none
Internet-Draft
Intended status: Informational
Expires: December 4, 2017

L. Qiang, Ed.
Huawei
P. Martinez-Julia
NICT
L. Geng
China Mobile
J. Dong
K. Makhijan
Huawei
A. Galis
University College London
S. Hares
Hickory Hill Consulting
S. Kuklinski
Orange

June 2, 2017

Gap Analysis for Network Slicing
draft-qiang-netslices-gap-analysis-00

Abstract

This document presents network slicing differentiation from the non-partition network or from simply partition of connectivity resources. It lists 15 standardization gaps related to 6 key requirements for network slicing. It also presents an analysis of existing related work and other potential solutions on network slicing.

This gap analysis document aims to provide a basis for future works in network slicing.

Table of Contents

1. Introduction

Network slicing is an approach of flexible isolation of network resources and functions for dedicated services, providing certain level of customization and quality guarantee. It establishes customized dedicated network upon a common infrastructure for vertical industries with flexible design of functions, different performance requirements, system isolation and OAM tools.

Several SDOs have investigated the network slicing. Open Network Foundation (ONF) has developed a recommendation on applying SDN architecture to Network Slicing [ONF-2016]. 3GPP is studying the network slicing focusing on radio networks and core networks and it issued an architecture for Next Generation System [NGS-3GPP-2016] September 2016. ITU-T IMT 2020 and ITU-T SG13 is studying network softwarization inclusive of network slicing and it has issues a number of recommendations: Gap Analysis [IMT2020-2015], Network Softwarization [IMT2020-2016], Terms [IMT2020-2016bis]. NGMN is studying the network slicing from the mobile network point of view [NGMN-2016]. Although other SDOs have done a lot of work, potential requirements especially in the transmission network and end-to-end enabling need to be investigated in order to elicit and identify the technical gaps in IETF for network-slice enabled networks.

In order to establish a network slice that meets various customer's demands, the infrastructure owner needs to understand how these demands map with the available network resources and accessible capabilities. This also requires end-to-end coverage and inter-domain operation or negotiation between different network segments.

Different levels of system abstraction are essential enablers for network slicing. For instance, the infrastructure owner needs to understand performance metrics such as bandwidth, latency, isolation requirements, and traffic forwarding restrictions from slice tenants. Furthermore, these requirements are expected to map with the capabilities of a specific network slice with the nature of flexibility, agility and certain level of customization. Slice tenants do not have to worry about what techniques the slice provider has adopted to meet their specific requirements. Meanwhile, the slice provider provides customized OAM to the tenants under provisioning. Slicing OAM approach is a fundamental capability to guarantee stable, effective and reliable services for the vertical industries. It is also expected to be capable of operations with customized granularity levels that provides robust management flexibilities.

This document presents the identified key requirements and investigate potential technical gaps accordingly. To assist understanding of this document, Section 2 outlines the terminology. Section 3 introduces overall requirements of network slicing. Section 4~9 illustrates end-to-end considerations, performance guarantee, system level abstractions and OAM concerns. Section 10 summarizes the identified gaps.

2. Terminology and Abbreviation

- CNC: customer network controller
- MDSC: multi-domain service coordinator, could be a hierarchical one
- PNC: physical network controller, each transport network domain has a PNC
- VN: virtual network
- PCC: path computation client, the physical device (normally is the ingress device of an LSP) which requests for a path computation service
- TN domain: transmission network domain
- NSI: network slice instance

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.

All of the network slicing related words used in this document are to interpreted as described in [NS-Framework].

3. Overall Requirements in Network Slicing

This section introduces 6 key requirements of network slicing devried from [NS-UseCase] as shown in Table 1. These 6 requirements are organized according to a general network slice working process as shown in Figure 1: specify the network slicing resource (Req.1); construct a performance guaranteed end-to-end network slice (Req.2 and Req.3); necessary abstraction for the constructed end-to-end network slice (Req. 4); Identify the network slice (Req. 5); and provide OAM operations (Req. 6).

```
   +----------------------------------------------------------+
   |      network slice management and orchestration          <-----+
   +----------------------^-------^---------------------------+     |
                          |       |                             resource
                          |  OAM  |                          specification
                          |       |                                 |
 +------------------------v-------+------------------------------+  |
 |            abstracted network slice instance 1                |  |
 +--------------------------------+------------------------------+  |
                                  |                                 |
 +--------------------------------v------------------------------+  |
 |            abstracted network slice instance 2                |  |
 +---------------------------------------------------------------+  |
                                                                    |
                                                                    |
  +---------+              +---------+              +---------+     |
  |NS-Domain| cross-domain |NS-Domain| cross-domain |NS-Domain<-----+
  | Manager <--------------> Manager <--------------> Manager |
  +---------+  negotiation +---------+  negotiation +---------+

  +---------+              +---------+              +---------+
  |         |              |         |              |         |
+-+---------+--------------+---------+--------------+---------+-+
|                  network slice instance 1                     <---+
+-+---------+--------------+---------+--------------+---------+-+   |
  | Domain 1|              | Domain 2|              | Domain 3|  isolation
+-+---------+--------------+---------+--------------+---------+-+   |
|                  network slice instance 2                     <---+
+-+---------+--------------+---------+--------------+---------+-+
  |         |              |         |              |         |
  +---------+              +---------+              +---------+
```

