Workgroup: Network Working Group
Internet-Draft:
draft-ma-teas-ietf-network-slice-deployment-02
Published: 23 October 2023
Intended Status: Informational
Expires: 25 April 2024
Authors: Y. Ma
China Telecom
R. Luo
China Telecom
A. Chan
China Mobile Hong Kong
B. Suen
China Mobile Hong Kong
J. Dong
Huawei Technologies
Y. Liu
China Unicom
H. Allahoum
Algeria Telecom

IETF Network Slice Deployment Status and Considerations

Abstract

Network Slicing is considered as an important approach to provide different services and customers with the required network connectivity, network resources and performance characteristics over a shared network. Operators have started the deployment of network slices in their networks for different purposes. This document introduces several deployment cases of IETF network slices in operator networks. Some considerations collected from these IETF network slice deployments are also provided.

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].

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 25 April 2024.

Table of Contents

1. Introduction

Network Slicing is considered as an important mechanism to provide different services and customers with the required network connectivity, resources and performance characteristics over a shared network. [I-D.ietf-teas-ietf-network-slices] describes network slicing in the context of networks built from IETF technologies, and discusses the general framework of IETF network slices. [I-D.ietf-teas-ietf-network-slices] also introduces the concept Network Resource Partition (NRP) as a set of network resources that are available to carry traffic and meet the SLOs and SLEs.

[I-D.ietf-teas-enhanced-vpn] describes the framework and candidate component technologies for providing enhanced VPN services, by utilizing an approach that is based on existing VPN and Traffic Engineering (TE) technologies and adds characteristics that specific services or customers require above traditional overlay VPNs. VPN+ is delivered using a VPN overlay and an underlying Virtual Transport Network (VTN) which has a set of dedicated or shared resources and is associated with a customized logical network topology in the underlay network. A centralized network controller can be used for the creation and operation of the VTNs, and the mapping of the enhanced VPN services to the appropriate VTNs. The enhanced VPN (VPN+) mechanism can be used for the realization of IETF network slices. VTN and NRP are considered as similar concepts, and NRP can be seen as an instantiation of VTN in the context of network slicing.

Although the concept of network slicing is firstly introduced for the 5G, the use cases of IETF network slices are not limited to 5G. Operators have started the deployment of IETF network slices based on VPN+ in their networks for different service scenarios. This document introduces several deployment cases of IETF network slices in operator networks. Some considerations about the IETF network slice deployments are also collected.

2. IETF Network Slice Deployment Status

2.1. China Telecom Ningxia

Service scenario: Multiple industrial services

Resource partitioning: Virtual sub-interface with dedicated bandwidth

Data Plane: SRv6

Control plane: SR Policy with link affinity

2.2. China Mobile Hong Kong

Service scenario: Fixed-Mobile convergence services

Resource partitioning: Flexible Ethernet interface and virtual sub-interface with dedicated bandwidth

Data plane: SR-MPLS

Control Plane: SR Policy with link affinity

2.3. China Unicom Hebei

Service scenario: Multiple types of services

Resource partitioning: Flexible Ethernet interface

Data Plane: SRv6

Control Plane: SR Policy with link affinity

2.4. Algeria Telecom

Service scenario: Live Video and other services

Data Plane: SRv6 with NRP-ID

Control Plane: SR Policy with NRP-ID

2.5. China GuangXi Electronic Government Extranet

Service scenarios: Multiple types of governmental affairs

Data Plane: SRv6 with NRP-ID

Control Plane: SR Policy with NRP-ID

3. IETF Network Slice Deployment Cases

3.1. Network Slicing for Multi-Industrial Network

China Telecom has deployed a dedicated SRv6 based network in Ningxia to carry multiple industrial services. The three major types of service in the network are: Healthcare service, Education service and Broadband services, and the operator plans to migrate a set of industrial and governmental services from dedicated private networks or Multi-Service Transport Platform (MSTP) networks to this IP based multi-industrial network. With the help of network slicing, services of different industries can be isolated from each other, so that the performance of each service can be guaranteed, and the cost of

maintaining and expanding the dedicated private networks for each industry can be reduced.

