nfvrg
Internet-Draft
Intended status: Informational
Expires: January 3, 2019

S. Homma
NTT
X. de Foy
InterDigital Inc.
A. Galis
University College London

July 2, 2018

Gateway Function for Network Slicing
draft-homma-nfvrg-slice-gateway-00

Abstract

This document describes the roles and requirements for a slice gateway that is a data plane function or function group for connecting/disconnecting and compose/decompose network slice subnets and providing network slices from end to end. The interworkings between management and control elements at the management and control planes with the gateway function for controlling and orchestrating end-to-end network slices are also presented in this document.

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 January 3, 2019.

Table of Contents

1. Introduction 3
2. Definition of Terms 4
3. Motivations and Roles of SLG 5
4. Architecture of Network Slicing System 8
4.1. Network Slice Management System Architecture 8
4.2. Position of SLG on ETSI NFV MANO 10
5. Requirements for SLG 11
5.1. Management of NS as Infrastructure 11
5.1.1. Data Plane Aspect 11
5.1.1.1. Identification/Classification 11
5.1.1.2. Transporting/Forwarding 12
5.1.1.3. Isolation between NSs 13
5.1.1.4. Service Chaining as Infrastructural Mechanism(*Optional) 13
5.1.2. Control/Management Planes Aspects 14
5.1.2.1. Interfaces to Controllers or Operation Systems . 14
5.1.2.2. Address Resolution/Routing 14
5.1.2.3. Authentication Authorization Accounting (AAA) . . 14
5.1.2.4. Operation Administration and Maintenance(OAM) . . 14
5.2. Management of Services on NS (*Optional) 14
5.2.1. Data Plane Aspect 14
5.2.1.1. Identification/Classification 14
5.2.1.2. QoS Control 15
5.2.1.3. Steering/Service Chaining(Cooperation with VNFs) 15
5.2.2. Control/Management Planes Aspects 15
5.2.2.1. Interfaces to Service Management Systems 15
5.2.2.2. Collection of Telemetry information 15
6. Deployment of SLG 15
6.1. Examples of Components Required to Maintain SLG Functions 16
6.2. SLG Types Depending on Locations on NS 16
6.2.1. Edge SLG(E-SLG) 16
6.2.2. Inter-Subnet SLG(IS-SLG) 16
6.2.3. Inter-Domain SLG(ID-SLG) 16
6.3. Horizontal Connection 16
6.4. Vertical Connection 19
6.5. Software vs. Hardware 20
7. Interconnection between NS subnets 20
7.1. Pre-arrangement of transport protocols 20
7.2. Quality Assurance between SLGs 20
7.3. Secure Interconnection 21

8. Security Considerations 21
9. IANA Considerations 21
10. Acknowledgement 21
11. Informative References 21
Appendix A. Requirements for each SLG Type 23
Authors' Addresses 25

1. Introduction

Network slicing is an approach to create separate virtual networks in support of service depending on several requirements on the same physical resources, and it enables networks to adapt to requirements, which is diverse more, inexpensively and flexibly. It's also expected to enhance usability of infrastructural networks for tenants and create new business opportunities. For example, by using network slices lent from infrastructure operators, other industrial companies can provide communication services including ensurance of network transport without having physical infrastructure.

From a business point of view, a slice includes a combination of all the relevant network resources, functions, and assets required to fulfill a specific business case or service, including OSS, BSS and DevOps processes.

From the network infrastructure point of view, network slice requires the partitioning and assignment of a set of resources that can be used in an isolated, disjunctive or non- disjunctive manner for that slice.

From the tenant point of view, network slice provides different capabilities, specifically in terms of their management and control capabilities, and how much of them the network service provider hands over to the slice tenant. As such there are two kinds of slices: (A) Inner slices, understood as the partitions used for internal services of the provider, retaining full control and management of them. (B) Outer slices, being those partitions hosting customer services, appearing to the customer as dedicated networks.

Network slices are established with combination of various technologies, such as software defined network (SDN), network function virtualization (NFV), or traffic engineering, and managed/ operated with automation technologies such as orchestrator.

Assumed use cases of network slices include establishment of virtual networks whose qualities are guaranteed from end to end under the supervision of multi-domain orchstrators. In such cases, a network slice subnet is created on each domain, such as access network and

core network, and an end-to-end network slices is composed of connected subnets.

Network slice subnets are built based on specification of the underlay network, and thus the used technologies might vary. Therefore, a gateway function, which enables to connect subnets while adapting the differentiations and forward data packets to/from the appropriate next subnet, is required.

In this document, the gateway function is called slice gateway or SLG, and the role and requirements are described. Defining a new data plane technology is not a goal of this draft. This draft aims to specify management-related requirements for an SLG, which may be implemented using existing data plane technologies.

2. Definition of Terms

Network Slicing: Network slicing is a technology or an approach to create separate virtual networks in support of services, depending on several requirements, on the same physical resources. This is possible by combinations of several network technologies.

Network Slice (NS): An NS is a virtual network established on network infrastructure. Some include additional network functions such as firewall or load-balancer in addition to basically forwarding functions such as switches or routers. It has an overlay architecture and is independent from the underlay network's topology.

NS Subnet: An NS subnet is partially virtual network established within a single domain.

End-to-End Network Slice (E2E-NS): An E2E-NS is a virtual network connecting between end points. E2E slices are composed of a single NS subnet or multiple NS subnets.

Network Slice as a Service (NSaaS): An NSaaS is a NS distribution model in which a third-party provider hosts NSs and makes them available to customers.