Figure 1: Illustration of Key Requirements

Requirements Illustrated in NS UseCase	Extracted KEY Requirements
1) Resource Reservation; 2) Transparency; 3) Multi-Access Knowledge; 4) Multi-Dimensional Service Vertical	Req 1. Network Slicing Resource Specification
5) Multi-Domain Coordination; 6) Automated Network Slice Management; 7) Resource Assurance	Req.2 Cross-Network Segment & Cross-Domain Negotiation
8) Performance Isolation; 9) Secure Isolation; 10) Operation Isolation; 11) Reliability	Req.3 Guaranteed Slice Performance and Isolation
12) Abstraction; 13) Subnet Concept; 14) Virtualization of Network Functions	Req.4 Network Slicing Domain-Abstraction
15) Agile Resource Adjustment; 16) Function Sharing; 17) Slice Identification	Req.5 Slice Identification
18) Independent per slice management plane	Req.6 OAM Operations with Customized Granularity

Table 1: Requirement Association

o Req.1 Network Slicing Resource Specification: The management system of both underlying resources/network functions and overlying resource/network functions provided by operator, regardless of being automated, human-guided, or human-operated, needs to manage the description of the resources/network functions it has "in stock" and "under its control". The objective for those systems to have such information is that the resources will form an important part of their business, and thus they must know "what they have" at every moment, so that, for instance, they are able to "deliver" the requests without incurring into any overutilization of their resources. Since the technology-specific actions will be taken accordingly for delivered requests, the way resources are described and specified must be homogeneous and compatible, even among separated domains, providers, and "slicing" platforms.

o Req.2 Cross-Network Segment & Cross-Domain Negotiation: Network users in relation to network slicing are entities that operate

some set of physical, logical, virtual, or, in general, abstracted resources that are not owned directly by them but provided by operators. From terminal to server (or other terminal), an end-to-end network slice may involve several network segments (e.g., RAN, TN, and CN) that owned by different operators. Each segment may be further divided into different administrative domains. That is an end-to-end slice is a logical entity composed by multiple separated components, and the cross-network segment & cross-domain negotiation is a way to integrate compoments.

- Req.3 Guaranteed Slice Performance and Isolation: In order to enable the safe, secure, performance guaranteed service for multi-tenancy on the common physical networks, the isolation in each of the Data /Control /Management /Service planes are needed in network slicing. In general, there are two tiers isolations: Soft and hard isolations. VPN, NVO3, etc. are typical soft isolation technologies, slices isolated through these technologies still may compete for underlying resources in extremes. For some critical services, hard isolation such as FlexE, OTN, etc. are necessary.

- Req.4 Network Slicing Domain-Abstraction: To complement the previous requirement (i.e.,Req.3), it is important for network slices to be aware but independent of the domain to which they belong. This implies that they are abstracted from any specific domain, so operators can change their behavior without requiring to reconfigure all individual parts and pieces of the overall system.

- Req.5 Slice Identification: Identify the network slices and discovery the corresponding slice. This requirement is associated with privacy and security characteristics of network slicing. The major functionalities may include identifier (ID) assignment, ID certification, ID resolution, etc. In order to implement slice discovery and identification, the negotiation, monitoring and other end-to-end orchestration operations are also required.

- Req.6 OAM Operations with Customized Granularity: Different network slice users (operators, customers) will have different requirements. On one end of the spectrum we have those operators that will require a finalized service that they will simply commercialize. On the other end we have those operators that need (or want) to fine-tune all the low-level aspects of the network resources that form their system or service. Moreover, in the middle there is plenty of room for variations. Therefore, the underlying network layers must offer different levels of granularity for the management of their resources, that the upper layer operators can choose according to their needs and objectives.

4. Network Slicing Resource Specification

4.1. Description

Network Slicing Resource Specification (NSRS) is meant to specify the network slicing resources and capture requirements of services, customers, and peer networks to characterize the service expected to be delivered by a network. These requirements include (non-exhaustive): reachability scope (e.g., limited scope, Internet-wide), direction, bandwidth requirements, performance metrics (e.g., one-way delay [RFC2679], loss [RFC2680], or one-way delay variation [RFC3393]), protection and high-availability guidelines (e.g., restoration in less than 50 ms, 100 ms, or 1 second), traffic isolation constraints, and flow identification. NSRS is used by a network provider to decide whether existing network slices can be reused or (some of them) even combined, or if another network slice instance is needed for a given service.

Technology-specific actions are then derived from the technology-agnostic requirements depicted in an NSRS. Such actions include configuration tasks and operational procedures.

A standard definition of NSRS is needed to facilitate the dynamic/automated negotiation procedure of NSRS parameters, but also to homogenize the processing of service requirements.

4.2. Related Work in IETF

4.2.1. NSRS Templates

As rightfully discussed in [I-D.wu-opsawg-service-model-explained], the IETF has already published several YANG data models that are used to model monolithic functions as well as very few services (e.g., L2SM, L3SM, EVPN). These models may be used in the context of network slicing if corresponding technologies are required for a given network slice, but none of them can be used to model an NSRS.

[RFC7297] describes the Connectivity Provisioning Profile (CPP) and proposes a CPP template to capture connectivity requirements to be met within a service delivery context . Such a generic CPP template is meant to

- o facilitate the automation of the service negotiation and activation procedures, thus accelerating service provisioning;

- o set (traffic) objectives of Traffic Engineering functions and service management functions;

o improve service and network management systems with 'decision-making' capabilities based upon negotiated/offered CPPs.