In order to provide the required resource and security isolation between the health care, education and broadband services, three NRPs are created in the network. All the NRPs share the same IGP instance, while each NRP is defined with a logical topology using different link administrative groups (i.e. color), and is allocated with a set of dedicated bandwidth resources on each involved physical link using the virtual sub-interface mechanism. In an NRP, each link is assigned with a SRv6 End.X SID to identify the sub-interface used for packet forwarding. With more industrial and governmental customers migrate to this network, more NRPs with dedicated network resources will be created.

Multiple L3VPNs belonging to the same industry are provisioned in the corresponding NRP. For example, the NRP created for the health care services is used to support the VPNs for the connection between hospitals belonging to the medical consortium, and the VPNs for connecting the hospitals and the insurance systems in the healthcare cloud. The VPN traffic mapped to a NRP is steered into the set of virtual sub-interfaces of the NRP based on the corresponding SRv6 End.X SIDs.

A centralized network controller is responsible for the management of the NRP and the VPNs. This includes the topology and resource planning of NRP, the NRP creation, the mapping of VPN services to the NRP, and the computation of SRv6 TE paths based on the service constraints and the topology and resource attributes of the NRP. The controller also collects the traffic statistics and performance information of the NRPs and the VPN services to enable the network slice services visualization and ensure the service SLAs are always met.

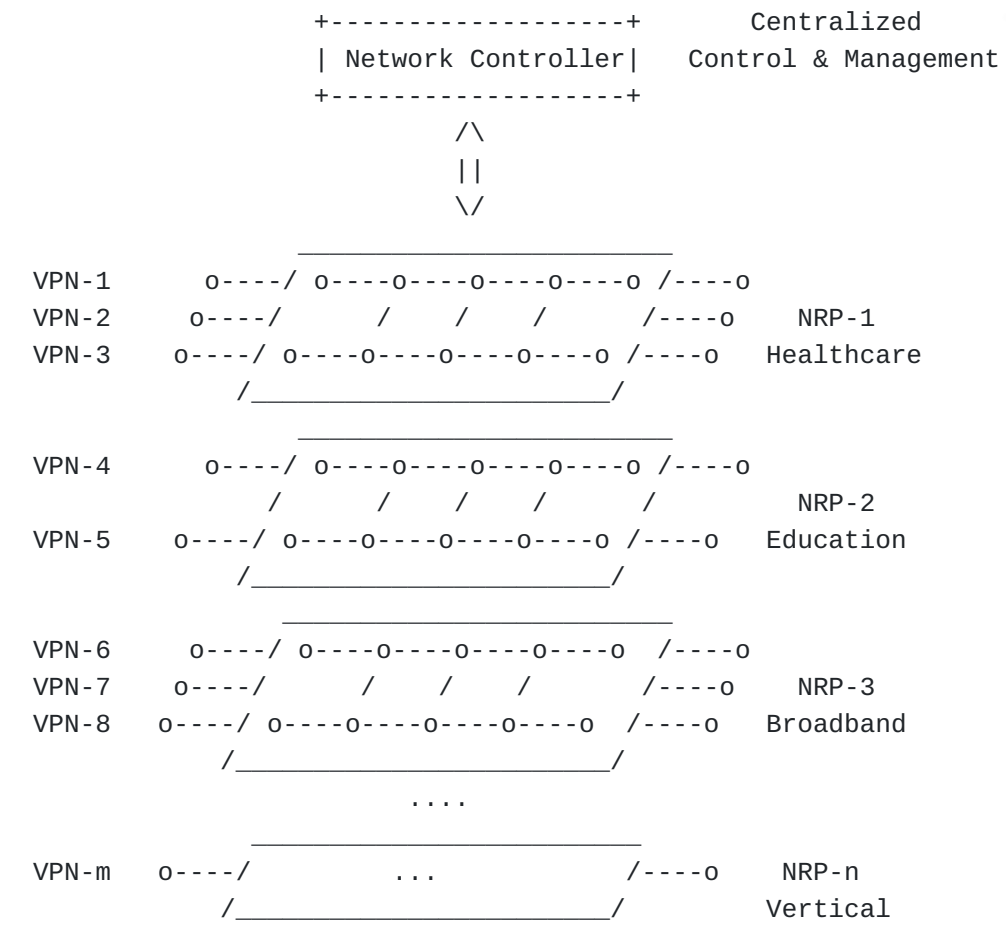

Figure 1. IETF network slice deployment in China Telecom Ningxia

3.2. Network Slicing for Fixed-Mobile Convergence

China Mobile Hong Kong (CMHK) has deployed network slices in their SR-MPLS based Fixed-Mobile Convergence (FMC) network, which is used to carry the mobile services, the enterprise private line services and the residential broadband services together. Each type of service has different traffic characteristics and performance requirements, thus independent network planning and operation for each service type is required.