Network Slice Tenant (NS Tenant): An NS tenant is a person or group that rents and occupies NSs from NS providers.

Domain: A domain is a group of a network and devices administrated as a unit with common rules and procedures.

Administrative Domain: An administrative domain is a group of networks and devices managed by an administrator.

Resource: A resource is element used to create virtual networks. There are several types of resources, i.e., connectivity, computing and storage.

Network Function Virtualization (NFV): NFV is the concept or technologies to provide dedicated network appliances as software.

Software Defined Network (SDN): SDN is the concept or technologies to separate network control plane from data plane, and control network devices dynamically and flexibly.

Virtual Network: A virtual network is a network running a number of virtual network functions.

Virtual Network Function (VNF): A virtual network function (VNF) is a network function whose functional software is decoupled from hardware. One or more virtual machines running different software and processes on top of industry-standard high-volume servers, switches and storage, or cloud computing infrastructure, and capable of implementing network functions traditionally implemented via custom hardware appliances and middleboxes (e.g., router, NAT, firewall, load balancer, etc.)

Slice Gateway Function (SLG): An SLG is a function or a group of functions to connect/disconnect NS subnets. The roles are described in the following sections.

Business Support System and Operation Support System (BSS/OSS): BSS/OSS are systems to support service providing and operation of network devices.

Orchestrator: Orchestrator is an entity to operate network components automatically. There are several types of orchestrators including NFV Orchestrator (NFVO) or service orchestrator defined by ETSI NFV and Open Source MANO (OSM) ([NFV-Architectural-Framework] and [OSM-White-Paper]).

SLG Controller (SLG-Ctrl): An SLG-Ctrl is an entity that controls SLGs. An SLG-Ctrl is controlled by upper-level operation systems such as OSS/BSS or orchestrator.

3. Motivations and Roles of SLG

One of the main roles of SLG is the enablement of interworkings between data plane with management and control elements for controlling and orchestrating end-to-end slices.

Use cases of network slices are discussed in several Standard Developing Organizations (SDOs). Some examples are described in use cases document ([I-D.netslices-usecases]).

In some proposed use cases, an NS is structured across multiple network domains. The capability of NS subnets might be different because the components are domain-specific. In particular, the differentiation in capability between different administrative domains is large.

For connecting some different NS subnets and providing a NS that guarantees the prescribed quality from end to end, SLGs are required to connect such NS subnets. SLGs enable to provide E2E-NSs independently of specifications of underlay networks by hiding the differentiations and connecting between NS subnets. An overview of this concept is shown in Figure 1. SLGs glue NS subnets established on each domain and provide an E2E-NS.

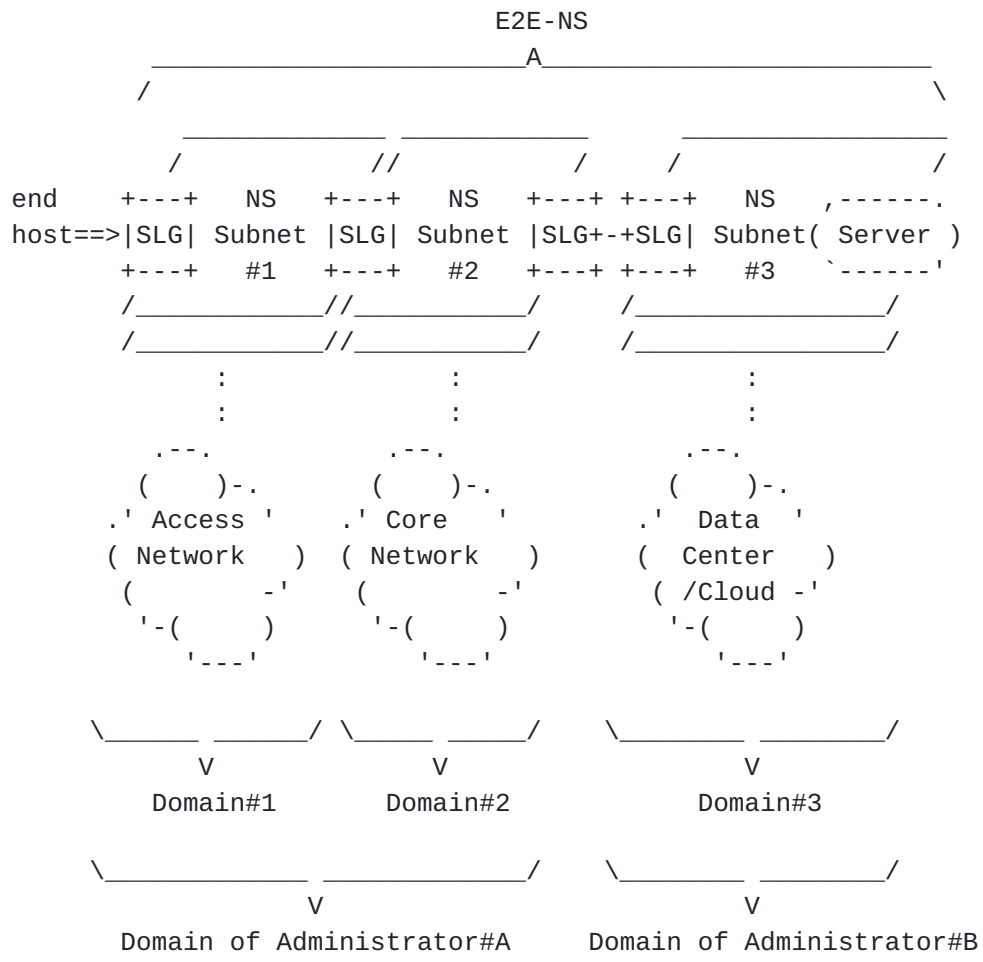

Figure 1: E2E-NS composed of multiple NS subnets

Moreover, identification of user service traffic and their allocation/disallocation to the appropriate NS subnet are required at the edges of E2E-NSs, as shown in Figure 2, and SLGs might take on these roles.

