

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 8 September 2022

Z. Li  
J. Dong  
Huawei Technologies  
R. Pang  
China Unicom  
Y. Zhu  
China Telecom  
7 March 2022

Framework for End-to-End IETF Network Slicing  
draft-li-teas-e2e-ietf-network-slicing-02

## Abstract

Network slicing can be used to meet the connectivity and performance requirement of different services or customers in a shared network. An IETF network slice may be used for 5G or other network scenarios. In the context of 5G, the 5G end-to-end network slices consist of three major types of network technology domains: Radio Access Network (RAN), Transport Network (TN) and Core Network (CN). The transport network slice can be realized as IETF network slices. In the transport network, the IETF network slice may span multiple network administrative domains.

In order to facilitate the mapping between network slices in different network technology domains and administrative domains, it is beneficial to carry the identifiers related to the 5G end-to-end network slice, the multi-domain IETF network slice together with the intra-domain network slice related identifier in the data packet.

This document describes the framework of end-to-end IETF network slicing, and introduces the identifiers related to 5G end-to-end network slice and the multi-domain IETF network slice. These identifiers can be carried in the data packet. The roles of the different identifiers in packet forwarding is also described. The network slice identifiers may be instantiated with different data planes.

## 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](#)].

Internet-Draft

E2E IETF Network Slicing

March 2022

## 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 8 September 2022.

## Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Framework . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Requirements on E2E IETF Network Slicing . . . . .	<a href="#">5</a>
<a href="#">3.1.</a>	Data Plane . . . . .	<a href="#">6</a>
<a href="#">3.2.</a>	Management Plane/Control Plane . . . . .	<a href="#">6</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Acknowledgements . . . . .	<a href="#">6</a>
<a href="#">7.</a>	References . . . . .	<a href="#">7</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">7</a>

<a href="#">7.2.</a> Informative References . . . . .	<a href="#">7</a>
Authors' Addresses . . . . .	<a href="#">7</a>

## [1.](#) Introduction

[I-D.ietf-teas-ietf-network-slices] defines the terminologies and the characteristics of IETF network slices. It also discusses the general framework, the components and interfaces for requesting and operating IETF network slices. A Network Resource Partition (NRP) is a collection of network resources in the underlay network that are available to carry traffic and meet the SLOs and SLEs.

[I-D.ietf-teas-enhanced-vpn] describes the framework and the candidate component technologies for providing enhanced VPN (VPN+) services based on existing VPN and Traffic Engineering (TE) technologies with enhanced characteristics that specific services require above traditional VPNs. It also introduces the concept of Virtual Transport Network (VTN), which is a virtual underlay network consisting of a set of dedicated or shared network resources allocated from the physical underlay network, and is associated with a customized 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. Enhanced VPN (VPN+) and VTN can be used for the realization of IETF network slices. In the context of IETF network slicing, NRP can be seen as an instantiation of VTN.

[I-D.dong-teas-nrp-scalability] describes the scalability considerations in the control plane and data plane of NRP, and proposed several suggestions to improve the scalability. In the control plane, It proposes the approach of decoupling the topology and resource attributes of NRP, so that multiple NRPs may share the same topology attributes and the result of topology based path computation. In the data plane, it proposes to carry a global NRP-ID of a network domain in the data packet to determine the set of resources reserved for the corresponding NRP.

An IETF network slice may span multiple network administrative domains. Further in the context of 5G, there are end-to-end network

slices which consists of three major types of network technology domains: Radio Access Network (RAN), Transport Network (TN) and Core Network (CN). In order to facilitate the mapping between network slices in different network technology domains and administrative domains, it may be beneficial to carry the identifiers related to the 5G end-to-end network slice, the identifiers of the multi-domain IETF network slices together with the intra-domain network slices related identifiers in the data packet.

This document describes the typical scenarios of end-to-end network slicing, and the framework of concatenating network slices in different network technology domains and administrative domains.

Multiple network slice related identifiers are defined for network slices with different network scopes. These network slice related identifiers can be instantiated using different data planes, such as IPv6 and MPLS.