Currently three NRPs are created for mobile service, enterprise service and the residential service respectively. Depends on the new service requirement of 5G, More NRPs may be created for 5G critical services in the future. According to the operator's network planning, each NRP is allocated with a set of dedicated bandwidth resources using either virtual sub-interface or Flexible Ethernet (FlexE) interface mechanism. All the NRPs share the same IGP instance, while the links belonging to different NRPs are assigned with different link administrative groups (i.e. color). In a NRP, each link is assigned with an SR-MPLS Adj-SID to identify the sub-interface or FlexE interface used for packet forwarding.

Multiple VPNs (EVPN, L3VPN and L2VPN) belonging to the one of the three major service types are mapped to the corresponding NRP. For example, the NRP created for the enterprise private line services is used to support the VPNs of a group of enterprise customers. The VPN traffic mapped to a NRP is steered into the set of virtual sub-interfaces or FlexE interfaces allocated to the NRP based on the corresponding SR-MPLS Adj-SIDs.

A centralized network controller is responsible for the management of the NRP and the VPNs. This includes the topology and resource planning of NRP, the NRP creation, the mapping of VPN services to the NRP, and the computation of SRv6 TE paths based on the service constraints together with the topology and resource attributes of the NRP. The controller also collects the traffic statistics and performance information of the NRPs and the VPN services to enable the network slice services visualization and ensure the service SLAs are always met.

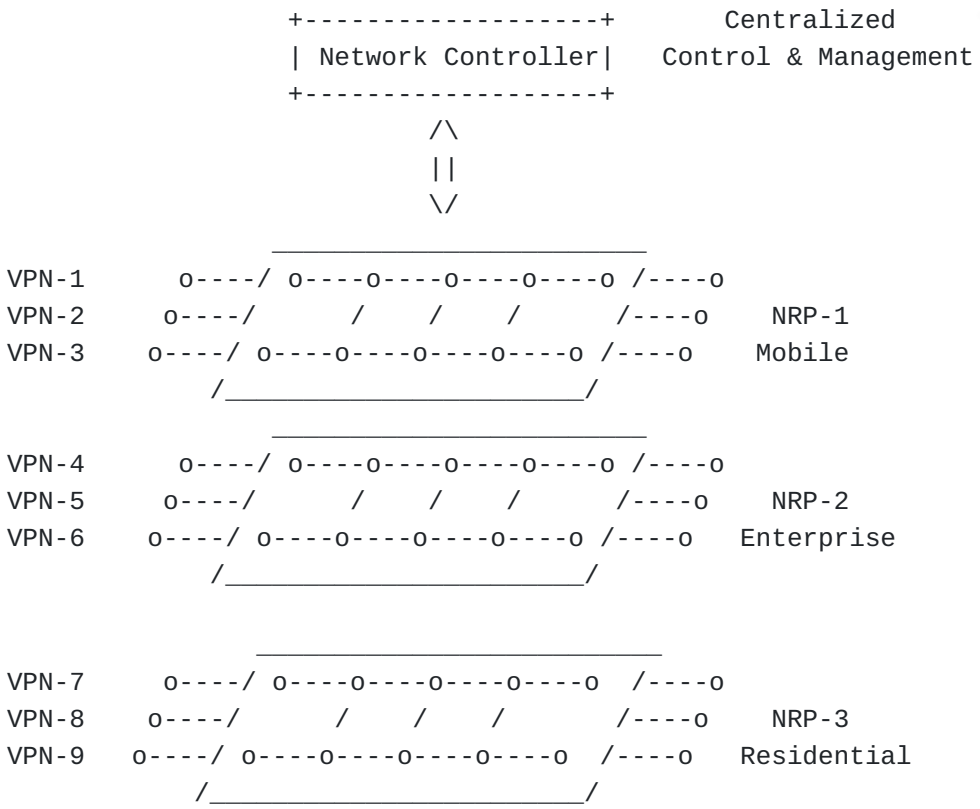

Figure 2. IETF network slice deployment in CMHK

3.3. Network Slicing for Government Affairs Separation

China Unicom has deployed an SRv6 based cloud network in Hebei for the transport of multiple types of services, including 5G mobile services, government affair service, business private line services and broadband service.