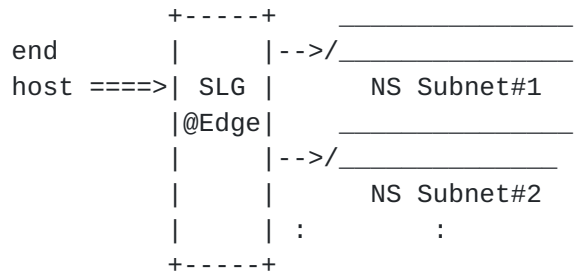

Figure 2: NS subnet selection of SLG

Note that, this model has the assumption that transitions of data packets from one NS subnet to another are executed at only SLGs. Also, an SLG is not necessarily implemented as a single device or virtual machine (VM).

4. Architecture of Network Slicing System

NSs are composed of several (virtual) network functions and links, and the charactaristics of each NS are based on the assumed service. Also, some of NSs are deployed accross multiple administrative domains. For deploying the appropriate NSs based on each service requirements, a management system, which enables to control network resources totally within a domain, and interaction between such management systems are required.

An SLG is a network function, and SLGs are installed at edge of NS subnets. NSs are dynamically created, deleted, and moved depending on requests from network opertor orNS tenants. Therefore, some SLGs would be required to be VNF for flexible deployment.

This section describes overview of NS management system architecture (Section 4.1) and position of SLG in NFV (Section 4.2).

4.1. Network Slice Management System Architecture

The architecture overview of NS management system is shown in Figure 3.

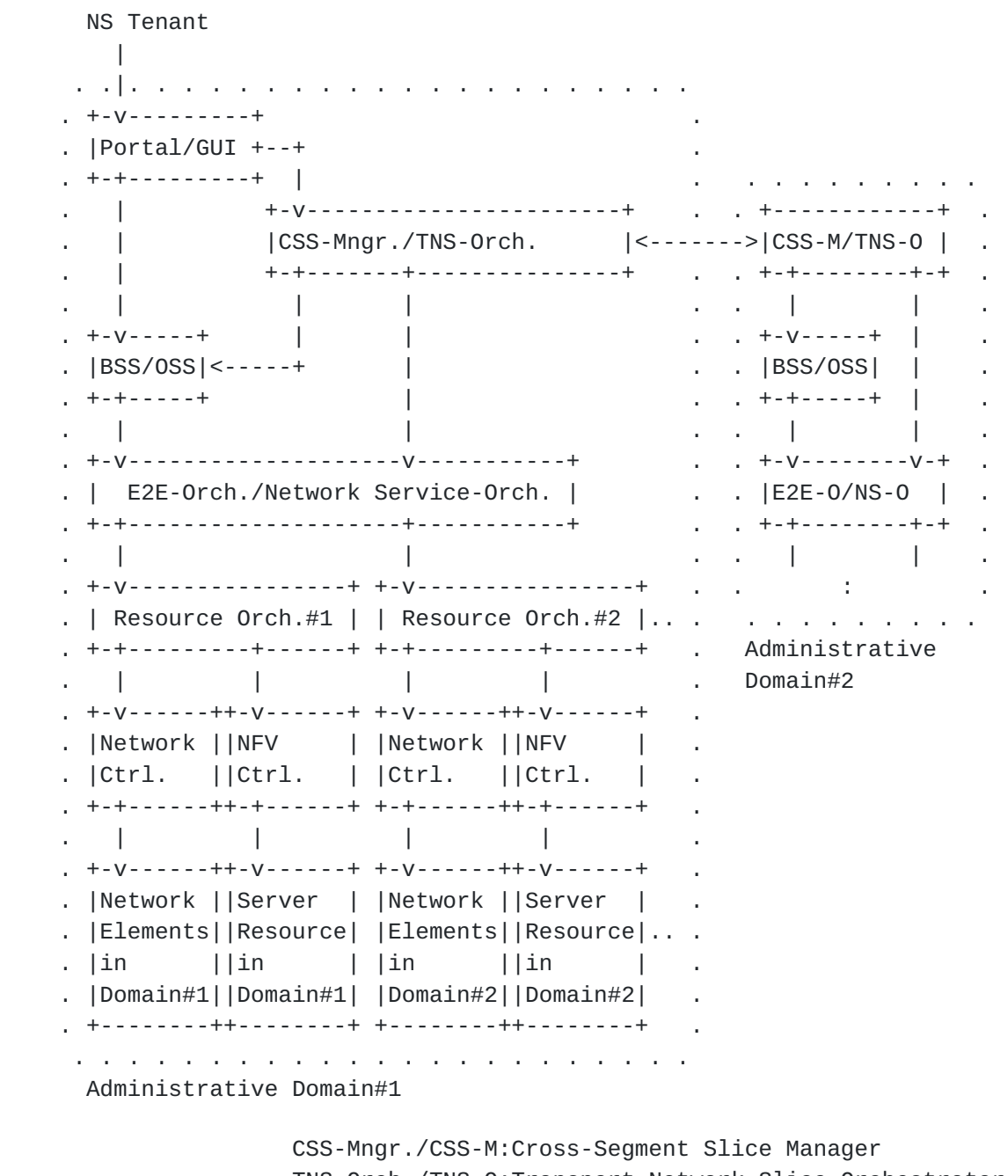

Figure 3: Overview of NS Management Architecture

Orchestrators manage whole resources including network elements and server resources (i.e., routing, bandwidth, compute or storage). In this figure, the resources including network elements and server resources are managed by resource orchestrators installed in each domain, and the E2E-orchestrator and network service orchestrator handle resource orchestrators.