[RFC7297] may be considered as a candidate specification for NSRS. Releasing a RFC7297-bis to take into account specific requirements from network slicing is needed. Since [RFC7297] may not be implemented by all providers, the [SLA-Exchange] can be used to negotiate the SLAs and report on SLA events. Further analysis is needed to provide a complete package.

4.2.2. Building NSRS from Protocol Independent Traffic Engineering Models

The NSRS requirement for reachability, direction, bandwidth requirements, performance metrics, traffic isolation constraints, and flow identification can be built utilizing protocol which can perform operations (read, write, notification, actions (aka rpcs)) on a yang service layer that supports these traffic engineer and resource definition at the service layers. The network slicing service data model can extend existing work in the TEAS and I2RS working group for protocol-independent topology models. These models support configuration or the dynamic datastores defined in [NMDA] which will be abbreviated as NMDA in this section. This section provides the detail on how the NSRS can be built from these models and the RESTCONF protocol.

4.2.2.1. Basic Topology Model

The basic topology model is defined in [I2RS-Yang] in the service layer as shown in Figure 2. This topology model is protocol independent and can be utilized as a configuration data model or a dynamic datastores model. The configuration data model must abide by the configuration persistence and referential requirements. The dynamic datastores do not need to abide by the same requirements. I2RS is defining a dynamic datastores reference model for a data store which ephemeral. The network slices may want to use configuration, ephemeral datastores, or define a third type of dynamic datastores. The I2RS WG provides a place to collaborate this work on the dynamic datastores.

```
                         +-------------------------------+
                        /           [X1]      "Service" /
                       /           / *  \        TEAS  /
                      /           /   *  \            /
                     /           /     *  \          /
                    /        [X2]       *  [X3]     /
                   +----------*----------*---*-----+
                              *           *  *
                              *            * *
                        +-----*-------------**----------+
                       /      *              *    "L3" /
                      /       *              *        /
                     /      [Y1]           [Y2]      /
                    /         *              *      /
                   /          *             **     /
                  +-----------*------------*-*----+
                              *           *  *
                              *          *   *
                       +------*---------*----*---------+
                      /     [Z1]       *   [Z2]       /
                     /                *              /
                    /                *              /
                   /                *              /
                  /               [Z3]  "Optical" /
                 +-------------------------------+
```

Figure 2: Topology Hierarchy (Stack) Example

4.2.2.2. TEAS Model Utilization of Basic Topology Model

The TEAS topology model [TE-Yang] provides a general description of a Traffic engineering model that provides:

- o abstract topologies with TE constraints (bandwidth, delay metrics, links to lower layers, some traffic isolation constraints, and some link identifiers);

- o templates for links or resources;

- o functionality to read, write, notification, and rpcs.

Options that need to be consider are:

Augmenting TEAS - The TEAS models provide substantial traffic engineering. It was envisioned in the early topology model that a service resource model would be part of the service layer. This work was delayed until the maturation of the service requirements from L2VPN, L3VPN, and EVPN plus the maturation of resource

requirements from 5G. Network slicing provides a good application use case for this work.

Why not Augment TEAS - If the TEAS models make a fundamental assumption that prohibits the use of the model within the network-slicing. [Research and discussion are needed with TEAS on this subject]

Dynamic models to combine TEAS models for network-slicing - The network slicing controller operating across domains may wish to create a multiple-domain data model based on the service layer data models exposed by different providers. These service models would not need to be configured, but only learned as providers exchange data with one another. The rules for combining these models could be defined as part of the dynamic datastore for network-slicing.

Protocol within a domain - The RESTCONF and NETCONf protocol can support read, write, notification and actions (rpcs) within a domain.

Protocol across domains: The RESTCONF protocol currently supports Configuration protocols and 90% of the dynamic datastores. The RESTCONF protocol is being enhanced to support the push of telemetry messages. The RESTCONF protocol could be used to exchange a specific Yang network-slicing service-layer topology (TE and Resources) and for the I2NSF security capabilities between domains.

If a multicast of telemetry data is required between domains, then the push model for telemetry information or the IPFIX protocol may be utilized. [More details are needed on the multicast need]

5. Cross-Network Segment & Cross-Domain Negotiation

5.1. Description

The cross-network segment & cross-domain negotiation requirement includes the following aspects:

- o Network slice resource/functions negotiation: for example, a tenant requests for a network slice with at most 10 ms latency from terminal to server. Different network segments/domains should negotiate to reach an agreement such as RAN provides at most 2 ms service, TN domain I provides at most 4ms service, TN domain II provides at most 2 ms service and CN provides at most 2 ms service;

- o Configuration information negotiation: for example, for a given TN domain, the configuration information such as VLAN ID, remote IP address, physical port ID, etc. need to be negotiated with other TN domains;

- o Other negotiations: for example, RAN (or other access network) needs to notify TN about the information of new attachment point when user moves.

From terminal to server, an end-to-end network slice will involve different network segments (e.g., RAN, TN and CN). Even within the same network segment, there will always involve multiple domains due to geographic isolation, administrative isolation and other reasons. There are two ways to enable an end-to-end network slice: based on a common platform or based on cross-network segment & cross-domain negotiation.

If all of the involved network segments and domains belong to the same operator or the same operator union, the common platform solution may be work. In this case, all of the network segments and domains only need to communicate with the common platform, and follow the coordination management of this common platform. Whilst the most common case is that the involved network segments and domains belong to different operators/administrative regions, making it difficult to realize such a common platform. Consequently, the cross-network segment & cross-domain negotiation will be essential throughout the whole lifecycle of an end-to-end network slice.