In order to meet the performance and isolation requirement of different type of services, four NRPs are provisioned in the network. All the NRPs share the same IGP instance, while each NRP is defined with a logical topology using different link administrative groups (i.e. color), and is allocated with a set of dedicated bandwidth resources on each involved physical link using FlexE. In an NRP, each FlexE client interface is assigned with a SRv6 End.X SID to steer packets to the set of link resources allocated to the NRP.

According to the service requirement, one or multiple EVPN instances are provisioned for each type of service, and are mapped to the corresponding NRP. For example, an NRP created for the government affair service is used to support the VPNs for the connection between government institution in different cities and towns, and the VPNs for connecting the government institution with the government affair cloud. Based on SRv6 Policy, VPN traffic is steered into a SRv6 TE path which comprises of the FlexE client interfaces of the NRP according to the corresponding SRv6 SID list.

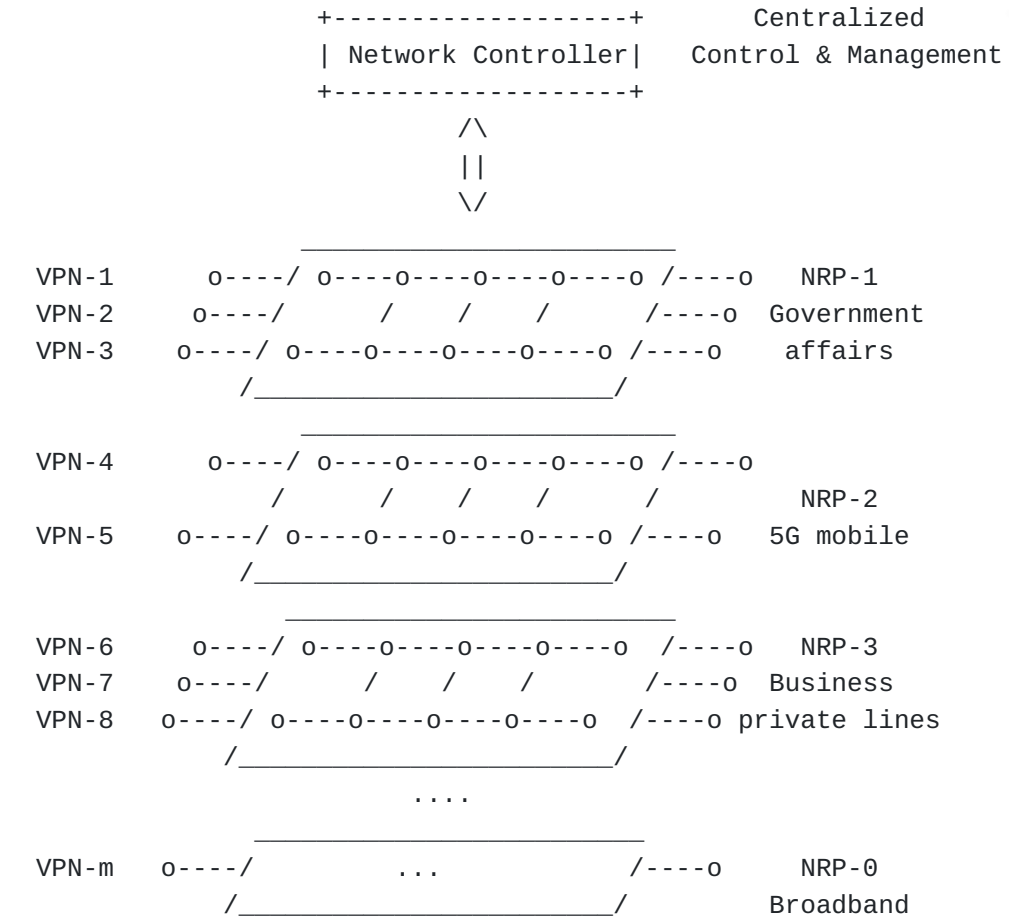

Figure 3. IETF network slice deployment in China Unicom Hebei

3.4. Network Slicing for Live Video Service

Algeria Telecom has deployed an SRv6 based metro network. The recent requirement is to deliver live video broadcast service for sports games, and the related intranet services and internet services together happening on the same sites, the SLA requirement of each type of service is different. There are also existing services which need to coexist with these three types of services.