NSs are requested from NS tenants via the portal system and the order of creations of an NS is given to the E2E orchestrator from the portal system via BSS/OSS. When an NS across multiple administrative domains are requested, the portal system that received the request forwards the order to create NS subnets to the other infrastructure providers' systems via Cross-Segment Slice Manager. The details of COMS architecture are described in the architecture document ([I-D.qiang-coms-architecture]).

SLGs are also controlled via orchestrators. An SLG basically belongs to a network element, and it might also belong to server resource if it runs as a VNF. (The position of SLG deployed as a VNF is shown in Section 4.2.)

The information model used in this architecture is described in information model document ([I-D.qiang-coms-netslicing-information-model]).

4.2. Position of SLG on ETSI NFV MANO

Some SLGs and the controllers are deployed and run on NSs as VNFs. An arechitecture for managing lifecycle of VNFs is under standardization in ETS NFV MANO.

The mapping of SLG as a VM into ETSI NFV MANO architecture is described in Figure 4. In some cases, SLGs are deployed with containor. VNFs are parts of NS compositions and NFV orchestrator would be controlled by upper control entities such as resource orchestrator.

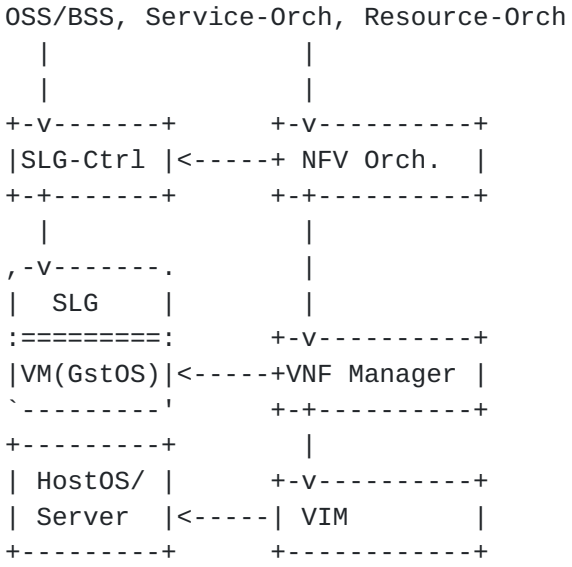

Figure 4: Position of SLG as a VM on ETSI NFV MANO

5. Requirements for SLG

An SLG is basically a component in the data plane and has the roles of data packet processing. Moreover, it is required to have functions for control/management processes such as connecting to underlay networks or managing NSs.

Furthermore, an SLG might be required to support handling services provided on NSs in addition to controlling of NS because an SLG is an edge node on an E2E-NS.

In this section, we describe the requirements for an SLG in terms of the following aspects and their interworkings.

1. Data plane for NSs as infrastructure

2. Control/management plane for NSs as infrastructure

3. Data plane for services on NSs

4. Control/management plane for services on NSs

5.1. Management of NS as Infrastructure

5.1.1. Data Plane Aspect

5.1.1.1. Identification/Classification

SLGs at the edge of E2E-NSs MUST have the capability to identify and classify data packets, and assign them to the appropriate E2E-NS. This requirement varies depending on the location.

Fixed Access: An SLG MUST identify and classify data packet with access point, including CPE or WiFi-AP, or subscriber ID such as VLAN-ID. Moreover, in some services, an SLG should identify and classify data packets based on user device or application used in the communication.

Mobile Access: An SLG MUST identify and classify data packet with subscriber-ID such as IMSI, radio-wave bandwidth, or identifier of tunnels. Moreover, in some services, an SLG should identify and classify data packets based on application used in the communication or location of the user equipment (UE).

Between NS subnets: An SLG MUST identify and classify data packet based on the tunnel-ID or virtual routing and forwarding (VRF) that received the packets. If specific slice identifier such as a

value mapped in the metadata field of the IP header is used; an SLG should identify and classify data packets with the ID.

5.1.1.2. Transporting/Forwarding

SLGs MUST provide functions for transport data packets depending on the specifications of the underlay networks.

Encapsulation/Decapsulation/Tagging: In network slicing, duplication of IP addresses of user packets between NSs MUST be accepted, thus, using techniques that enable separation of a network logically is preferred. In short, some tunnel protocols or tagging approaches should be used as transport of NSs. For this reason, SLG MUST support encapsulation or tagging of data packets based on the specification of the underlay network. Also, SLG MUST support the packets' decapsulation or untagging. Examples of tunnel protocols and tags that can be used for creating NSs on L2/L3 segments are described below.

L2 Segment: VLAN, MPLS, Segment Routing MPLS (SR-MPLS), PPPoE, etc.

L3 Segment: GRE, L2TP, GTP-U, VxLAN, IPv6 Segment Routing (SRv6), etc.

