

6MAN working group
Internet-Draft
Intended status: Standard Track
Expires: August 2020

J. Dong
Z. Li
Huawei
February 10, 2020

Carrying Virtual Transport Network (VTN) Identifier in IPv6 Extension Header for Enhanced VPN

[draft-dong-6man-enhanced-vpn-vtn-id-00](#)

Abstract

This document proposes a new option type to carry virtual transport network identifier (VTN ID) in the IPv6 extension headers to identify the virtual transport network 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 10, 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Requirements Language	3
3. New IPv6 Extension Header Option for VTN	3
4. Procedures	4
4.1. VTN Option Insertion	4
4.2. VTN based Packet Forwarding	5
5. Security Considerations	5
IANA Considerations	5
Contributors	6
Acknowledgments	6
References	6
Normative References	6
Informative References	6
Authors' Addresses	7

[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 in data 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 [RFC2119] [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 Type	Option Data Len	Option Data
+-----+	+-----+	+-----+
BBCTTTT	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:

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.

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](#)].



4. Procedures

4.1. VTN Option Insertion

The VTN option is inserted at the edge of the IPv6 network which provides enhanced VPN service. On receipt of a data packet, the ingress node determines the associated enhanced VPN based on traffic classification or local policies, then it SHOULD insert the corresponding VTN ID option into the IPv6 extension header of the packet. If SRv6 is enabled, the VTN option SHOULD be included in the outer IPv6 header which MAY optionally include the SRH [I-D.ietf-6man-segment-routing-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 the Hop-by-Hop option header of the IPv6 packet.

4.2. VTN based Packet Forwarding

On receipt of a packet with the VTN option, each network node which can support the VTN option SHOULD use the VTN ID to identify the virtual network the packet belongs to, and the set of local network resources allocated the processing of the packet. This means the forwarding behavior is based on both the destination IP address and the VTN option.

There can be different implementations of allocating local network resources to the VTNs. On each interface, the resources allocated to a particular VTN can be considered as a virtual sub-interface with dedicated bandwidth. 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 SHOULD ignore this option and SHOULD forward the packet. 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. Security Considerations

TBD

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

Contributors

Zhibo Hu
Email: huzhibo@huawei.com

Juhua Xu
Email: xujuhua@huawei.com

Acknowledgments

The authors would like to thank XXX for the review and valuable comments.

References

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>>.

Informative References

- 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+) Service", [draft-ietf-teas-enhanced-vpn-04](#) (work in progress), January 2020.
- [I-D.dong-teas-enhanced-vpn-vtn-scalability] Dong, J., Li, Z., Qin, F., "Scalability Considerations of Enhanced VPN", [draft-dong-teas-enhanced-vpn-vtn-scalability-00](#) (work in progress), February 2020.

[I-D.ietf-6man-segment-routing-header] Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", [draft-ietf-6man-segment-routing-header-26](#) (work in progress), October 2019.

[I-D.ietf-spring-srv6-network-programming] Filsfils, C., Camarillo, P., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "SRv6 Network Programming", [draft-ietf-spring-srv6-network-programming-07](#) (work in progress), December 2019.

[TS23501] "3GPP TS23.501", 2019, <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>>.

Authors' Addresses

Jie Dong
Huawei

Email: jie.dong@huawei.com

Zhenbin Li
Huawei

Email: lizhenbin@huawei.com