In order to meet the performance and isolation requirement of these type of services, four NRPs are provisioned in the network:

*NRP-1 for live video services

*NRP-2 for intranet services

*NRP-3 for internet services

*NRP-0 for other services

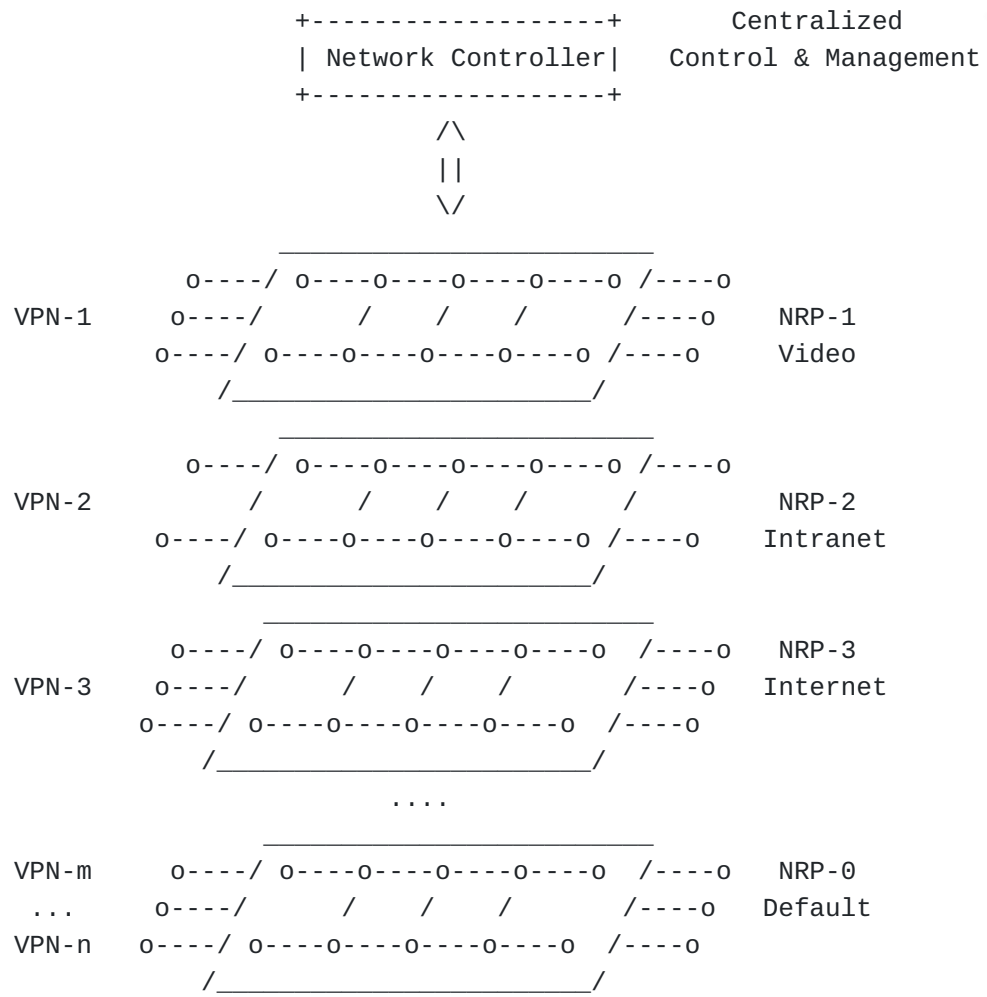

Figure 4. IETF network slice deployment in Algeria Telecom

All these NRPs share the same IGP instance, while each NRP is allocated with a subset of dedicated network resources. On each physical link which participates in an NRP, a set of link bandwidth is allocated using FlexE, and the FlexE client interface is associated with the NRP-ID.

According to the service requirement, one or multiple L2 or L3 EVPN instances are provisioned for each type of service, and are mapped to the corresponding NRP. For example, an NRP created for the live video broadcast service is used to support the EVPNs for the connection between the stadiums and the video broadcasting center.