VxLAN, SR-MPLS, and SRv6 are described in their specification documents ([RFC7348], [I-D.ietf-spring-segment-routing-mpls], and [I-D.ietf-6man-segment-routing-header]).

Translation of Encapsulation/Tagging Form: SLG MUST support to translate tunnel header or tag of received packets to the appropriate tunnel header or tag when it forwards data packets to the next NS subnet that has different transport capability.

Distribution of Traffic: Some NSs have multiple route between the same end points within the same NS subnet because of traffic engineering, switching to a redundant path, or other reasons, and SLG MAY forward data packets with the appropriate route based on some trigger information. An example of the overview of this requirement is shown in Figure 5. In this figure, there are two routes, main and sub, between SLGs, and an SLG switches forwarding route depending on the network situation such as congestion occurrence on the current route.

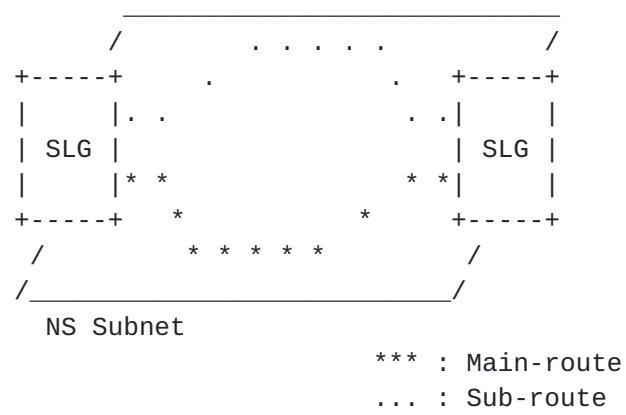

Figure 5: An example of traffic distribution by SLG

5.1.1.3. Isolation between NSs

In NSaaS, isolation control is required for avoiding an NS being affect by other NSs. Traffic engineering or QoS control is ones of the most fundamental approaches to prevent disturbances between NSs.

Traffic Shaping/Policing: An SLG MUST execute traffic shaping and policing at its egress and ingress ports to avoid an NS using excessive traffic bandwidth.

Quality of service (QoS) Control: If there is an order of priority between NSs on the same underlay infrastructure, an SLG should remark the appropriate QoS parameter of the outer-most header of each packet following the preconfigured setting and provide packet scheduling based on the QoS parameter for providing priority control. The field that SLG refers may vary depending on the specification of the underlay network. For example, COS value is remarked in L2 segments; on the other hand, DSCP value is remarked in L3 segments.

5.1.1.4. Service Chaining as Infrastructural Mechanism(*Optional)

If an SLG is composed of a combination of several components, a service chaining mechanism is required to make them work together and achieve SLG functionality.

Moreover, some NSs may traverse NFVs such as firewalls or cache servers for providing value-added services to their users. In such cases, SLG might be required to support service chaining mechanisms, such as handling of network service header (NSH) defined in [RFC8300]. If an NS includes the service chaining architecture defined in [RFC7665], some SLG would be required to support following

functions; classifier(CF), service function forwarder (SFF), and inter boundary node(IBN). (Details of CF, SFF and IBN are described in SFC documents; [RFC7665], [I-D.ietf-sfc-hierarchical].)

5.1.2. Control/Management Planes Aspects

5.1.2.1. Interfaces to Controllers or Operation Systems

SLG MUST have interface to its controller or operation systems for set parameters related to the data plane functions described in Section 5.1.1. In addition, an SLG at the edges of E2E-NSs MUST have interfaces to authentication servers.

5.1.2.2. Address Resolution/Routing

An SLG MUST support address resolution or routing mechanisms to connect to underlay network elements including routers or L2 switches.

5.1.2.3. Authentication Authorization Accounting (AAA)

For preventing entry of irregular traffic to NSs, an SLG at the edge of E2E-NS MUST support AAA mechanism for incoming traffic. Also, when an SLG connects to another SLG in other administrative domain, SLGs should have a mechanism to confirm that the connection is established with the regular processes. For example, an SLG is required to support authentication of the opponent SLG with key information indicated from higher-level operation systems.

5.1.2.4. Operation Administration and Maintenance(OAM)

In management of NSs, OAM or monitoring mechanisms for both underlay and overlay networks is required for SLGs. For an underlay network, an SLG MUST have OAM functions to confirm connectivity to interconnect equipment. For an overlay network, an SLG MUST have OAM functions to confirm connectivity to the some node on the same NS, and measure the traffic amount of flowing packets on each NS.

5.2. Management of Services on NS (*Optional)

5.2.1. Data Plane Aspect

5.2.1.1. Identification/Classification

In NSaaS, some NS tenants may need delivery of an individual service to each user, device, or application on the same NS. For such service deliveries, an SLG might be required to identify and classify user traffic based on some information such as subscriber ID or

payload of data packets. Also, an SLG should be controllable from the NS tenant.

5.2.1.2. QoS Control

An NS accommodates several communication devices and SLGs might be required to have fair queueing mechanisms for maintaining service quality of each user. Also, different types of service traffic that have different priorities might coexist on an NS. For example, some NS providers might provide telephone and internet access services to their users with an NS. In such cases, SLG might be required to provide QoS control mechanisms for enforcing priority control based on service priorities.

These QoS controls are executed depending on the information of inner packets and are independent of isolation mechanisms as infrastructure. An SLG might be required to have a hierarchical QoS control mechanism in case that both QoS controls for services over NSs and isolation between NSs are required.

