Network Working Group
Internet-Draft
Intended status: Informational
Expires: 31 August 2025

Z. Li
J. Dong
Huawei Technologies
R. Pang
China Unicom
Y. Zhu
China Telecom
L. Contreras
Telefonica

27 February 2025

Realization of Composite IETF Network Slices
draft-li-teas-composite-network-slices-04

Abstract

A network slice offers connectivity services to a network slice customer with specific Service Level Objectives (SLOs) and Service Level Expectations (SLEs) over a common underlay network. RFC 9543 describes a framework for network slices built in networks that use IETF technologies. As part of that framework, the Network Resource Partition (NRP) is introduced as a collection of network resources that are allocated from the underlay network to carry a specific set of network slice service traffic and meet specific SLOs and SLEs. In some network scenarios, network slices using IETF technologies may span multiple network domains, and they may be composed hierarchically, which means a network slice itself may be further sliced. In the context of 5G, a 5G end-to-end network slice consists of three different types of network technology segments: Radio Access Network (RAN), Transport Network (TN) and Core Network (CN). The transport segments of the 5G end-to-end network slice can be provided using network slices described in RFC 9543.

This document first describes the possible use cases of composite network slices built in networks that use IETF network technologies, then it provides considerations about the realization of composite network slices. For the multi-domain network slices, an Inter-Domain Network Resource Partition Identifier (Inter-domain NRP ID) may be introduced. For hierarchical network slices, the structure of the NRP ID is discussed. And for the interaction between IETF network slices with 5G network slices, the identifiers of the 5G network slices may be introduced into IETF networks. These network slice-related identifiers may be used in the data plane, control plane and management plane of the network for the instantiation and management of composite network slices. This document also describes the management considerations of composite network slices.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[RFC9543] defines network slicing in networks built using IETF technologies. These network slices may be referred to as RFC 9543 Network Slices, in this document we simply use the term "network slice" to refer to this concept when only the network slices as described in [RFC9543] is referred to.

A network slice aims to offer connectivity service to a network slice customer with specific Service Level Objectives (SLOs) and Service Level Expectations (SLEs) over a common underlay network. [RFC9543] defines the terminologies and the characteristics of network slices. It also discusses the general framework, the components and interfaces for requesting and operating network slices. The concept of a Network Resource Partition (NRP) is introduced by [RFC9543] as part of the realization of network slices. An NRP is a collection of network resources in the underlay network, which can be used to ensure the requested SLOs and SLEs of network slice services are met.

[I-D.ietf-teas-enhanced-vpn] describes a layered architecture and the candidate technologies in different layers and planes for providing NRP-based enhanced VPN services. Enhanced VPNs aim to meet the needs of customers or applications which require connectivity services with advanced characteristics, such as the assurance of SLOs and specific SLEs. Enhanced VPN services can be delivered by mapping one or a group of overlay VPNs to an NRP which is allocated with a set of network resources. The enhanced VPN architecture and technologies could be used for the realization of network slices. [I-D.ietf-teas-ns-ip-mpls] describes a solution to realize network slicing in IP/MPLS networks.

In some network scenarios, network slices using IETF technologies may span multiple network domains, and they may be composed hierarchically, which means a network slice itself may be further sliced. In the context of 5G, a 5G end-to-end network slice consists of three different types of network technology segments: Radio Access

Network (RAN), Transport Network (TN) and Core Network (CN). The transport segments of the 5G end-to-end network slice can be provided using network slices described in [RFC9543].

Section 5.3 of [RFC9543] gives high level descriptions of network slice composition, which include hierarchical composition and sequential composition. This document first describes the possible use cases of composite network slices built using IETF network technologies, then it provides considerations about the realization of composite network slices based on NRPs. For sequential composite network slices which span multiple network domains, an Inter-Domain Network Resource Partition Identifier (Inter-domain NRP ID) may be introduced. For hierarchical composite network slices, the structure of the NRP ID is also discussed. And for the interaction between IETF network slices with 5G network slices, the identifiers of the 5G network slices may be introduced into IETF networks. These network slice-related identifiers may be used in the data plane, control plane and management plane of the network for the instantiation and management of composite network slices. This document also describes the management considerations of composite network slices.

