Network Working Group J. Dong
Internet-Draft Z. Li
Intended status: Standards Track Huawei Technologies
Expires: 18 November 2023 C. Xie
C. Ma
China Telecom
G. Mishra
Verizon Inc.
17 May 2023

Carrying Virtual Transport Network (VTN) Information in IPv6 Extension Headers

draft-ietf-6man-enhanced-vpn-vtn-id-04

Abstract

Virtual Private Networks (VPNs) provide different customers with logically separated connectivity over a common network ~~infrastructure~~. ~~With the introduction and evolvement of 5G~~In some contexts and other network scenarios, some ~~existing or new~~ customers may require connectivity services with advanced ~~characteristics~~ features comparing to ~~traditional~~ conventional VPN services. Such kind of network service is called enhanced VPNs (VPN+). VPN+ can be used, for example, ~~-~~to deliver IETF network slice services~~, and could also be used for other application scenarios~~.

A Virtual Transport Network (VTN) is a virtual underlay network which consists of a set of dedicated or shared network resources allocated from the physical underlay network, and is associated with a customized logical network topology. VPN+ services can be delivered by mapping one or a group of overlay VPNs to the appropriate VTNs as the virtual underlay. For forwarding along a specific VTN, ~~In packet forwarding, s~~some packet fields ~~in the data packet needs to be~~are ~~-~~used to identify the VTN ~~the~~ a packet belongs to~~,~~. In doing so, ~~that~~ VTN-specific processing ~~can be~~is performed ~~on each node the packet traverses~~along a VTN-specific path.

This document ~~proposes~~ specifies a new Hop-by-Hop option ~~of IPv6 extension header~~ to carry the VTN related information in data packets, which could used to identify the VTN specific processing to be performed on the packets. ~~The procedure of processing the VTN option is also specified.~~

Status of This Memo

Commenté [BMI1]: I would generalize as many "conventional" customers already require some strict commitment.

Commenté [BMI2]: Not sure this adds much.

Commenté [BMI3]: Which one?

Commenté [BMI4]: To be consistent with the teas framework.

Commenté [BMI5]: Why not echoing what is in the VPN+ spec: "A VTN is a virtual underlay network that is associated with a network topology, and is allocated with a set of dedicated or shared resources from the underlay physical network.
"

Commenté [BMI6]: As per RFC8200, the draft should elaborate further on the following:

"There has to be a very clear justification why any new hop-by-hop option is needed before it is standardized."

This Internet-Draft will expire on 18 November 2023.

Copyright Notice

Table of Contents

1. Introduction

Virtual Private Networks (VPNs) provide different customers with logically isolated connectivity over a common network ~~infrastructure~~. With the introduction and evolvement of 5G and other network scenarios, some existing or new customers may require connectivity services with advanced characteristics comparing to traditional VPNs, such as resource isolation from other services or guaranteed performance. Such kind of network service is called enhanced VPN (VPN+). VPN+ service requires the coordination and integration between the overlay VPNs and the capability and resources of the underlay network. VPN+ can be used, e.g., to deliver IETF network slices [I-D.ietf-teas-ietf-network-slices].

Commenté [BMI7]: You may cite Section 3.10 of RFC4026.

Commenté [BMI8]: Same comments as in the abstract.

[I-D.ietf-teas-enhanced-vpn] describes a framework and the candidate component technologies for providing VPN+ services. It also introduces the concept of Virtual Transport Network (VTN). A VTN is a virtual underlay network which consists of a set of dedicated or shared network resources allocated from the physical underlay network, and is associated with a logical network topology. VPN+ services can be delivered by mapping one or a group of overlay VPNs to the appropriate VTNs as the underlay, so as to provide the network characteristics required by the customers. In packet forwarding, traffic of different VPN+ services needs to be processed separately based on the network resources and the logical topology associated with the corresponding VTN. In the context of network slicing, ~~VTN and~~ Network Resource Partition (NRP) ~~are considered as similar concepts, and NRP~~ can be seen as an instantiation of VTN.

[I-D.ietf-teas-nrp-scalability] describes the scalability considerations and the possible optimizations for providing a relatively large number of VTNs for VPN+ services. One approach to improve the data plane scalability of VTN is to introduce a dedicated VTN Resource Identifier (VTN Resource ID) in the data packet to identify the set of network resources allocated to a VTN, so that VTN-specific ~~packet processing can be performed using that set of~~ Resources are invoked along packets that are forwarded over a VTN, which avoids the possible resource competition with services in other VTNs. This is called Resource Independent (RI) VTN. A VTN Resource ID represents a subset of the resources (e.g., bandwidth, buffer and queuing resources) allocated on a given set of links and nodes which constitute a logical network topology. The logical topology ~~associated~~ of ~~with~~ a VTN could be defined using mechanisms such as Multi-Topology [RFC4915], [RFC5120], or Flex-Algo [RFC9350]~~, etc~~.