5.2. Related Work in IETF

There are some related works studies the inter-operation/negotiation between different entities. This subsection will briefly review these related work to provide a basis for the gap analysis.

5.2.1. Autonomic Networking Integrated Model and Approach (ANIMA)

Autonomic Networking Integrated Model and Approach (ANIMA) WG provides a series of tools for distributed and automatic management, which includes: Generic Autonomic Signaling Protocol (GRASP) , Autonomic Networking Infrastructure (ANI), etc.

GRASP [ANIMA-GRASP] is a protocol for the negotiation between ASAs (Autonomic Service Agent). In GRASP, ASAs could be considered as "APPs" installed on a device. Different ASAs fulfill different management tasks such as parameter configuration, service delivery, etc. Based on GRASP, the same purpose ASAs that installed on different devices are able to inter-operate and negotiate with each other. Network slicing could make use of GRASP for the coordination

among devices in the underlying infrastructure layer, as well as the negotiation among different domain (or different network segment) managers. However, the security issue incurred by cross-network segment & cross-domain usage should be fixed in GRASP.

ANI [ANI] is a technical packet consisting of BootStrap (for authentication, domain certification distribution, etc.), ACP (a separate control plane), and GRASP (for control message coordination). ANI could be used to construct the management tunnel among devices in underlying infrastructure layer within a single domain. While the network slicing and cross-domain oriented extensions are necessary.

5.2.2. Abstraction and Control of Traffic Engineered Networks (ACTN)

ACTN [TEAS-ACTN] is an information model proposed by TEAS WG, which enables the multi-domain coordination in transport network. In order to enable the network slicing in transport network, portion of transport domain will need to be engineered. In particular about building a TE entity and stitching service for this entity, that is within the scope of ACTN. As an end-to-end network slicing solution, ACTN is able to provide the cross-network segment negotiation. In ACTN, each physical transport network domain is under the control of a PNC as shown in Figure 3. Based on a MDSC, multiple PNCs coordinate with each other. Although the MDSC may be a hierarchical structure, the hierarchical MDSC still could be regarded as a logical common platform. As Section 5.1 discussed, such common platform solution has a strict presumption. Thus, ACTN is not a clear E2E model. It is a multi-tier multi-service provider abstraction that heavily relies on centralization using SDN methods.

ACTN does carry out some network slicing-related work, some proposed concepts are even close to the concepts of today's network slicing, like virtual network (VN, similar concept of slice instance). ACTN enables VN based on LSP technique, different LSP tunnels correspond to different VNs. From the isolation perspective, LSP belongs to the soft-isolation category. For those critical services that have very strict isolation requirement, the soft-isolation is not enough since different VNs/network slices (i.e, LSP tunnels in ACTN) still may compete for underlying resources.

The biggest factor that prevents ACTN from being directly applied to network slicing is that, ACTN and network slicing have totally different management modes. ACTN is path-oriented (i.e., TE tunnel based), whilst network slicing is resource-oriented. Take the scenario shown in Figure 4 as an example, there are two LSPs: LSP1 (A->C->D, 20G) and LSP2 (B->C->D, 20G). If the data-rate from node A changes from 20G to 10G and B changes from 20G to 30G, both LSP1 and

LSP2 have to be reconfigured, even through path from C->D has no change. In summary,

```
                  +-------+     +-------+       +-------+
                  | CNC-A |     | CNC-B |       | CNC-C |
                  +---+---+     +---+---+       +---+---+
                      |             |               |
                      +-------\     |CMI     /------+
                               \    |       /
                          +---------+---------+
                          | (Hierarchical)MDSC |
                          +---------+---------+
                              /     |      \
                     +-------+      |MPI    +---------+
                     |              |                 |
                 +---+---+      +-------+        +----+--+
                 |  PNC  |      |  PNC  |        |  PNC  |
                 +-------+      +-------+        +-------+
```

Figure 3: A Three-tier ACTN Control Hierarchy

- o In-segment resource: ACTN only abstracts the topology and link features, it neither supports standard resource capability exposure nor facilitates distributed resource changes.

- o L2 resource negotiation: ACTN does not provide the L2 resource negotiation among devices.

- o Network perspective coordination: any change in a single tunnel requires re-computation of path on MDSC, which is expensive and not well coordinated. I.e. there is no notion of distributed negotiation of resources among different TE tunnels.

```
                  20G->10G  +---+
                 ---------->+ A +----+20G->10G
                            +---+    |
                                     +--->+---+ 40G  +---+
                                          | C +----->+ D |
                                     +--->+---+      +---+
                  20G->30G  +---+    |
                 ---------->+ B +----+20G->30G
                            +---+
```

Figure 4: An Illustration Example for Path-Oriented Management

5.2.3. Connectivity Provisioning Negotiation Protocol (CPNP)

[I-D.boucadair-connectivity-provisioning-protocol] defines the Connectivity Provisioning Negotiation Protocol (CPNP) that is meant to dynamically exchange and negotiate connectivity provisioning parameters, and other service-specific parameters, between a Customer and a Provider. CPNP is a tool that introduces automation in the service negotiation and activation procedures, thus fostering the overall service provisioning process.

CPNP runs between a Customer and a Provider carrying service orders from the Customer and respective responses from the Provider to the end of reaching a connectivity service provisioning agreement. As the services offered by the Provider are well-described, by means of the CPP template, the negotiation process is essentially a value-settlement process, where an agreement is pursued on the values of the commonly understood information items (service parameters) included in the service description template.