## 2. Framework

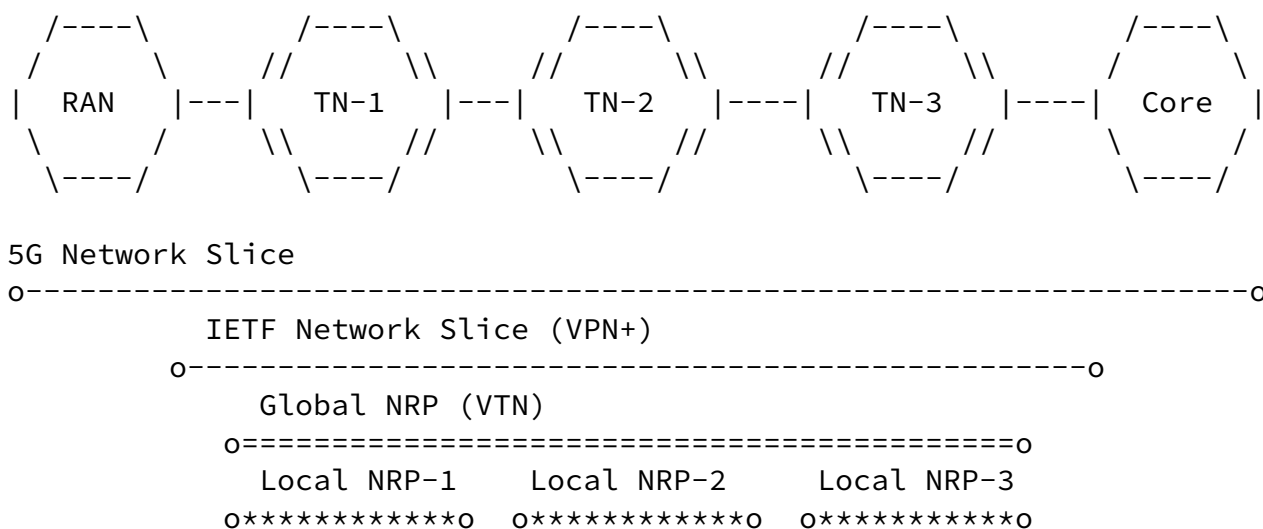


Figure 1. 5G end-to-end network slicing scenario

One typical scenario of 5G end-to-end network slicing is shown in figure 1. The 5G end-to-end network slice is identified by the S-NSSAI (Single Network Slice Selection Assistance Information). In

the transport network, the 5G network slice is mapped to an IETF network slice. In a multi-domain transport network, an IETF network slice can be realized with a multi-domain VPN+ service. In the underlay network, the multi-domain VPN+ service can be supported by a multi-domain VTN, which is the concatenation of multiple intra-domain NRPs in different domains. In each domain, a domain-significant NRP-ID can be carried in the packet to identify the set of network resource reserved for the NRP in the corresponding domain. Note this is similar to the Option C mode of inter-domain VPN service [[RFC4364](#)]. Using Option A or Option B mode of inter-domain VPN for 5G end-to-end network slicing is also possible, which is out of the scope of the current version of this document.

In order to concatenate multiple domain-wide NRPs into a multi-domain NRP, the global NRP-ID can be carried in the packet, which is used by the domain border nodes to map to the local NRP-IDs in each domain. And in order to facilitate the network slice mapping between RAN, Core network and transport network, the S-NSSAI may be carried in the packet sent to the transport network, which can be used by the transport network to map the 5G end-to-end network slice to the corresponding IETF network slice.

According to the above end-to-end network slicing scenario, there can be three network slice related identifiers in the data packet:

- \* Domain NRP-ID: This is the NRP-ID as defined in [[I-D.dong-teas-nrp-scalability](#)]. It is used by the network nodes in a network domain to determine the set of local network resources reserved for an NRP. It SHOULD be processed by each hop along the path in the domain.
- \* End-to-end NRP-ID: This is the identifier which uniquely identifies a multi-domain NRP. In each network domain, the domain border nodes map the global NRP-ID to the domain NRP-ID for packet forwarding.

- \* 5G end-to-end network slice ID (S-NSSAI): This is the identifier of the 5G end-to-end network slice. When required, it may be used by the network nodes to provide traffic monitoring at the end-to-end network slice granularity.

For the above network slice identifiers, the domain NRP-ID is mandatory, the global NRP-ID and the 5G S-NSSAI are optional. The existence of the Global NRP-ID depends on whether the NRP spans multiple network domains in the transport network, and how the domain NRP-IDs are managed. In some network scenarios, different network domains can have consistent NRP ID allocation, then the domain NRP-ID can have the same value as a global NRP-ID. The existence of the 5G S-NSSAI depends on whether an IETF network slice is used as part of the 5G end-to-end network slice.