This document ~~proposes~~ specifies a mechanism to carry the VTN related information in a new Hop-by-Hop option (Section 4.3 of [RFC8200], called "VTN option". ~~of IPv6 extension header [RFC8200] of IPv6 packet,~~ This option ~~so that on each network node along the packet forwarding path, the VTN option in the packet~~ is parsed by intermediate nodes, and the obtained VTN Resource ID is used to ~~instruct the network node to use the set of network resources allocated to the corresponding VTN to process and forward the packet~~invoked VTN-specific resources along the forwarding path. ~~The procedure for processing the VTN option is also specified.~~ This provides a scalable solution to support a relatively large number of VTNs in an IPv6 network.

Although the application of the VTN option ~~in this document~~ is to carry the resource ID information, the VTN option is considered as a generic mechanism to convey network wide VTN identifiers with different semantics to meet the possible use cases in the future.

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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all

Commenté [BMI9]: It would be good to align with the wording used in the VPN+ spec

Commenté [BMI10]: You may cite [I-D.ietf-teas-ietf-network-slices].

Commenté [BMI11]: I'm not convinced we need two concepts to basically refer to the same thing. I'm not insisting in this is what we have currently in the VPN+.

Commenté [BMI12]: Not sure this is a generic characteristic of VTN. Some resources may be shared without strict resource reservation.

Commenté [BMI13]: This refers to what?

Commenté [BMI14]: I don't find a discussion about this in draft-ietf-teas-enhanced-vpn.

Commenté [BMI15]: Not used in the doc.

Commenté [BMI16]: The option uses "VTN ID". You may first introduce that ID.

Commenté [BMI17]: Isn't this what NRP refers to?

Commenté [BMI18]: Does this assume that « VTN Resource ID" is used by these protocols to maintain/compute the specific topologies, or this ID is used only by ingress nodes to bind a packet to a topology?

Commenté [BMI19]: Not sure what is scalable here. Really.

Commenté [BMI20]: I'm afraid this is too short to help assessing what is claimed here.

capitals, as shown here.

2. New IPv6 Extension Header Option for VTN

A new Hop-by-Hop option type "VTN" is defined to carry the VTN related information~~ in an IPv6 packet~~. Its format is shown ~~as below~~in Figure 1~~:~~.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |  Option Type  |  Opt Data Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Flags     | Context Type  |            Reserved           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                            VTN ID                             ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1. The format of VTN Option

Option Type: 8-bit identifier of the type of option. The type of VTN option is to be assigned by IANA. The 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 is set to 0 to indicate this option does not change en route.

* TTTTT To be assigned by IANA.

Opt Data Len: 8-bit unsigned integer indicates the length of the option Data field of this option, in octets.

Flags: 8-bit flags field. The most significant bit is defined in this document.