A network controller performs the path computation using the topology and resources of the NRP as constraints, and SRv6 Policy is used to provision the SRv6 TE paths associated with each NRP to the ingress nodes, using the mechanism defined in [I-D.dong-idr-sr-policy-nrp]. SRv6 Policy is also used to steer the VPN service traffic to SRv6 paths which could meet the service requirement, For VPN traffic which is steered into an SRv6 Policy in an NRP, in addition to encapsulating the SRv6 SID list, the packet is also encapsulated with the global unique NRP-ID in the IPv6 HBH extension header based on the mechanism defined in [I-D.ietf-6man-enhanced-vpn-vtn-id], and the NRP-ID is used to determine the FlexE client interfaces which are used to forward the traffic mapped to the NRP.

3.5. Network Slicing for Multi-type Government Affairs

China Guangxi Province has deployed an SRv6 based network for multi-type government affairs. The purpose is to replace a number of dedicated networks built for different government public affairs in the past. The major services include government portal service, government management service, mobile government affairs, data sharing service, public safety service, video conference service, etc. These services have diverse requirements on network connectivity, bandwidth, latency and reliability. In order to meet the service requirements in one underlay network, three Network Resource Partitions (NRPs) are deployed, and more NRPs may be introduced in the future.

*NRP-1 for public safety service

*NRP-2 for video conference service

*NRP-0 for other services

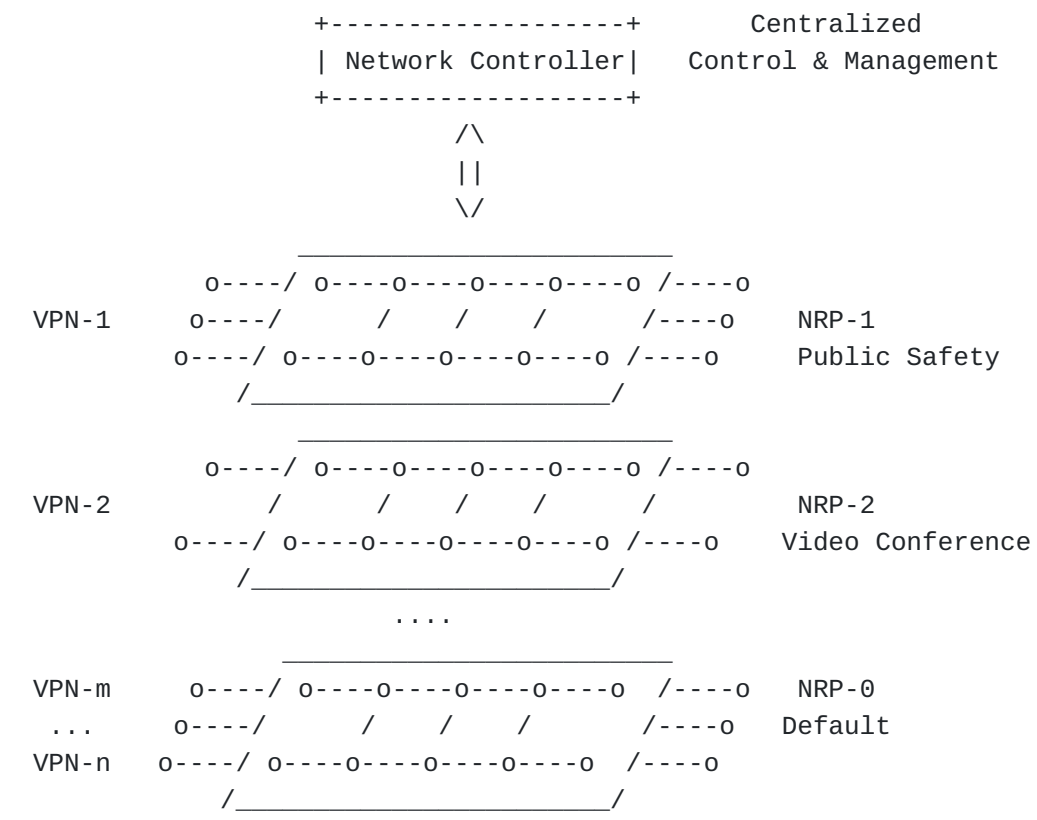

Figure 5. IETF network slice deployment in Guangxi Government Extranet

All these NRPs share the same IGP instance, while each NRP is allocated with a subset of dedicated network resources. On each physical link which participates in an NRP, a set of link bandwidth is allocated using FlexE, and the FlexE client interface is associated with the NRP-ID.