The protocol is transparent to the content that it carries and to the negotiation logic, at Customer and Provider sides, that manipulates the content.

The protocol aims at facilitating the execution of the negotiation logic by providing the required generic communication primitives.

CPNP can be used in the context of network slicing to request for network resources together with a set of requirements that need to be satisfied by the Provider. Such requirements are not restricted to basic IP forwarding capabilities, but may also include a characterization of a set of service functions that may be invoked.

5.3. Other Potential Solutions

5G Exchange (5GEx) [FGEx] is a 5G-PPP project which aims to enable cross-domain orchestration of services over multiple administrations or over multi-domain single administration networks. The main infrastructure considered in 5GEx is the NFV/SDN compatible software defined infrastructure, which limits the scope of network slicing to SDN based architecture.

6. Guaranteed Slice Performance and Isolation

6.1. Description

With network slicing, it is expected to enable the deployment of various services with diverse requirements independently on the common physical networks. Each network slice is characterized with

particular service requirements, which usually are expressed in the form of several key performance indicators (KPIs) such as bandwidth, latency, jitter, packet loss, etc., and different degrees of isolation. It should be noted that the requirement on isolation is not just related to guaranteed performance, for some services it is also critical to achieve the isolation in terms of network privacy, security, management and operation, etc.

It is important that the performance and isolation requirements of each network slice can always be met regardless of what is happening in any other network slices. Otherwise it is likely that some of the services would still be deployed in their dedicated networks rather than in a shared network infrastructure using network slicing. The requirements on guaranteed performance and isolation cannot simply be met with the creation of separate virtual networks, more importantly it depends on how to instantiate these virtual networks properly on the shared physical network infrastructure with appropriate resource allocation policy and mechanisms, so that the diversified performance and isolation requirements of network slices can be guaranteed in a flexible and efficient way.

6.2. Related Work in IETF

6.2.1. Virtual Private Networks

Virtual Private Networks (VPN) technologies such as L3VPN [RFC4364], L2VPN [RFC4664], EVPN [RFC7432], etc. have been widely deployed to provide different virtual networks on the common service provider networks. Although VPNs can provide logically separated routing/bridging domains between different VPN customers, essentially it is an overlay network technology with little control of the network resources, so it is challenging for VPN to meet the performance and isolation requirement of some emerging application scenarios such as industrial verticals.

6.2.2. NVO3

[NVO3-WG] defines several network encapsulations which support the network virtualization and multi-tenancy in the data center networks. Similar to the VPN technologies of service provider networks, NVO3 is also an overlay network technology, which relies on the performance characteristics provided by the IP-based underlay networks. Thus NVO3 may not meet the performance and isolation requirements of network slicing.

6.2.3. RSVP-TE

RSVP-TE [RFC3209] is the signaling protocol to establish end-to-end traffic-engineered Label Switched Paths (LSPs). It can reserve the required link bandwidth along an end-to-end path for specific network flows, which is suitable for services with particular requirement on traffic bandwidth. RSVP-TE LSPs can be used as the underlay tunnels of the VPN service connections. However, the requirement of some emerging services is not only about traffic bandwidth, but also has quite strict requirement on latency, jitter, etc. Such requirements can hardly be met with existing RSVP-TE.

6.2.4. Segment Routing

[I-D.ietf-spring-segment-routing] provides the ability to specify a traffic-engineered path by the source node of data packets, which is also known as a approach for source routing. It can provide comparable traffic-engineering features as RSVP-TE with better scalability, by eliminating the per-path state in the transit network nodes. It is therefore a candidate method of creating an NSI, mapping a packet into an NSI and specifying the passage of the packet through the resources dedicated to the NSI. Segment Routing as designed today could be used within an NSI without further modification, but its use as a method providing an NSI requires further study. With respect to performance guarantee and isolation, some further investigation may be needed to understand whether SR can provide the same or better performance characteristics as RSVP-TE without the flow state in the transit node. In addition, it is not clear whether SR-based LSPs can provide the guaranteed latency and jitter performance required by network slicing.

6.2.5. Deterministic Networking

[DETNET-WG] is working on the deterministic data paths over layer 2 and layer 3 network segments, such deterministic paths can provide identified flows with extremely low packet loss rates, low packet delay variation (jitter) and assured maximum end-to-end delivery latency. This is accomplished by dedicating network resources such as link bandwidth and buffer space to DetNet flows and/or classes of DetNet flows. DetNet also aims to provide high reliability by replicating packets along multiple paths. It is a characteristic of DetNet that it is concerned solely with worst-case values for the end-to-end latency.

The primary target of DetNet is real-time systems and as such average, mean, or typical latency values are of not protected, because they do not affect the ability of a real-time system to perform their tasks. This contrasts with a normal priority-based

queuing scheme which will give better average latency to a data flow than DetNet, but of course, the worst-case latency can be essentially unbounded. As such DetNet seems to be a useful technique that may be applied to either a complete NSI, or to components of the traffic within an NSI to address the emerging low latency requirement for real time application.

Where an NSI is created recursively, there must be a mapping between the latency requirements of the child NSI onto the latency SLA provided by the parent, which in turn must trace back to the SLA provided by the underlay.

DetNet is not currently designed with network slicing in mind. As such the mapping between an NSI and a DetNet service needs to be defined.