### [3.](#) Requirements on E2E IETF Network Slicing

This section lists the requirements on E2E IETF network slicing.

#### [3.1.](#) Data Plane

To facilitate the mapping between 5G end-to-end network slice and IETF network slice, and the mapping between multi-domain IETF network slice and the intra-domain IETF network slice, different network slice related identifiers, including the S-NSSAI, the Global NRP-ID, domain NRP-ID need to be carried in the data packet.

In a multi-domain IETF network slice, the domain border nodes should support to map the Global NRP-ID to the domain NRP-ID of the local domain. In a 5G end-to-end network slicing scenario, the edge nodes of IETF network slice should support to map the S-NSSAI to the global NRP-ID and the domain NRP-ID. When the correlation between S-NSSAI and the NRP-ID needs to be maintained, the edge nodes of IETF network slices should be able to derive the S-NSSAI from the data packet

received from RAN and CN, and encapsulate both the S-NSSAI and the NRP-ID into an outer packet header when traversing the transport network domains.

### [3.2.](#) Management Plane/Control Plane

For multi-domain IETF network slice, a centralized IETF network slice controller is responsible for the allocation of the Global NRP-ID and the domain NRP-IDs, and the provisioning of the mapping relationship between the Global NRP-ID and the domain NRP-IDs to the border nodes in different network domains.

For 5G end-to-end network slice, when S-NSSAI is used for the mapping from RAN or CN network slices to IETF network slices, the IETF network slice controller is responsible for the provisioning of the mapping relationship between S-NSSAI and the Global and local NRP-IDs at the edge nodes of IETF network slices.

## [4.](#) IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

## [5.](#) Security Considerations

TBD

## [6.](#) Acknowledgements

TBD

## [7.](#) References

### [7.1.](#) 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+) Services", Work in Progress, Internet-Draft, [draft-ietf-](#)

[teas-enhanced-vpn-09](https://www.ietf.org/archive/id/draft-ietf-teas-enhanced-vpn-09), 25 October 2021,  
<<https://www.ietf.org/archive/id/draft-ietf-teas-enhanced-vpn-09.txt>>.

[I-D.ietf-teas-ietf-network-slices]

Farrel, A., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "Framework for IETF Network Slices", Work in Progress, Internet-Draft, [draft-ietf-teas-ietf-network-slices-08](https://www.ietf.org/archive/id/draft-ietf-teas-ietf-network-slices-08), 6 March 2022,  
<<https://www.ietf.org/archive/id/draft-ietf-teas-ietf-network-slices-08.txt>>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](https://www.rfc-editor.org/info/rfc2119), [RFC 2119](https://www.rfc-editor.org/info/rfc2119), DOI 10.17487/RFC2119, March 1997,  
<<https://www.rfc-editor.org/info/rfc2119>>.

## [7.2](#). Informative References

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

Dong, J., Li, Z., Gong, L., Yang, G., Guichard, J. N., Mishra, G., Qin, F., Saad, T., and V. P. Beeram, "Scalability Considerations for Network Resource Partition", Work in Progress, Internet-Draft, [draft-dong-teas-nrp-scalability-01](https://www.ietf.org/archive/id/draft-dong-teas-nrp-scalability-01), 7 February 2022,  
<<https://www.ietf.org/archive/id/draft-dong-teas-nrp-scalability-01.txt>>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", [RFC 4364](https://www.rfc-editor.org/info/rfc4364), DOI 10.17487/RFC4364, February 2006, <<https://www.rfc-editor.org/info/rfc4364>>.

## Authors' Addresses

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

Li, et al.

Expires 8 September 2022

[Page 7]

---

Internet-Draft

E2E IETF Network Slicing

March 2022

Email: [lizhenbin@huawei.com](mailto:lizhenbin@huawei.com)



Jie Dong  
Huawei Technologies  
Huawei Campus, No. 156 Beiqing Road  
Beijing  
100095  
China  
Email: jie.dong@huawei.com

Ran Pang  
China Unicom  
Email: pangran@chinaunicom.cn

Yongqing Zhu  
China Telecom  
Email: zhuyq8@chinatelecom.cn