According to the service requirement, one or multiple L2 or L3 EVPN instances are provisioned for each type of service, and are mapped to the corresponding NRP. For example, the NRP created for the video conference service is used to support all the public video conference services between different departments and organizations on the goverment extranet.

A network controller is deployed for path computation using the topology and resources of the NRP as constraints, and SRv6 Policy is used to provision the SRv6 TE paths associated with each NRP to the ingress nodes, using the mechanism defined in [I-D.dong-idr-sr-policy-nrp]. SRv6 Policy is also used to steer the VPN service traffic to SRv6 paths which could meet the service requirement, For VPN traffic which is steered into an SRv6 Policy in an NRP, in addition to encapsulating the SRv6 SID list, the packet is also encapsulated with the global unique NRP-ID in the IPv6 HBH extension header based on the mechanism defined in [I-D.ietf-6man-enhanced-vpn-vtn-id], and the NRP-ID is used to

determine the FlexE client interfaces which are used to forward the traffic mapped to the NRP.

4. Network Slice Deployment Considerations

Based on the network slice deployment cases collected in section 2, this section describes some of the operators' considerations about network slice deployment.

4.1. Isolation

Network slicing is introduced to operators' network to meet the connectivity and performance requirements of different services or customers. Since many services or customers are migrated from their own dedicated networks to network slices, it is expected that services or customers carried by a network slice will not be affected by any other traffic in the network, thus the resource, policy and security isolation from other services becomes a typical requirement.

Operators have considered the usage of several forwarding plane mechanisms, such as FlexE interface or virtual sub-interfaces to allocate different set of network resources for the NRPs used for different services or customers. The services or customers which do not have specific requirement on resource or security isolation may be provisioned as separated VPNs, while these VPNs can be aggregated and mapped to a shared NRP with a set of aggregated network resources.

4.2. Topology and Connection Types

According to the deployment scenarios of network slices, there can be different requirements on the topology and connection type of the network slices. When a network slice is provided for a particular service type or for a particular industry, the network slice usually covers a network scope similar to the scope of the physical network, and there are usually a large number of end points attached to the network slice, which requires meshed multipoint-to-multipoint connectivity between them. When a network slice is provided for a specific private line service customer, the network slice could have a customized topology covering a portion of the physical network, and usually has a small number of end points attached, in this case the network slice may be expressed as a set of point-to-point connections.

The suitable mechanisms to define the topology of the NRP and build the connectivity needed by network slice service streams. For example, the administrative groups (i.e. color) can be used by a centralized controller to specify the topology of a NRP and compute the constraint paths for network slice services in the NRP. The

Distributed control plane based mechanism for topology definition and the constraint path computation may be used for network slices which require meshed connectivity between a large number of end points.

4.3. Scalability

As shown in several IETF network slice deployments, the number of NRPs at the initial stage can be small (e.g. less than 10). While there are also cases in which hundreds of network slices are needed for industrial and premium private line customers. It is expected that the number of NRPs required in the future could be at the hundreds or even thousands level. Thus the scalability considerations and optimization mechanisms as described in [I-D.dong-teas-nrp-scalability] need to be considered to allow the deployment of a larger number of network slices in the network in future.

4.3.1. Data Plane Scalability

The current deployment of network slices are mainly based on SR-MPLS or SRv6 data plane, with which each NRP is allocated with a separate group of SR SIDs, and the SIDs are associated with a group of dedicated network resources [I-D.ietf-spring-resource-aware-segments]. This provides a practical approach to deliver IETF network slices to meet the requirements in the early stage. While with the number of the required NRPs increases, the increasing amount of SR SIDs will bring challenges both to the forwarding tables and to the network management and operation. It is expected that the mechanisms with dedicated NRP-ID encapsulation as defined in [I-D.ietf-6man-enhanced-vpn-vtn-id] could help to reduce the number of SR SIDs needed, and simplify the large scale network slice provisioning and management.

4.4. Automation

The centralized network controller plays an important role in the life cycle management of network slices. With the number of network slices increases, it is necessary that the planning, creation, monitoring and the optimization of IETF network slices can be automated to reduce the burden in the network slice management and operation.