6.2.6. Flexible Ethernet

[FLEXE-1.0] is initially defined by Optical Internetworking Forum (OIF) as an interface technology which allows the complete decoupling of the Media Access Control layer (MAC) data rates and the standard-based Ethernet Physical layer (PHY) rates. The channelization capability of FlexE can be used to partition a FlexE interface into several independent sub-interfaces, which can be considered as a useful component for the slicing of network interfaces. Currently there is ongoing work in IETF to define the control plane framework for FlexE, which aims to identify the routing and signaling extensions needed for establishing FlexE-based end-to-end LSPs in IP/MPLS networks.

7. Network Slicing-Domain Abstraction

7.1. Traditional Network Abstraction Technologies

It is important for a network slice to be isolated from other slices and is traditionally achieved through network abstraction technologies such as virtual private networks (VPN [RFC4364]) and other overlays (VLANs, NVO3 [NVO3-WG]). VPNs essentially are private networks of enterprises by connecting remote sites. It is only the partial goal of network slice domain that determines reachability. There are two issues with VPNs:

- o An end-to-end VPN tunnel competes with other traffic in the network and end-to-end network resource policies cannot be guaranteed.

o The reachability and resource reservation protocols are not tightly integrated and often solutions require centralized PCE-P like methods.

Network slices partition the infrastructure across multiple domains. They may also share databases from provider or other slices (e.g. subscriber information).

In regards to VPN or network virtualization following gaps are identified,

o The resources allocated to a slice shall not compete with other traffic, yet have the elasticity scale on-demand.

o New service verticals in IoT or mMTC arena are sensitive to data plane or bits on wire overheads. Therefore, encapsulation in the form of labels, VLANs, VxLANs shall be optional in data path (In VPNs etc., some form of tagging is always carried).

7.2. Decoupling of Control Planes

One of the attributes of abstraction is decoupling of hardware from software for higher flexibility and support for multiple functionalities. In the context of slices the functionality may need to run different control plane protocols than in other slices. As an example, it may be just a layer 3 topology and corresponding routing resource descriptions while another slice, may be an entirely non-IP control plane. The notion of abstraction in slicing shall allow both

o Decoupling of control plane of physical network and a sliced network.

o Between two slice network instances.

Although, care must be taken in the handling of this requirement as excessive control packet processing will lead to a network node's performance degradation and it may need to speak/enable multiple control protocols.

7.3. Abstraction of Network in Network

To compose a slice across multiple domains, the details of network topology of that domain shall not be exposed at the network slice level. Furthermore,

o Inter-play of multiple technologies shall be considered and a common representation for a slice across these domains is required.

To explain by example, what this means is that a segment in a network domain can be

- o A cloud deployed, NFV enabled, chain of network functions in a virtualized 5G core.

- o A segment routing [I-D.ietf-spring-segment-routing] based IGP network transport/aggregation or slice-specific application functions.

- o A PCE [RFC4655] monitored TE-tunnel with ingress and egress points.

- o Optical, carrier Ethernet or cellular networks.

A slice instance will be a combination of some of the above technologies. It creates a compelling need for a common resource centric interface across these domains over which resources can be negotiated/allocated for end-to-end slice realization.

The network slice operator shall be able to build/visualize own forwarding graph or service chain among these segments. Inside in its network each segment assures resource association with the slice.

It is even more efficient to not expose those details to slice orchestrator in order to minimize fine-grained centralized repositories for a large scale multi-domain network.

This gap/requirement is tied to resource specification, as well as cross-domain negotiation. Each domain, processes/negotiates the resource spec with respect to a slice, coordinates with the orchestrator and returns an abstract managed object to be used by slice operator.

7.4. Forwarding/Data-plane Abstraction

A network slice data plane, may or may not follow traditional data plane tagging/labeling. However, each network element (router/ switch) still has to classify an incoming packet and associated with the slice instance for proper treatment. The corresponding forwarding rules shall not have to be programmed at per flow level as this could have adverse impact on scale of the forwarding entries in the routers. NS resource specification shall provide a uniform mapping for a vast set of virtual/logical network entry points from radio, optical, wireless and fixed networks such as ports, interfaces, labels, IP address, MAC address, wavelength lambda etc.

7.5. Notion of QoS in Network Slices

This sub-section is not meant to argue that there is a gap in QoS abstraction, but indicates that QoS abstraction is not required in network slicing. End-to-end resource awareness is a key differentiating aspect of network slicing. In traditional networks differentiated services, QoS markings, IP precedence or FEC are used to label a group or provide preferential packet treatment. It is expected that a slice has already been engineered for the service with pre-allocation of network resources. Therefore, it can be argued that these parameters have no meaning. A packet or flow in the network slice need not be marked and does not belong to a class.

8. Slice Identification

8.1. Description

Network slice instance identification is essential for network element to make local decisions on forwarding policies, QoS mechanism and etc. The performance requirements of a network slice instance can therefore been met by making the correct decision. Meanwhile, it is also important for OAM so that configuration and provisioning can be delicately performed to particular network slice instances by their identifications.

For flow identification, many existing technologies provide mature solutions. These approaches might be able to be re-used in network slicing by adding an additional layer of mapping to a network slice instance ID. The network slice instance ID further maps to a group of performance requirements and OAM profiles, based on which the network elements within the slice can make local decisions.