2. Composite Network Slice Use Cases

2.1. Multi-domain Network Slices

One typical scenario of multi-domain network slice is to support 5G network slicing as shown in Figure 1. 5G end-to-end network slices consists of the slice subnets in RAN, Mobile Core and Transport networks. In the RAN and Mobile Core networks, the 5G end-to-end network slices are identified by Single Network Slice Selection Assistance Information (S-NSSAI). In the transport network, the 5G network slices are mapped to one or multiple RFC 9543 network slices.

The RFC 9543 network slice itself may span multiple network domains. It may be realized as an inter-domain enhanced VPN service, which is an inter-domain VPN with additional resource and performance commitments. In the underlay network, the IETF network slices can be mapped to an inter-domain NRP, which is the concatenation of multiple intra-domain NRPs from different network domains.

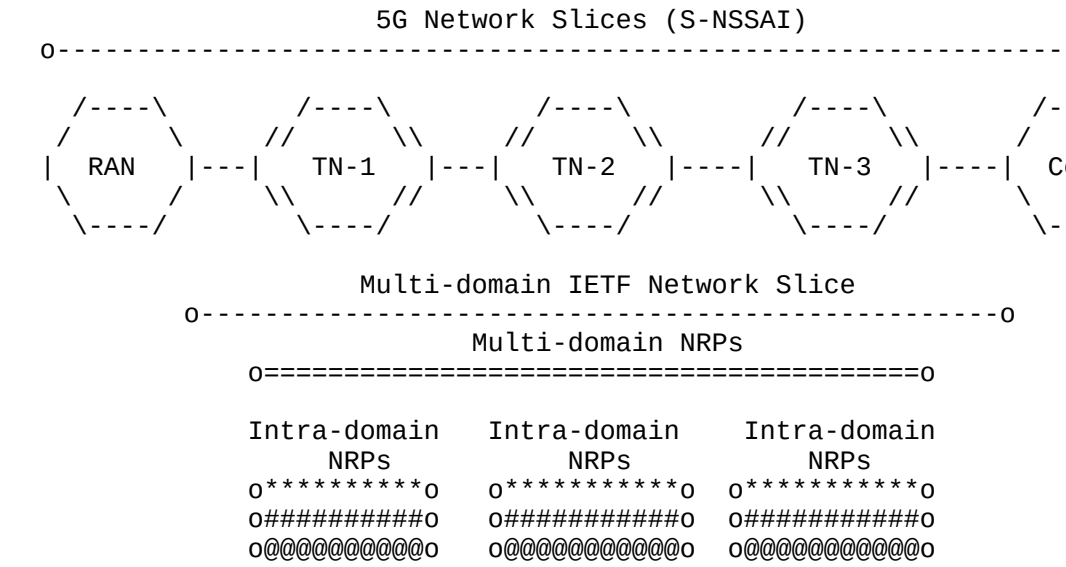

Figure 1. Multi-domain IETF Network Slice in 5G Scenario

2.2. Hierarchical Network Slices

This section gives some example use cases of hierarchical NRP and network slices, in which two levels of NRPs/slices are described. More than two levels of NRPs is also possible, while it is out of the scope of this document.

2.2.1. Per-Customer Network Slices in an Industrial Slice

A typical hierarchical network slice deployment scenario is in the multi-industrial network case, in which a shared physical network is used to deliver services to multiple vertical industries. Separate NRPs and network slices are provided for different industries, such as health-care, education, manufacturing, governmental affairs, etc. Then within the NRP of a specific industry, it may be necessary to create separate NRPs and network slices for specific customers.

For example, within the NRP created for the education industry, some of the universities may require a separate NRP and network slices to connect the branch campuses. Another example is within the NRP created for health-care industry, some of the hospitals may require a separate NRP and network slices for the connectivity and services between a set of the branch hospitals.