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|S|U U U U U U U|
+-+-+-+-+-+-+-+-+
```

* S (Strict Match): The S flag is used to indicate whether the VTN ID MUST be strictly matched for the processing of the packet. When S flag is set to 1, if the VTN ID in the VTN option does not match with any of the VTN ID provisioned on the network node, the packet MUST be dropped. When S flag is set to 0, if the VTN ID does not match with any of the VTN ID provisioned on the network node, the packet SHOULD be forwarded using the default behavior as if the VTN option does not exist.

* U (Unused): These flags are reserved for future use. They ~~SHOULD~~MUST be set to 0 on transmission and MUST be ignored on receipt.

Context Type (CT): One-octet field used to indicate the semantics and

Commenté [BMI21]: Add a pointer to rfc8200#section-4.2

Commenté [BMI22]: Do you allow VTN ID to change along the path when reclassification happens, for example?

Commenté [BMI23]: You may consider moving the structure to the IANA consideration section.

Commenté [BMI24]: So, dropping the packet would be acceptable in this case?

Commenté [BMI25]: Why noy managing this via control plane and instruct the nodes about the expected behavior?

length of the VTN ID carried in the option. The context value defined in this document is as follows:

* CT=0: The VTN ID is a 4-octet resource ID, which is used to identify a subset of network resources on the network nodes and links involved in the VTN.

Reserved: 2-octet field reserved for future use. They ~~SHOULD~~ MUST be set to 0 on transmission and MUST be ignored on receipt.

VTN ID: The identifier of a Virtual Transport Network, the semantics and length of the ID is determined by the Context Type.

Note that, if a deployment found it useful, the four-octet VTN ID field may be derived from the four-octet Single Network Slice Selection Assistance Information (S-NSSAI) defined in 3GPP [TS23501].

3. Procedures

~~As the VTN option needs to be processed by each node along the forwarding path, it MUST be carried in IPv6 Hop-by-Hop Options header.~~ This section describes the procedures for VTN option processing when the Context Type in the VTN option is set to 0. The processing procedures for VTN option with other Context Types are out of the scope of this document and will be specified in separate documents which introduce those Context Types.

3.1. Adding VTN Options to Packets

When an ingress node of an IPv6 domain receives a packet, according to the traffic classification and mapping policy, the packet is steered into one of the VTNs in the network, then the packet MUST be encapsulated in an outer IPv6 header, and the Resource ID of the VTN which the packet is mapped to MUST be carried in the VTN option of the Hop-by-Hop Options header, which is associated with the outer IPv6 header.

3.2. VTN based Packet Forwarding

On receipt of a packet with the VTN option, each network node which can process the VTN option in fast path MUST use the VTN Resource ID to determine the set of local network resources which are allocated to the VTN. The packet forwarding behavior is based on both the destination IP address and the VTN Resource ID. More specifically, the destination IP address is used to determine the next-hop and the outgoing interface, and VTN Resource ID is used to determine the set of network resources on the outgoing interface which are allocated to the VTN for processing and sending the packet. If the VTN Resource ID does not match with any of the VTN Resource ID provisioned on the outgoing interface, the S flag in the VTN option is used to determine whether the packet is dropped or forwarded using the default set of network resources of the outgoing interface. The Traffic Class field of the outer IPv6 header can be used to provide differentiated treatment for packets which belong to the same VTN. The egress node of the IPv6 domain MUST decapsulate the outer IPv6 header and the Hop-by-Hop Options header which includes the VTN option.

Commenté [BMI26]: Why this can be inferred from the 'Opt Data Len" field?

Commenté [BMI27]: Why do you need to impose the length?

Commenté [BMI28]: I interpret this as the resource ID refers to a subset of VTN resources. How the identification of the VTN is made then? Is it part of the resource ID structure?

Commenté [BMI29]: As you already have a set of unused flags, do you need to have this field?

Commenté [BMI30]: With CT=0, what is then the subtlety between VTN resource ID vs VTN ID?

Can you provide a concrete example of a resource ID?

Commenté [BMI31]: Why specifically call this case?

Commenté [BMI32]: Only if a match is found!

a mis en forme : Surlignage

Commenté [BMI33]: What address is used as destination @?

Commenté [BMI34]: You should first describe how this is made available to the node.

Commenté [BMI35]: Should be defined.

Commenté [BMI36]: Please note the following from RFC8200:

```
   NOTE: While [RFC2460] required that
all nodes must examine and
   process the Hop-by-Hop Options header,
it is now expected that nodes
   along a packet's delivery path only
examine and process the
   Hop-by-Hop Options header if
explicitly configured to do so.
```

Commenté [BMI37]: So, you exclude that this is used with other steering headers.

Commenté [BMI38]: The outgoing interface may depend on the logical topology that is used for a VTN!

a mis en forme : Surlignage

In the forwarding plane, there can be different approaches of partitioning the local network resources and allocating them to different VTNs. For example, on one physical interface, a subset of the forwarding plane resources (e.g. bandwidth and the associated buffer and queuing resources) can be allocated to a particular VTN and represented as a virtual sub-interface or a data channel with reserved bandwidth resource. In packet forwarding, the IPv6 destination address of the received packet is used to identify the next-hop and the outgoing layer-3 interface, and the VTN Resource ID is used to further identify the virtual sub-interface or the data channel on the outgoing interface which is associated with the VTN.

Network nodes which do not support the processing of Hop-by-Hop Options header SHOULD ignore the Hop-by-Hop options header and forward the packet only based on the destination IP address. Network nodes which support Hop-by-Hop Options header, but do not support the VTN option SHOULD ignore the VTN option and forward the packet only based on the destination IP address. The network node MAY process the rest of the Hop-by-Hop options in the Hop-by-Hop Options header.

4. Operational Considerations

As described in [RFC8200], network nodes may be configured to ignore the Hop-by-Hop Options header, drop packets containing a Hop-by-Hop Options header, or assign packets containing a Hop-by-Hop Options header to a slow processing path. In networks with such network nodes, it is important that packets of a VTN are not dropped due to the existence of the Hop-by-Hop Options header. Operators need to make sure that all the network nodes involved in a VTN can either process the Hop-by-Hop Options header in the fast path, or ignore the Hop-by-Hop Options header. Since a VTN is associated with a logical network topology, one practical approach is to ensure that all the network nodes involved in that logical topology support the processing of the Hop-by-Hop Options header and the VTN option in the fast path, and constrain the packet forwarding path to the logical topology of the VTN.

[I-D.ietf-6man-hbh-processing] specifies the modified procedures for the processing of IPv6 Hop-by-Hop Options header, with the purpose of making the Hop-by-Hop Options header useful. Network nodes complying with [I-D.ietf-6man-hbh-processing] will not drop packets with Hop-by-Hop Options header and the VTN option.

5. Considerations about Generalization

During the discussion of this document in the 6MAN WG, one of the suggestions received is to make the VTN option more generic in terms of semantics and encoding. This section gives some analysis about to what extent the semantics of VTN could be generalized, and how the generalization could be achieved with the proposed encoding.

Based on the VTN definition in [I-D.ietf-teas-enhanced-vpn], the concept of VTN could be extended as: a virtual transport network which is associated with a set of network-wide attributes and states maintained on each participating network node. The attributes associated with an VTN may include but not limited to: network resource attributes, network topology attributes, and network function attributes etc.

* The network resource can refer to various type of data plane resources, including link bandwidth, bufferage and queueing resources.

* The network topology can be multipoint-to-multipoint, point-to-point, point-to-multipoint or multipoint-to-point.

* The network functions may include both data forwarding actions and other types network functions which can be executed on data packets mapped to a VTN.

This shows the semantics of VTN can be quite generic. Although generalization is something good to have, it would be important to understand and identify the boundary of generalization. In this document, It is anticipated that for one network attribute to be included in VTN, it needs to be a network-wide attribute rather than a node-specific attribute. Thus whether a network-wide view can be provided or not could be considered as one prerequisite of making one attribute part of the VTN option.

The format of the VTN option contains the Flags field, the Context Type field and the Reserved field, which provide the capability for future extensions. That said, since the VTN option needs to be processed by network nodes in the fast path, the capability of network devices need to be considered when new semantics and encoding are introduced.

6. IANA Considerations

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

Commenté [BMI39]: Add a pointer to https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2 + follow the structure provided there.

Value	Description	Reference
TBA	VTN Option	this document

This document requests IANA to create a new registry for the "VTN Option Context Type" under the "Internet Protocol Version 6 (IPv6) Parameters" registry. The allocation policy of this registry is "Standards Action". The initial codepoints are assigned by this document as follows:

Value	Description	Reference
0	Resource ID	this document
1-254	Unassigned	
255	Reserved	

7. Security Considerations

The security considerations with IPv6 Hop-by-Hop Options header are described in [RFC8200], [RFC7045], [RFC9098] [RFC9099] and [I-D.ietf-6man-hbh-processing]. This document introduces a new IPv6 Hop-by-Hop option which is either processed in the fast path or ignored by network nodes, thus it does not introduce additional security issues.

8. Contributors

Zhibo Hu
Email: huzhibo@huawei.com

Lei Bao
Email: baolei7@huawei.com

9. Acknowledgements

The authors would like to thank Juhua Xu, James Guichard, Joel Halpern, Tom Petch, Aijun Wang, Zhenqiang Li, Tom Herbert, Adrian Farrel, Eric Vyncke and Erik Kline for their review and valuable comments.

10. References

10.1. Normative References

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Network (VPN+)", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-12, 23 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-enhanced-vpn-12>.

[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.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-08, 30 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-hbh-processing-08>.

[I-D.ietf-teas-ietf-network-slices]
Farrel, A., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "A Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-19, 21 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-19>.

[I-D.ietf-teas-nrp-scalability]

Dong, J., Li, Z., Gong, L., Yang, G., Guichard, J., Mishra, G. S., Qin, F., Saad, T., and V. P. Beeram, "Scalability Considerations for Network Resource Partition", Work in Progress, Internet-Draft, draft-ietf-teas-nrp-scalability-01, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-nrp-scalability-01>.

[RFC4915] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, DOI 10.17487/RFC4915, June 2007, <https://www.rfc-editor.org/info/rfc4915>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <https://www.rfc-editor.org/info/rfc7045>.

[RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <https://www.rfc-editor.org/info/rfc9098>.

[RFC9099] Vyncke, É., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <https://www.rfc-editor.org/info/rfc9099>.

[RFC9350] Psenak, P., Ed., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", RFC 9350, DOI 10.17487/RFC9350, February 2023, <https://www.rfc-editor.org/info/rfc9350>.

[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

Gyan Mishra
Verizon Inc.
Email: gyan.s.mishra@verizon.com