5.2.1.3. Steering/Service Chaining(Cooperation with VNFs)

SLG might be required to support steering or service chaining function for conveying data packets to the appropriate network functions deployed on an NS based on the classification result and user's contract information.

5.2.2. Control/Management Planes Aspects

5.2.2.1. Interfaces to Service Management Systems

An SLG might have interfaces to controllers for managing user policies on each NS. Some controllers might be deployed on the same NS. If some controllers are located at external networks, they might require SLGs to have APIs.

5.2.2.2. Collection of Telemetry information

In an NSaaS, collection of telemetry information of each NS might be required for understanding traffic usage. Thus, an SLG might be required to support to collect and report telemetry information of connected NSs.

6. Deployment of SLG

This section describes considerations related with deployment of SLGs.

6.1. Examples of Components Required to Maintain SLG Functions

For providing E2E-NSs on existing network infrastructures, some components located at boundaries of domains are required to have the same set of functionality as an SLG. Examples of such components in each domain type are described below.

Fixed Network: CPE/HGW, Service Edge, Gateway Router, etc.

Mobile Network: User Equipment, Radio-AP, eNodeB, S/P-GW ([LTE-Specs]), etc.

Data Center: Gateway Router, L2 switch, ToR switch, Server, etc.

6.2. SLG Types Depending on Locations on NS

There are mainly three types of SLG for creating E2E-NS across multiple administrative domains. The requirements of each SLG type are listed in Appendix A.

6.2.1. Edge SLG(E-SLG)

This is located at an edge of an E2E-NS, and supports identification, classification and authentication of user traffic in addition to fundamental SLG functions, such as transport and isolation. Also, it might be required to have capabilities for services delivered on an NS.

6.2.2. Inter-Subnet SLG(IS-SLG)

This is located between NS subnets within a single administrative domain and has only fundamental functions. It is not necessarily required if a common transport mechanism in all domains is used.

6.2.3. Inter-Domain SLG(ID-SLG)

This is located between NS subnets established on different domains. It supports authentication for connecting to the opponent SLG in addition to fundamental functions.

6.3. Horizontal Connection

The connection form of an SLG varies depending on which type it is. Examples of horizontal connection forms of each SLG type are described below.

E-SLG: An E-SLG accommodates several hosts and NS subnets. This has a forwarding table of end hosts and insert their packets to the

appropriate NS subnet. An overview of this connection is shown in Figure 6.

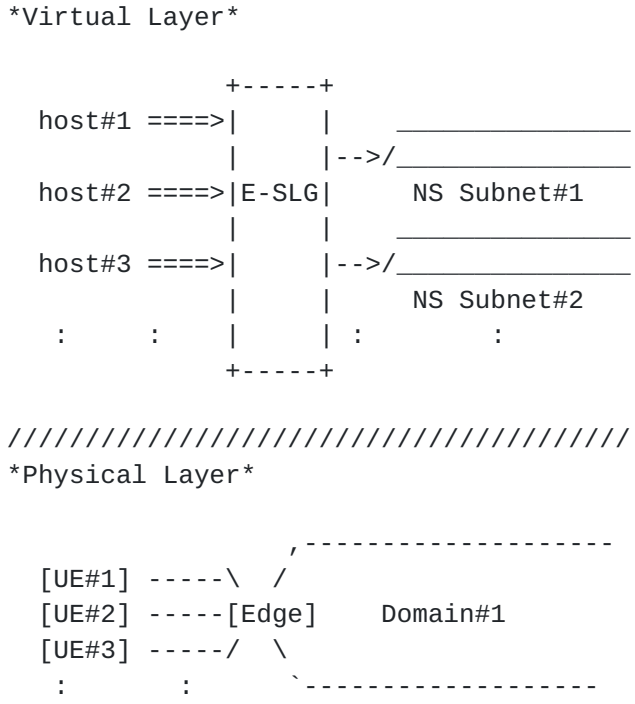

Figure 6: Overview of horizontal connection of E-SLG

IS-SLG: An IS-SLG has the role of mediator between NS subnets and passes packets received from an NS subnet to the next one. If transport methods used in each domain are different, the IS-SLG translate packet form to the appropriate one. An overview of this connection is shown in Figure 7.

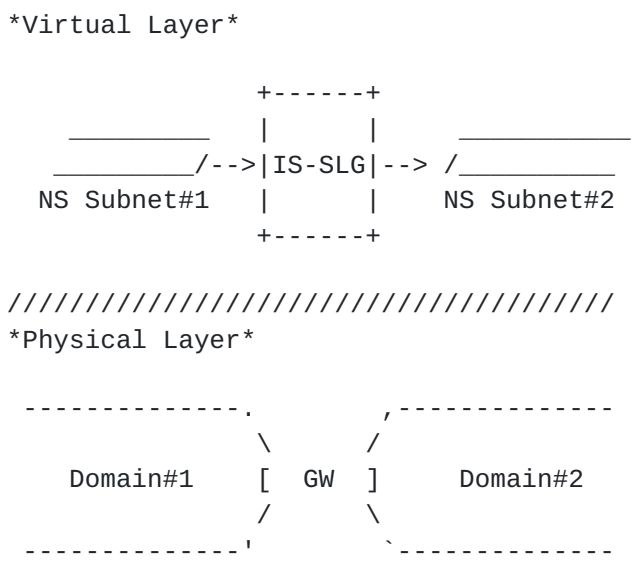

Figure 7: Overview of horizontal connection of IS-SLG

ID-SLG: An ID-SLG passes data packets to another ID-SLG located on a different administrative domain. Some tunnel established between them in advance may be used for the passing of packets. An overview of this connection is shown in Figure 8.

