Network Working Group J. Dong
Internet-Draft Z. Li
Intended status: Standards Track Huawei Technologies
Expires: January 14, 2021 C. Xie
C. Ma
China Telecom
July 13, 2020

Carrying Virtual Transport Network Identifier in IPv6 Extension Header
draft-dong-6man-enhanced-vpn-vtn-id-01

Abstract

This document proposes a new option type to carry virtual transport network identifier (VTN ID) in the IPv6 extensions headers to identify the Virtual Transport Network (VTN) the packet belongs to. The procedure of processing the VTN option is also specified. This provides a scalable solution for data plane encapsulation of enhanced VPN (VPN+) as described in I-D.ietf-teas-enhanced-vpn. One typical use case of VPN+ is to provide transport network slicing in 5G, while it could also be used in more general cases.

Table of Contents

1. Introduction

Virtual private networks (VPNs) have served the industry well as a means of providing different groups of users with logically isolated connectivity over a common network. Some customers may request a connectivity services with advanced characteristics such as complete isolation from other services or guaranteed performance. These services are "enhanced VPNs" (known as VPN+). [I-D.ietf-teas-enhanced-vpn] describes the framework and candidate component technologies for providing enhanced VPN services. One typical use case of VPN+ is to provide transport network slicing in 5G, while it could also be used in more general cases.

The enhanced properties of VPN+ require tighter coordination and integration between the underlay network resources and the overlay network. VPN+ service is built on a Virtual Transport Network (VTN) which has a customized network topology and a set of dedicated or shared network resources allocated from the underlay network. The overlay VPN together with the corresponding VTN in the underlay provide the VPN+ service. In the network, traffic of different VPN+ services need to be processed separately based on the topology and the network resources associated with the corresponding VTN.

[I-D.dong-teas-enhanced-vpn-vtn-scalability] describes the scalability considerations of enhanced VPN, in which one approach to improve the data plane scalability is to introduce a dedicated identifier indata packet to identify the VTN the packet belongs to, so as to perform resource specific packet processing. This is called Resource Independent (RI) VTN.

This document proposes a mechanism to carry the VTN Identifier (VTN ID) in the IPv6 extensions headers [RFC8200] of packet, so that the packet will be processed by network nodes using the network resources allocated to the corresponding VTN. The procedure of processing the VTN ID is also specified. This provides a scalable solution for enhanced VPN data plane, so that it could be used to support a large number of transport network slices in IPv6 network.

2. 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 BCP14 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. New IPv6 Extension Header Option for VTN

A new option type of IPv6 extension headers is defined to carry the Virtual Transport Network Identifier (VTN ID) in IPv6 packet header. Its format is shown as below:

```
           Option   Option       Option
            Type   Data Len       Data
         +--------+--------+--------+--------+
         |BBCTTTTT|00000100|  4-octet VTN ID |
         +--------+--------+--------+--------+
```

Option Type: 8-bit identifier of the type of option. The type of VTN option is TBD by IANA. The highest-order bits of the type field are defined as below:

- o BB 00 The highest-order 2 bits are set to 00 to indicate that a node which does not recognize this type will skip over it and continue processing the header.

- o C 0 The third highest-order bit are set to 0 to indicate this option does not change en route.

Opt Data Len: 8-bit unsigned integer indicates the length of the option Data field of this option, in octets. The value of Opt Data Len of VTN option SHOULD be set to 4.

Option Data: 4-octet VTN which uniquely identifies a virtual transport network.

Editor's note: The length of the VTN ID is defined as 4-octet partially for the matching with the 4-octet network slice identifier defined in 3GPP [TS23501].

```
                  8-bit              24-bit
             +------------+-----------------------+
             |    SST     |   Slice Differentiator  |
             +------------+-----------------------+
```

4. Procedures

4.1. VTN Option Insertion

When an ingress node of an IPv6 or SRv6 domain receives a packet, according to traffic classification or mapping policy, the packet SHOULD be encapsulated in an outer IP header, and the VTN-ID of the virtual transport network which the traffic is mapped to SHOULD be carried in the extension header associated with the outer IPv6 header . The ingress node MAY also encapsulate the SRH as defined in [RFC8754] in the Routing Header of the outer IPv6 header.