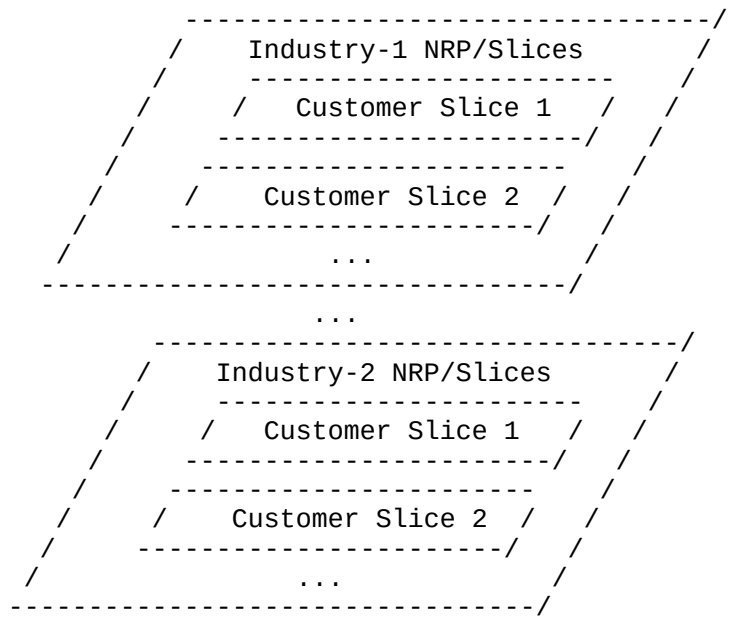

Figure 2. Hierarchical Network Slices: Scenario 1

2.2.2. Per-Application Network Slices in a Customer Slice

Another network slice deployment case is to provide an NRP and network slices for some important customers as the first-level network slices. While the customers may require to further split the resources of their NRP into different sub-NRP and sub-slices for a subset of applications.

For example, an NRP for a hospital may be further divided to carry different types of medical applications, such as remote patient monitoring, remote ultrasound diagnosis, medical image transmission etc.

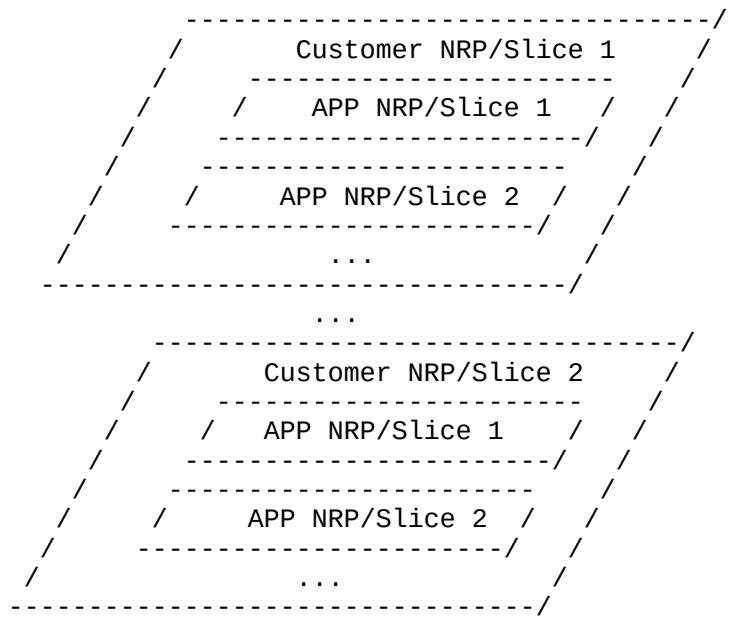

Figure 3. Hierarchical Network Slices: Scenario 2

2.2.3. Network Slice Services in a Wholesale Network Slice

An NRP or network slice can also be delivered as a wholesale service to other network operators. In this case, a network operator can be the customer of a network slice, and it may also need to deliver IETF network slice services to its customers. This is similar to the Carrier's Carrier VPN service, while additional requirements on the SLOs and SLEs required by the second-level network slice customer is fulfilled by a wholesale NRP.