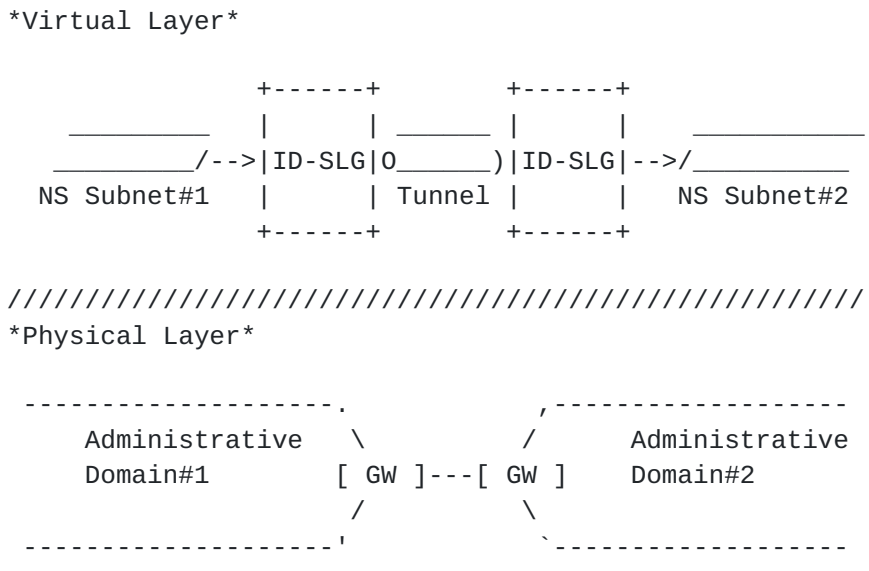

Figure 8: Overview of horizontal connection of ID-SLG

6.4. Vertical Connection

There are two patterns of vertical connection of SLGs in the middle of E2E-NSs. The first pattern is that the SLGs accommodate only a set of NS subnets, which are composition of the same E2E-NS. In this pattern, such SLGs are not required to support NS subnet selection, however, establishment of a new SLG is required when a new E2E-NS is created. This might causes extra overheads because of deploying many SLGs.

The other pattern is that such SLGs are acceptable to accommodate multiple NS subnets from each domain. In this pattern, SLGs are support NS subnet selection. On the other hand, this pattern can restrain the number of SLGs. Also, it is easy to provide transit of data packets from an NS subnet to other subnet on the same domain.

The overviews of these patterns are shown in Figure 9 and Figure 10.

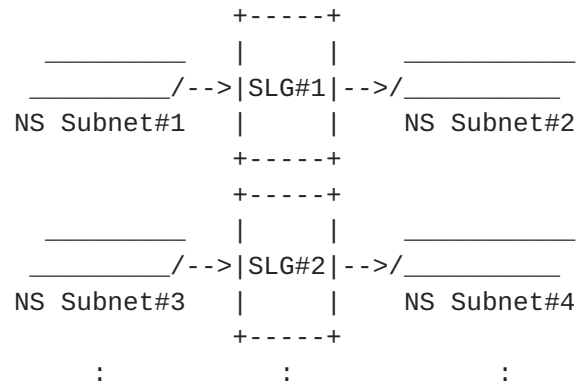

Figure 9: Overview of vertical connection of SLG: Separated Pattern

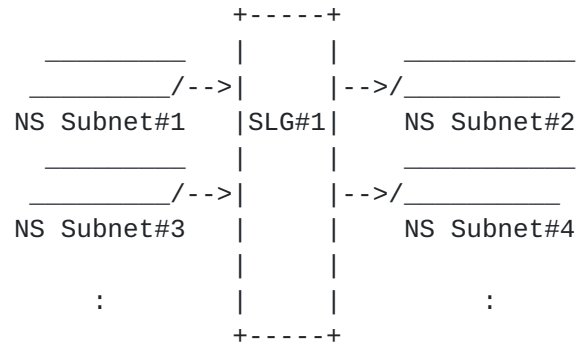

Figure 10: Overview of vertical connection of SLG: Shared Pattern

6.5. Software vs. Hardware

An SLG can be created as either a software or hardware function. NSs are virtual networks created depending on requests from external NS tenants, and thus software would be more compatible with usage for NSs in terms of flexibility or manageability. Moreover, it enables to increase or decrease for each function if SLG is composed of combination of several components. However, it is difficult to provide high performance or sufficient throughput for carrier-grade networks with software function. In addition, it would be difficult to implement sufficient QoS control mechanisms with general servers, because they requires special hardware structures.

On the other hand, hardware appliances are able to provide high throughput compared with software. However, they are inflexible in terms of provisioning.

From the above considerations, operators should prepare SLG in appropriate ways depending on their usages or locations.

7. Interconnection between NS subnets

SLG provides interconnectivity between NS subnets. The concept and fundamental framework including the related NS information model are described in subnets interconnection document ([I-D.defoy-coms-subnet-interconnection]).

This section is focused on interconnection between NS subnets established on different administrative domains, and describes considerations related to this condition.

7.1. Pre-arrangement of transport protocols

For interconnection between different administrative NS subnets, pre-arrangement of the transport protocol, which is used to connect between SLGs is required. Orchestration systems indicate the protocol and configuration to each SLG.