In order to make the VTN option be processed by each node along the path, it is RECOMMENDED that the VTN option be carried in IPv6 extension headers which can be processed hop-by-hop in forwarding plane. It can be carried in either the Hop-by-Hop Options header, or some new extension headers which can be processed on each hop along the path.

4.2. VTN based Packet Forwarding

On receipt of a packet with the VTN option, each network node which can parse the VTN option SHOULD use the VTN ID to identify the virtual network the packet belongs to. This means the forwarding behavior is based on both the destination IP address and the VTN option.The destination IP address is used for the lookup of the next-hop node, and VTN-ID can be used to determine the set of network resources reserved for processing and sending the packet to the next-hop node. The domain egress node SHOULD decapsulate the outer IPv6 header.

There can be different implementations of reserving local network resources to the VTNs. On each interface, the resources allocated to a particular VTN can be seen as a virtual sub-interface with dedicated bandwidth and other associated resources. In packet forwarding, the IPv6 destination address of the received packet is used to identify the next-hop and the outgoing interface, and the VTN ID is used to further identify the virtual sub-interface which is associated with the VTN on the outgoing interface.

Routers which do not support Hop-by-Hop options header SHOULD ignore the Hop-by-Hop options header and forward the packet merely based on the destination IP address. Routers which support Hop-by-Hop Options, but do not recognize the VTN option SHOULD ignore the option and continue to forward the packet merely based on the destination IP address.

5. Operational Considerations

As described in [RFC8200], nodes may be configured to ignore the Hop-by-Hop Options header, and the packets containing a Hop-by-Hop Options header may be dropped or assigned to a slow processing path. When VTN option is carried in Hop-by-Hop option header, operator needs to make sure that all the network nodes involved in the VTN can either process the Hop-by-Hop Options header in packet forwarding, or ignore the Hop-by-Hop Option header but continue to forward the packet based on other fields and headers. In other words, Packet mapping to a VTN MUST NOT be dropped due to the existence of the Hop-by-Hop Options header. It is RECOMMENDED to configure the nodes to process the Hop-by-Hop Option header if there is a nob for this.

6. IANA Considerations

This document requests IANA to assign a new option type from "Destination Options and Hop-by-Hop Options" registry.

Value	Description	Reference
TBD	Virtual Transport Network Identifier	this document

7. Security Considerations

TBD

8. Contributors

Zhibo Hu
Email: huzhibo@huawei.com

Lei Bao
Email: baolei7@huawei.com

9. Acknowledgements

The authors would like to thank Juhua Xu for his review and valuable comments.

10. References

10.1. Normative References

[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>.

10.2. Informative References

[I-D.dong-teas-enhanced-vpn-vtn-scalability]
Dong, J., Li, Z., and F. Qin, "Virtual Transport Network (VTN) Scalability Considerations for Enhanced VPN", draft-dong-teas-enhanced-vpn-vtn-scalability-00 (work in progress), February 2020.

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Services", draft-ietf-teas-enhanced-vpn-05 (work in progress), February 2020.

[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>.

[TS23501] "3GPP TS23.501", 2016, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.

Authors' Addresses

Jie Dong
Huawei Technologies
Huawei Campus, No. 156 Beiqing Road
Beijing 100095
China

Email: jie.dong@huawei.com

Zhenbin Li
Huawei Technologies
Huawei Campus, No. 156 Beiqing Road
Beijing 100095
China

Email: lizhenbin@huawei.com

Chongfeng Xie
China Telecom
China Telecom Beijing Information Science & Technology, Beiqijia
Beijing 102209
China

Email: xiechf@chinatelecom.cn

Chenhao Ma
China Telecom
China Telecom Beijing Information Science & Technology, Beiqijia
Beijing 102209
China

Email: machh@chinatelecom.cn