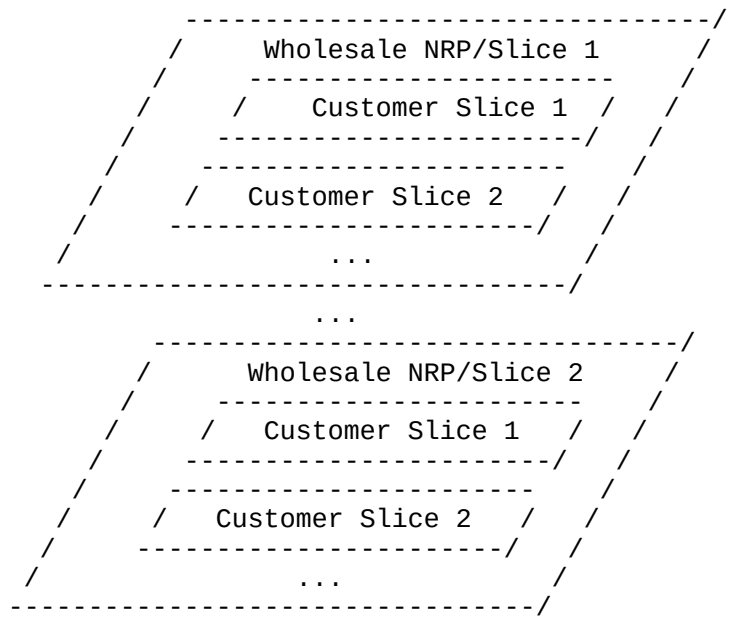

Figure 4. Hierarchical Network Slices: Scenario 3

3. Realization of Composite Network Slices

The realization of composite network slices may require additional capability and functionality in the data plane, control plane and management plane technologies. Considerations about the realization of composite network slices are analyzed in the following subsections.

3.1. Composite Network Slice Related Identifiers

For the realization of multi-domain network slices, the following network slice related identifiers may be introduced in the management plane, control plane and/or the data plane.

* Intra-domain NRP ID: This is the NRP-ID as defined in [I-D.ietf-teas-nrp-scalability]. It is used by network nodes in a network domain to determine the set of local network resources allocated to an NRP.

* Multi-domain NRP ID: This identifier uniquely identifies a multi-domain NRP. In each network domain, the domain border nodes can map the multi-domain NRP-ID to the intra-domain NRP IDs used within the local network domain.

A multi-domain network slice may be supported by a multi-domain NRP in the underlay, which consists of the concatenation of multiple intra-domain NRPs. Each intra-domain NRP can be identified using a network-wide NRP ID. In order to facilitate the concatenation of multiple intra-domain NRPs into a multi-domain NRP, the multi-domain NRP may be needed in the management plane, control plane and/or data plane.

In the context of 5G end-to-end network slicing, in order to facilitate the mapping and management of 5G network slice services in the IETF network slices, the identifier of 5G network slice may be introduced into the transport network.

* 5G network slice ID (S-NSSAI): This identifies a 5G network slice. When required, S-NSSAI may be used by network entities of RFC 9543 network slices for traffic mapping and monitoring at the 5G network slice granularity.

For network slice scenarios which are not specific to 5G network slicing, some types of service identifiers may be used by network entities of RFC 9543 network slices to classify and map the network slice services to the corresponding NRPs.

The requirement of multi-domain NRP-ID depends on how the intra-domain NRP IDs are managed. In some network scenarios, different network domains are under the same network administration, and can have consistent NRP ID assignment, then the same intra-domain NRP ID can be used in different network domains, and may be further used to identify a multi-domain NRP built across these domains. In other network scenarios, a multi-domain NRP ID would be needed for the identification of the concatenation of intra-domain NRPs in different domains. The awareness of the S-NSSAI and other network slice service identifiers depend on whether the performance of the 5G or other network slice services need to be monitored in the transport network.

For the realization of hierarchical network slices, since network resources may be partitioned hierarchically, different NRP IDs may be used to identify the first-level NRPs and the second-level NRPs respectively.

3.2. Composite Slice Network Resource Partitioning

For multi-domain network slices, in order to fulfil the end-to-end network slice service commitment, it is important that the network resources in each of the involved network domain can be partitioned for different NRPs, so that intra-domain NRPs can be created in each network domain, which together constitute the multi-domain NRPs for the end-to-end network slice services.

For hierarchical network slices, the network resources in the underlay network may need to be partitioned hierarchically. Taking a two-level hierarchical network slice as an example, the bandwidth and associated resources of a physical interface may need to be partitioned into two levels.