7.2. Quality Assurance between SLGs

In addition to establishing connection, quality control of communication is important. SLGs of egress side should execute traffic shaping to prevent some NSs from excessively occupying the link between SLGs. Moreover, some SLGs are connected to several other SLGs that are deployed on the different locations. Therefore SLGs of the ingress side should execute traffic policing to avoid excessive inflow of traffic into some NSs. The parameters for these controls are pre-configured by orchestration systems.

The above approaches are ones of the simplest ways to provide quality assurance of inter-administrative subnets. If there is stricter isolation request, more considerations would be required.

7.3. Secure Interconnection

For connecting networks of different administrators, secure interconnection schemes are required. Especially, in an NSaaS, networks might be connected to several networks, and schemes for ensuring secure connectivity would be more important.

SLGs confirm whether the opponent SLG is regular when it requests to connect, and reject the request if the SLG is not regular. In some cases, SLGs might be confirm whether the inner packets received from the other SLGs are sent from regular users.

8. Security Considerations

Requirements and considerations for SLG related to security are described in Section 5 and Section 7.

9. IANA Considerations

This memo includes no request to IANA.

10. Acknowledgement

The authors would like to thank Li Qiang for her kind review and valuable feedback.

11. Informative References

[I-D.defoy-coms-subnet-interconnection]
Foy, X., Rahman, A., Galis, A., kiran.makhijani@huawei.com, k., and L. Qiang, "Interconnecting (or Stitching) Network Slice Subnets", draft-defoy-coms-subnet-interconnection-01 (work in progress), October 2017.

[I-D.ietf-6man-segment-routing-header]
Previdi, S., Filsfils, C., Raza, K., Dukes, D., Leddy, J., Field, B., daniel.voyer@bell.ca, d., daniel.bernier@bell.ca, d., Matsushima, S., Leung, I., Linkova, J., Aries, E., Kosugi, T., Vyncke, E., Lebrun, D., Steinberg, D., and R. Raszuk, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-08 (work in progress), January 2018.

[I-D.ietf-sfc-hierarchical]
Dolson, D., Homma, S., Lopez, D., and M. Boucadair, "Hierarchical Service Function Chaining (hSFC)", draft-ietf-sfc-hierarchical-05 (work in progress), November 2017.

[I-D.ietf-spring-segment-routing-mpls]
Filsfils, C., Previdi, S., Bashandy, A., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with MPLS data plane", draft-ietf-spring-segment-routing-mpls-11 (work in progress), October 2017.

[I-D.netslices-usecases]
kiran.makhijani@huawei.com, k., Qin, J., Ravindran, R., Geng, L., Qiang, L., Peng, S., Foy, X., Rahman, A., Galis, A., and G. Fioccola, "Network Slicing Use Cases: Network Customization and Differentiated Services", draft-netslices-usecases-02 (work in progress), October 2017.

[I-D.qiang-coms-netslicing-information-model]
Qiang, L., Galis, A., 67, 4., kiran.makhijani@huawei.com, k., Martinez-Julia, P., Flinck, H., and X. Foy, "Technology Independent Information Model for Network Slicing", draft-qiang-coms-netslicing-information-model-01 (work in progress), October 2017.

[LTE-Specs]
3rd Generation Partnership Project (3GPP), "3GPP TS 36.300", December 2007, <http://www.qtc.jp/3GPP/Specs/36300-830.pdf>.

[NFV-Architectural-Framework]
Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG), "Network Functions Virtualisation (NFV); Architectural Framework", December 2014, <http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf>.

[OSM-White-Paper]
ETSI, "OSM White Paper", October 2016, <https://osm.etsi.org/images/OSM-Whitepaper-TechContent-ReleaseONE-FINAL.pdf>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

Appendix A. Requirements for each SLG Type

The requirements for each SLG type are listed in Figure 11.

	E-SLG	IS-SLG	ID-SLG	Reference
*Data-Plane of NS as Infrastructure				
Identification/Classification	M	O	O	Section 5.1.1.1.
Transport/Forwarding	M	O	M	Section 5.1.1.2.
Isolation	M	M	M	Section 5.1.1.3.
Service Chain	O	O	O	Section 5.1.1.4.
*Control/Management-Plane of NS as Infrastructure				
IF to Ctrl/OpS	M	M	M	Section 5.1.2.1.
Addr Resolution/Routing	M	M	M	Section 5.1.2.2.
AAA	M	-	M	Section 5.1.2.3.
OAM	M	M	M	Section 5.1.2.4.
*Data-Plane for Service on NS				
Identification/Classification	O	-	O	Section 5.2.1.1.
QoS Control	O	O	O	Section 5.2.1.2.
Steering/Service Chain	O	-	O	Section 5.2.1.3.
*Control/Management-Plane for Service on NS				
IF to Service Manager	O	O	O	Section 5.2.2.1.
Telemetory	O	O	O	Section 5.2.2.2.

M: Mandatry, O: Optional, - : Not Required

Figure 11: List of Requirements for each SLG

Authors' Addresses

Shunsuke Homma
NTT, Corp.
3-9-11, Midori-cho
Musashino-shi, Tokyo 180-8585
Japan

Email: homma.shunsuke@lab.ntt.co.jp

Xavier de Foy
InterDigital Inc.
1000 Sherbrooke West
Montreal
Canada

Email: Xavier.Defoy@InterDigital.com

Alex Galis
University College London
Torrington Place
London WC1E 7JE
United Kingdom

Email: a.galis@ucl.ac.uk