets.

o Highly difficult to implement

According to the definition of [RFC8200], the DOH and HBH option extension headers are suitable for carrying information. If the DOH

is placed before the SRH, each endpoint node can read the content of the DOH; if it is placed after the SRH, only the destination node can read the content of the DOH.

If it is required that the forwarding nodes along the way can read the flow information, the information can only be carried through HBH. However, due to historical reasons, current mainstream network devices generally support HBH only limitedly. Although currently IETF has some discussions and related documents on HBH, such as [I-D.ietf-6man-hbh-processing], it is still difficult for routers to support HBH

In this realistic situation, it is hoped that the information along with the flow can be carried without increasing the length of the packet, and the intermediate router can realize the function relatively easily. IPv6 source address has become an unavoidable choice.

IPv6 addresses have a relatively large 128-bit space. SRv6 uses this feature to define segments with various behaviors, most of which can be used as IPv6 destination addresses. When the IPv6 destination address of a packet is a segment instantiated locally, the Endpoint processes the packet according to the definition of the segment. The transit node only uses the destination address for basic IPv6 forwarding. [I-D.ietf-6man-sids] also explains this situation.

This document discusses the need for IPv6 source address programmability. It is hoped that as the source address of the IPv6 header, it can be used to identify the source node of the tunnel encapsulation, and at the same time, it can also carry related information of the flow.

The intermediate nodes of the forwarding path, not limited to the endpoint, can obtain the necessary information from the source address, and guide the forwarding and processing of the flow together with the destination address

Address structures for programmable source addresses are outside the scope of this document

4. Scenarios of IPv6 source address programmability

This section lists some scenarios where flow information needs to be carried with the packet.

o Scenario of network slicing

Network slicing provides the ability to partition a physical network into multiple isolated logical networks of varying sizes, structures, and functions so that each slice can be dedicated to specific services or customers. [I-D.ietf-teas-ietf-network-slices] defines the term "IETF Network Slice" and establishes the general principles of network slicing in the IETF context.

Packets belong to a network slice need to be forwarded using the specific network resources. [I-D.ietf-teas-ietf-network-slices] defines the network resource mapped to the network slice as NRP, that is, the Network Resource Partition, and defines the nrp-id to identify the NRP used in the forwarding process.

In a network that provides slicing services, the NRP-ID can be carried in the packet. In the process of packet forwarding, the routers on the forwarding path can extract NRP-ID from the packet, determine the NRP to which the packet belongs, and then forward the packet using the resources associated with the NRP.

There are still various discussions on how to carry NRP-ID. For example, [I-D.ietf-6man-enhanced-vpn-vtn-id] defines options for carrying NRP-ID through IPv6 extension headers. [I-D.liu-spring-nrp-id-in-srv6-segment] proposes to carry the NRP-ID through the arg field of the segment. [I-D.cheng-spring-srv6-encoding-network-sliceid] proposed to carry NRP-ID through source address.

Therefore, for network slicing, carrying the NRP-ID through the source address is a direction that can be considered.

o Scenario of APN

[I-D.li-apn-problem-statement-usecases] analyzes the existing problems caused by lack of application awareness, and outlines various use cases that could benefit from Application-aware Networking (APN) architecture.

[I-D.li-apn-ipv6-encap] defines the option to carry the APN attribute in the IPv6 data plane, which can be applied to DOH, HBH option extension header, and TLV of SRH.

Of course, APN attributes can be very rich, but if the APN attribute can be abstracted into a digital APN ID, which can represent the application to which a flow belongs, the intermediate node of the forwarding path can apply related policies based on this APN ID. Then this APN-ID can also be carried by the source IPv6 address.

o Scenario of MVPN

The provider offer VPN service, and after the user traffic reaches the egress router, it needs to know which VPN the user traffic belongs to. How to identify which VPN the user traffic belongs to, unicast and multicast behave differently.

Still taking the IPv6 data plane as an example, SRv6 is used to provide unicast L3VPN services. When the user traffic reaches the egress router, its destination address is usually the segment of the End.DT4/End.DT6/End.DT46[RFC8986] type of the egress router. These segments are created on the egress router and associated with the local VPN. The egress router continues to forward the decapsulated user traffic within the VPN associated with the segment.

For multicast VPN, encapsulated user traffic is sent to multiple egress routers at the same time through multicast forwarding, so the segment of the egress router cannot be used like unicast VPN service.

Therefore, multicast VPN is also a potential scenario where IPv6 source addresses can be programmed.

5. IANA Considerations

This document has no IANA actions.

6. Security Considerations

TBD

7. References

7.1. Normative References

[I-D.ietf-6man-hbh-processing] Hinden, R. M. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", Work in Progress, Internet-Draft, draft-ietf-6man-hbh-processing-05, 23 February 2023.

[I-D.ietf-6man-sids] Krishnan. S, "Segment Identifiers in SRv6", Work in Progress, Internet-Draft, draft-ietf-6man-sids-02, 11 October 2022.

[I-D.ietf-teas-ietf-network-slices] Farrel, A., Gray, E., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "Framework for IETF Network Slices", draft-ietf-teas-ietf-network-slices-19 (work in progress), January 2023.

[I-D.li-apn-problem-statement-usecases] Li, Z., Peng, S., Voyer, D., Xie, C., Liu, P., Qin, Z., and Mishra, G., " Problem Statement and Use Cases of Application-aware Networking (APN) ", draft-li-apn-problem-statement-usecases-07 (work in progress), April 2023.

[I-D.li-apn-ipv6-encap] Li, Z., Peng, S., and Xie, C., " Application-aware IPv6 Networking (APN6) Encapsulation ", draft-li-apn-ipv6-encap-06 (work in progress), December 2022.

[I-D.ietf-6man-enhanced-vpn-vtn-id] Dong, J., Li, Z., Xie, C., Ma, C., and G. Mishra, "Carrying Virtual Transport Network (VTN) Identifier in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-ietf-6man-enhanced-vpn-vtn-id-02, April 2023.

[I-D.liu-spring-nrp-id-in-srv6-segment] Liu, Y., Lin, C., Li, H., and Gong, L., "NRP ID in SRv6 segment", draft-liu-spring-nrp-id-in-srv6-segment-01 (Work in Progress), April 2023.

[I-D.cheng-spring-srv6-encoding-network-sliceid] Cheng, W., Lin, C., Gong, L., Zadok, S., and X. Wang, "Encoding Network SliceIdentification for SRv6", Work in Progress, Internet-Draft, draft-cheng-spring-srv6-encoding-network-sliceid-05, April 2023.

[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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 0.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

Contributors

Authors' Addresses

Weiqiang Cheng
China Mobile
Beijing
China

Email: chengweiqiang@chinamobile.com

Liyan Gong
China Mobile
Beijing
China
Email: gongliyan@chinamobile.com

Changwang Lin
New H3C Technologies
Beijing
China

Email: linchangwang.04414@h3c.com

Hao Li
New H3C Technologies
Beijing
China

Email: lihao@h3c.com