In different network domains or different network slice hierarchy, different technologies may be used for the data plane resource partitioning. For example, for resource partitioning of multi-domain network slices, it could be the case that in one network domain, the network resources are partitioned using Flexible Ethernet (FlexE), while in another network domain, the network resources may be partitioned using virtual sub-interfaces or dedicated queues under the same interface. Similarly, for hierarchical network resource partitioning, the network resources of the first-level NRPs may be partitioned using separate FlexE or virtual sub-interfaces with guaranteed link bandwidth, while the second-level NRPs may be further partitioned using virtual data channels under the FlexE or virtual sub-interfaces.

3.3. Data Plane Encapsulation

The considerations about the data plane encapsulation is mainly related to the mechanisms used to determine to which network slice a data packet belongs.

At the ingress of an IETF network slice, service flows of network slice can be classified and mapped to corresponding NRPs using flexible matching rules based on operators' local policy, so that the set of network resources of the corresponding NRPs can be used for processing and forwarding the service packet. Such matching can be done based on one or multiple fields in the data packet. While on the intermediate network nodes, a dedicated data plane NRP ID [I-D.ietf-teas-nrp-scalability] can facilitate the identification of the NRP a packet belongs to.

3.3.1. Multi-domain Network Slice Encapsulation

When network slice service packets traverse a multi-domain NRP, the multi-domain NRP ID may be carried in the packet, then the border nodes of each network domain can use it to determine the local domain NRP according to the mapping relationship between the multi-domain NRP ID and the local intra-domain NRP ID. The intra-domain NRP ID may also be carried in the packet for the NRP-specific packet processing on network nodes in the local domain. This requires that the involved network domains are considered as in the same trusted domain, in which the assignment of multi-domain NRP IDs is possible.

3.3.2. Hierarchical Network Slice Encapsulation

For hierarchical IETF network slices, each level of the hierarchical NRP needs to be identified using some fields in the data packet. One possible approach is to use NRP-specific resource-aware SIDs [I-D.ietf-spring-resource-aware-segments] to identify the set of resources allocated in the first-level NRPs, then use a dedicated NRP ID to identify the set of resources in the second-level NRPs. Alternatively, for better scalability [I-D.ietf-teas-nrp-scalability], dedicated NRP IDs may be used to identify both the first-level NRPs and the second-level NRPs. When dedicated NRP ID is used for both hierarchies, there are different options in the design of the data plane NRP ID for hierarchical network slices.

* The first option is to use a unified data plane NRP ID for both the first-level NRPs and the second-level NRPs. In this case, the first-level NRPs and the second-level NRPs are distinguished using different NRP ID values.

* The second option is to use hierarchical identifiers for the first-level NRP and the second-level NRP respectively. In this case, the first part of the identifier may be used to identify the first-level NRP, and the second part of the identifier may be used to identify the second-level NRP. Depends on the data plane technologies used, the hierarchical NRP may be encapsulated in one field, or may be positioned in separate fields in the packet.

3.3.3. 5G E2E Network Slice Encapsulation

In the context of 5G end-to-end network slicing, in order to facilitate the mapping and management of 5G network slice services to IETF network slices, the S-NSSAI of 5G network slice may be carried in the data packet sent to the transport network. For network slicing scenarios which are not specific to 5G, other types of service identifiers may be carried in the packet sent to the

transport network.

3.4. Composite Slice Control Plane

The control plane of multi-domain IETF network slices would be similar to that of the Inter-AS VPN services [RFC4364], possibly with additional information of network slice related characteristics signaled in the control plane. The Inter-AS Option C mode is preferred due to the simplicity in network slice service endpoints provisioning, which requires to establish multi-domain NRPs in the underlay network. The Option A or Option B mode of inter-domain VPN may also be used for multi-domain IETF network slices, while they are not the focus of this document.

In each network domain, the provisioning and distribution of the intra-domain NRP information may be done via either the local domain network slice controllers or a distributed control plane, then the multi-domain NRP is realized as the concatenation of multiple intra-domain NRPs. The allocation of the multi-domain NRP-ID and the mapping relationship between the multi-domain NRP ID and intra-domain NRP ID in each domain can be done by a IETF network slice controller which is responsible for multiple network domains. Alternatively, distributed control plane may be used to advertise or signal the necessary information for stitching the NRP-specific paths of intra-domain NRPs into a multi-domain NRP-specific path. For 5G end-to-end network slices, when S-NSSAI is carried in the network slice service packets, the IETF network slice controller may be responsible for the provisioning of the mapping relationship between the S-NSSAIs and the multi-domain NRP IDs at the edge of the transport network.