8.2. Related Work in IETF

With traditional IP/MPLS VPNs, the set of Route Targets configured for the VPN can be used as some sort of identifier of the VPN in the control plane, and in the data plane, the VPN service labels can be used to identify the data packets belonging to a particular VPN. NVO3 uses the Virtual Network Identifiers (VNIs) in the header of data packets to identify different overlay network tenants. However, It is not clear if the existing identifiers can meet the requirements of network slicing in terms of making local decisions on forwarding policy, QoS and OAM mechanisms, etc.

9. OAM Operation with Customized Granularity

9.1. Description

In accordance with [RFC6291], OAM is used to denote the following:

- o Operations: refer to activities that are undertaken to keep the network and the services it deliver up and running. It includes monitoring the underlying resources and identifying problems.

- o Administration: refer to activities to keep track of resources within the network and how they are used.

- o Maintenance: refer to activities to facilitate repairs and upgrades. Maintenance also involves corrective and preventive measures to make the managed network run more effectively, e.g., adjusting configuration and parameters.

As per [RFC6291], network slicing provisioning operations are not considered as part of OAM. Provisioning operations are discussed in other sections.

Maintaining automatically-provisioned slices within a network raises the following requirements:

- o Ability to run OAM activities on a provider's customized granularity level. In other words, ability to run OAM activities at any level of granularity that a service provider see fit. In particular:

  * An operator must be able to execute OAM tasks on a per slice basis.

  * These tasks can cover the "whole" slice within a domain or a portion of that slice (for troubleshooting purposes, for example).

  * For example, OAM tasks can consist in tracing resources that are bound to a given slice, tracing resources that are invoked when forwarding a given flow bound to a given network slice, assessing whether flow isolation characteristics are in conformance with the NS Resource Specification, or assessing the compliance of the allocated slice resource against flow/ customer requirements.

  * An operator must be able to enable differentiated failure detect and repair features for a specific/subset of network slices. For example, a given slice may require fast detect and

repair mechanisms (e.g., as a function of the nature of the traffic (pattern) forwarded through the NS), while others may not be engineered with such means.

* When a given slice is shared among multiple services/customers, an operator must be able to execute (per-slice) OAM tasks for a particular service or customer.

o Ability to automatically discover the underlying service functions and the slices they are involved in or they belong to.

o Ability to dynamically discover the set of network slicing that are enabled within a network. Such dynamic discovery capability facilitates the detection of any mismatch between the view maintained by the control plane and the actual network configuration. When mismatches are detected, corrective actions must be undertaken accordingly.

9.2. Related Work in IETF

9.2.1. Overview of OAM tools

The reader may refer to [RFC7276] for an overview about available OAM tools. These technology-specific tools can be reused in the context of network slicing. Providers that deploy network slicing capabilities should be able to select whatever OAM technology-specific feature that would be address their needs. No gap that would legitimate specific requirements has been identified so far.

9.2.2. Overlay OAM

[I-D.ooamdt-rtgwg-ooam-header]specifies a generic OAM header that can be used if overlay technologies are enabled. Obviously, this effort can be reused in the context of network slicing when overlay techniques are in use. Nevertheless, For slice designs that do not assume an overlay technology, OAM packets must be able to fly over the appropriate slice and for a given service/customer. This is possible by reusing some existing tools if and only if no specific fields are required (e.g., carry a slice identifier as Req. 5 stated).

9.2.3. Service Function Chaining

SFC WG [SFCWG] is chartered to define SFC-specific OAM. Extensions that will be specified by the SFC WG will be reused in the context of network slicing. Nevertheless, The current charter of the WG does not imply work on the automated discovery of SF instances and their

capabilities, nor the automatic discovery of control elements. An additional specification effort is therefore required in this area.

10. Summary

The following table is a summary of the identified gaps based on previous analysis in this document.

Requirements	Gaps
Network Slicing Resource Specification	1) A detailed specification of NSRS; 2) A companion YANG data model for NSRS; 3) Mechanisms/protocols for capability exposure; 4) Mechanism/protocols for NS state monitoring;
Cross-Network Segment & Cross-Domain Negotiation	5) Mechanisms for secure cross-network segment and cross-domain negotiation/inter-operation; 6) Information model for network slicing related message exchange; 7) Mechanisms/protocols for E2E NS composition/decomposition;
Guaranteed Slice Performance and Isolation	8) Mechanisms for on-demand, isolated, elastic and efficient network slice instantiation and resource association;
Network Slicing-Domain Abstraction	9) Common representation mechanism for network slices across multi-domain; 10) Mechanisms for customized network slices;
Slice Identification	11) Mechanisms and framework for network slice identification;12) Mechanisms for dynamic discovery of instantiated network slices; 13) Mechanisms for network slicing E2E repository;
OAM Operation with Customized Granularity	14) Mechanisms for dynamic discovery of service with function instances and their capabilities; 15) Mechanisms for customized network slices OAM when overlay techniques are not in use.

Table 2: Summary of Gaps

11. Security Considerations

This document analyzes the standardization work on network slicing in different WGs. As no solution proposed in this document, no security concern raised.

12. IANA Considerations

There is no IANA action required by this document.

13. Acknowledgements

The authors wish to thank Hannu Flinck, Akbar Rahman and Ravi Ravindran for their detailed and constructive reviews. Many thanks to Susan Hares, Mohamed Boucadair, Christian Jacquenet and Stewart Bryant for their valuable contributions and comments.

14. Informative References

[ANI] "A Reference Model for Autonomic Networking", <https://datatracker.ietf.org/doc/draft-ietf-anima-reference-model/?include_text=1>.