For example, in a network where multiple IETF network slices are deployed, when the bandwidth utilization of one NRP reaches a specific threshold, there are two possible approaches for the NRP capacity expansion. The first approach is to expand the capacity of the physical network, which usually can take a long time. The second approach is to adjust the resource allocation of different NRPs

based on the utilization ratio. The network controller can provide the monitoring and visualization of the resource utilization of the NRPs and VPNs, and gives recommendations about the optimal resource adjustment strategy to the network operation.

4.5. Hierarchical Network Slicing

In the beginning of the network slice deployment, a group of network slice services are provisioned in the same NRP for a particular industry or service type, such as an NRP for all the business private line services. While some of customers within an industry or service type may require to have a set of dedicated network resources allocated within the industry or service type based NRP. This brings the requirement of hierarchical network slicing to the operators. Thus it is expected that the deployed network slices can evolve to support hierarchical network slices according to the service demand.

5. IANA Considerations

This document makes no request of IANA.

6. Security Considerations

TBD

7. Contributors

Terence Ho
Email: terenceho@hk.chinamobile.com

Jimmy Tu
Email: jimmytu@hk.chinamobile.com

Jonathan Chung
Email: jonathanchung@hk.chinamobile.com

Kristy Li
Email: kristyli@hk.chinamobile.com

Tommy Zou
Email:tommyzou@hk.chinamobile.com

Chaohong Tan
Email: tanch@gxi.gov.cn

Jining Chen
Email: chenjn@gxi.gov.cn

Zhenbin Li
Email: lizhenbin@huawei.com

Zhibo Hu
Email: huzhibo@huawei.com

Juhua Xu
Email: xujuhua@huawei.com

Lei Bao
Email: baolei7@huawei.com

8. Acknowledgements

The authors would like to thank XXX for his valuable 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 Enhanced Virtual Private Network (VPN+)", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-14, 28 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-enhanced-vpn-14>.

[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 Network Slices in Networks Built from IETF Technologies", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-25, 14 September 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-25>.

[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>.

9.2. Informative References

[I-D.dong-idr-sr-policy-nrp] Dong, J., Hu, Z., and R. Pang, "BGP SR Policy Extensions for Network Resource Partition", Work in Progress, Internet-Draft, draft-dong-idr-sr-policy-nrp-03, 5 September 2023, <https://datatracker.ietf.org/doc/html/draft-dong-idr-sr-policy-nrp-03>.

[I-D.dong-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-dong-teas-nrp-scalability-02, 16 May 2022, <https://datatracker.ietf.org/doc/html/draft-dong-teas-nrp-scalability-02>.

[I-D.ietf-6man-enhanced-vpn-vtn-id] Dong, J., Li, Z., Xie, C., Ma, C., and G. S. Mishra, "Carrying Virtual Transport Network (VTN) Information in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-ietf-6man-enhanced-vpn-vtn-id-05, 6 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-enhanced-vpn-vtn-id-05>.

[I-D.ietf-spring-resource-aware-segments]
Dong, J., Bryant, S., Miyasaka, T., Zhu, Y., Qin, F., Li, Z., and F. Clad, "Introducing Resource Awareness to SR Segments", Work in Progress, Internet-Draft, draft-ietf-spring-resource-aware-segments-07, 31 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-resource-aware-segments-07>.

[I-D.ietf-spring-sr-for-enhanced-vpn]
Dong, J., Bryant, S., Miyasaka, T., Zhu, Y., Qin, F., Li, Z., and F. Clad, "Segment Routing based Virtual Transport

Network (VTN) for Enhanced VPN", Work in Progress, Internet-Draft, draft-ietf-spring-sr-for-enhanced-vpn-05, 31 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-for-enhanced-vpn-05>.

Authors' Addresses

Yusong Ma
China Telecom

Email: mayusong.nx@chinatelecom.cn

Rui Luo
China Telecom

Email: luorui.nx@chinatelecom.cn

Alex Chan
China Mobile Hong Kong

Email: alexckchan@hk.chinamobile.com

Ben Suen
China Mobile Hong Kong

Email: bensuen@hk.chinamobile.com

Jie Dong
Huawei Technologies

Email: jie.dong@huawei.com

Yang Liu
China Unicom

Email: liuyang118@chinaunicom.cn

Houcine Allahoum
Algeria Telecom

Email: allahoum@algerietelecom.dz