For hierarchical network slices, the control plane is responsible for the distribution of the attributes and states of NRPs in different hierarchy both among network nodes in the NRP and to the network controller. According to the modeling of network resource partitioning in different hierarchy, the NRP information may be advertised as either layer-3 or layer-2 network information, and the control protocols may be extended correspondingly. The details of the control plane extensions are out of the scope of this document.

4. Management Considerations

For multi-domain network slices, some coordination in management plane among different network domains would be needed. That includes but not limited to the planning of intra-domain NRPs to meet the same or similar set of SLO and SLEs, the allocation and mapping of intra-domain NRP IDs with the multi-domain NRP IDs.

For the hierarchical network slices, the management system of network operator needs to provide life-cycle management to both the first-level and the second-level NRPs and network slices. The first-level and second-level NRPs and network slices may be managed separately, while the relationship between the first-level and second-level NRPs and network slices also need to be maintained in the management system. Thus management system may need to support additional functions and procedures for the management of hierarchical network slices. Further analysis of management plane requirements is for future study.

5. IANA Considerations

This document makes no request of IANA.

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

6. Security Considerations

Several broad security considerations exist, and Section 6 of [RFC9543] highlights several important security aspects for network slice deployment and operation. These security considerations will apply to the architecture and techniques outlined in this document and multi-domain NRPs for end-to-end network slices.

Ensuring that only authorised customers have access to end-to-end network slices is important. In addition, malicious intent to access, delete or modify the end-to-end service should also be mitigated or negated.

The control plane may distribute attributes of different levels of hierarchical NRPs among network nodes, including communicating this information to the controller. Therefore, secure methods will be required to disseminate, control, and store NRP related information.

Multiple data plane methods are applicable for instantiating the end-to-end network slice services. However, these techniques have security advantages and disadvantages and must be considered when deploying multi-domain and hierarchical network slices. In addition, some encapsulation methods will have stronger security or encryption capabilities that may be required for certain customer slice applications where confidentiality or securing data being transmitted across the end-to-end slice is needed.

Future versions of this document will expand the security discussion and propose techniques to address security concerns, and highlight any missing requirements specific to this document.

7. Contributors

Zhibo Hu
Email: huzhibo@huawei.com

8. Acknowledgements

The authors would like to thank Daniel King for his review and comments.

9. References

9.1. Normative References

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Network Resource Partition (NRP) based Enhanced Virtual Private Networks", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-20, 14 June 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-enhanced-vpn-20>.

[RFC9543] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "A Framework for Network Slices in Networks Built from IETF Technologies", RFC 9543, DOI 10.17487/RFC9543, March 2024, <https://www.rfc-editor.org/info/rfc9543>.

9.2. Informative References

[I-D.ietf-spring-resource-aware-segments]
Dong, J., Miyasaka, T., Zhu, Y., Qin, F., and Z. Li, "Introducing Resource Awareness to SR Segments", Work in Progress, Internet-Draft, draft-ietf-spring-resource-aware-segments-10, 12 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-resource-aware-segments-10>.

[I-D.ietf-teas-nrp-scalability]
Dong, J., Li, Z., Gong, L., Yang, G., and G. S. Mishra, "Scalability Considerations for Network Resource Partition", Work in Progress, Internet-Draft, draft-ietf-teas-nrp-scalability-06, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-nrp-scalability-06>.

[I-D.ietf-teas-ns-ip-mpls]
Saad, T., Beeram, V. P., Dong, J., Wen, B., Ceccarelli, D., Halpern, J. M., Peng, S., Chen, R., Liu, X., Contreras, L. M., Rokui, R., and L. Jalil, "Realizing Network Slices in IP/MPLS Networks", Work in Progress, Internet-Draft, draft-ietf-teas-ns-ip-mpls-04, 28 May 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ns-ip-mpls-04>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, 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
Email: 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

Luis M. Contreras
Telefonica
Email: luismiguel.contrerasmurillo@telefonica.com