[ANIMA-GRASP] "A Generic Autonomic Signaling Protocol (GRASP)", <https://datatracker.ietf.org/doc/draft-ietf-anima-grasp/>.

[DETNET-WG] "Deterministic Networking", <https://datatracker.ietf.org/wg/detnet/about/ >.

[FGEx] "5G Exchange (5GEx) - Multi-domain Orchestration for Software Defined Infrastructures", <https://www.researchgate.net/publication/296486303_5G_Exchange_5GEx_-_Multi-domain_Orchestration_for_Software_Defined_Infrastructures>.

[FLEXE-1.0] "Flexible Ethernet 1.0", <http://www.oiforum.com/wp-content/uploads/OIF-FLEXE-01.0.pdf>.

[I-D.boucadair-connectivity-provisioning-protocol] Boucadair, M., Jacquenet, C., Zhang, D., and P. Georgatsos, "Connectivity Provisioning Negotiation Protocol (CPNP)", draft-boucadair-connectivity-provisioning-protocol-14 (work in progress), May 2017.

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-11 (work in progress), February 2017.

[I-D.ooamdt-rtgwg-ooam-header]
Mirsky, G., Kumar, N., Kumar, D., Chen, M., Yizhou, L., and D. Dolson, "OAM Header for use in Overlay Networks", draft-ooamdt-rtgwg-ooam-header-03 (work in progress), March 2017.

[I-D.wu-opsawg-service-model-explained]
Wu, Q., LIU, W., and A. Farrel, "Service Models Explained", draft-wu-opsawg-service-model-explained-06 (work in progress), May 2017.

[I2RS-Yang]
"A Data Model for Network Topologies", <https://datatracker.ietf.org/doc/draft-ietf-i2rs-yang-network-topo/ >.

[IMT2020-2015]
"Report on Gap Analysis", <http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx >.

[IMT2020-2016]
"Draft Technical Report Application of network softwarization to IMT-2020 (O-041)", <http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx >.

[IMT2020-2016bis]
"Draft Terms and definitions for IMT-2020 in ITU-T (O-040)", <http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx >.

[NGMN-2016]
"Description of Network Slicing Concept", <https://www.ngmn.org/uploads/media/160113_Network_Slicing_v1_0.pdf>.

[NGS-3GPP-2016]
"Study on Architecture for Next Generation System-latest version v1.0.2", <http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/Latest_SA2_Specs/Latest_draft_S2_Specs >.

[NMDA] "Network Management Datastore Architecture", <https://datatracker.ietf.org/doc/draft-ietf-netmod-revised-datastores/>.

[NS-Framework] "NS Framework", <https://datatracker.ietf.org/doc/draft-geng-netslices-architecture/>.

[NS-UseCase] "NS Use Case", <https://datatracker.ietf.org/doc/draft-qin-netslices-use-cases/>.

[NVO3-WG] "Network Virtualization Overlays".

[ONF-2016] "Applying SDN Architecture to 5G Slicing", <https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Applying_SDN_Architecture_to_5G_Slicing_TR-526.pdf >.

[RFC2679] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, DOI 10.17487/RFC2679, September 1999, <http://www.rfc-editor.org/info/rfc2679>.

[RFC2680] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, DOI 10.17487/RFC2680, September 1999, <http://www.rfc-editor.org/info/rfc2680>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <http://www.rfc-editor.org/info/rfc3209>.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, DOI 10.17487/RFC3393, November 2002, <http://www.rfc-editor.org/info/rfc3393>.

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

[RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <http://www.rfc-editor.org/info/rfc4655>.

[RFC4664] Andersson, L., Ed. and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, DOI 10.17487/RFC4664, September 2006, <http://www.rfc-editor.org/info/rfc4664>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <http://www.rfc-editor.org/info/rfc5440>.

[RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, DOI 10.17487/RFC6291, June 2011, <http://www.rfc-editor.org/info/rfc6291>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <http://www.rfc-editor.org/info/rfc7276>.

[RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, DOI 10.17487/RFC7297, July 2014, <http://www.rfc-editor.org/info/rfc7297>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <http://www.rfc-editor.org/info/rfc7432>.

[SFCWG] "\Service Function Chaining (sfc)", <https://datatracker.ietf.org/wg/sfc/about/>.

[SLA-Exchange] "Inter-domain SLA Exchange Attribute", <https://datatracker.ietf.org/doc/draft-ietf-idr-sla-exchange/>.

[TE-Yang] "YANG Data Model for TE Topologies", <https://datatracker.ietf.org/doc/draft-ietf-teas-yang-te-topo/>.

[TEAS-ACTN] "Information Model for Abstraction and Control of TE Networks (ACTN)", <https://datatracker.ietf.org/doc/html/draft-ietf-teas-actn-info-model>.

Authors' Addresses

Li Qiang (editor)
Huawei

Email: qiangli3@huawei.com

Pedro Martinez-Julia
NICT

Email: pedro@nict.go.jp

Liang Geng
China Mobile

Email: gengliang@chinamobile.com

Jie Dong
Huawei

Email: jie.dong@huawei.com

Kiran Makhijani
Huawei

Email: Kiran.Makhijani@huawei.com

Alex Galis
University College London

Email: a.galis@ucl.ac.uk

Susan Hares
Hickory Hill Consulting

Email: shares@ndzh.com

Slawomir
Orange

Email: slawomir.kuklinski@orange.com