None
Internet-Draft
Intended status: Informational
Expires: April 21, 2018

K. Makhijani, ed
J. Qin
R. Ravindran
Huawei Technologies
L. Geng
China Mobile
L. Qiang
S. Peng
Huawei Technologies
X. de Foy
A. Rahman
InterDigital Inc.
A. Galis
University College London
G. Fioccola
Telecom Italia

October 18, 2017

Network Slicing Use Cases: Network Customization and Differentiated Services
draft-netslices-usecases-02

Abstract

Network Slicing is meant to enable creating (end-to-end) partitioned network infrastructure that may include the user equipment, access/ core transport networks, edge and central data center resources to provide differentiated connectivity behaviors to fulfill the requirements of distinct services, applications and customers. In this context, connectivity is not restricted to differentiated forwarding capabilities but it covers also advanced service functions that will be invoked when transferring data within a given domain.

The purpose of this document is to focus on use cases that benefit from the use of network slicing.

Copyright Notice

Table of Contents

1. Introduction

Network Slicing enables the creation of (end-to-end) partitioned network infrastructure that may include the user equipment, access/ core transport networks, edge and central data center resources to provide differentiated connectivity behaviors to fulfill the requirements of distinct services, applications and customers. In this context, connectivity is not restricted to differentiated forwarding capabilities but it also spans service, management and control plane support offered to a slice instance.

1.1. 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.

1.2. Terminology

Please refer to [I-D.geng-netslices-architecture] for related terminologies and definitions.

Additionally, the following terms are used:

- V2X (Vehicle-to-everything): Is a communication of information from a vehicle to any other entity that may be another vehicle, road-side network element or application end point.

- ITS (Intelligent Transportation Systems): Considered as an aspect of how using Internet of Things resource like road sensors can creates a smart transport network. The network offers services related to transport and traffic management systems through flow of information between road-side sensors, vehicles, smart devices and humans.

- Over-the-top (OTT): A service, e.g., content delivery using a CDN or a social networking service, operated by a different service providers to which the users of the NSP service are attached to, and to whom it serves as a communication (or bit pipe) provider

- Industry vertical: A collection of services or tools specific to an industry, trade or market sector. also, referred to as Service Verticals in this document.

- TETRA: Terrestrial trunked radio is a digital trunked mobile radio standard to meet needs of public safety, transportation and utilities like organizations.

- SLA: Service Level Agreement - A contract between a service provider and an end user that stipulates a specified level of service, support option, a guaranteed level of system performance as relates to downtime or up-time.

2. Scope

To maximize resource utilization and minimize infrastructure cost, services will need to operate over a shared network infrastructure, as against the traditional monolithic model operated either as dedicated network or as an overlay. Service operators can utilize or benefit from Network Slicing through multi-tenancy, enabling different customized network infrastructures for different group of services across different network domains and operating them independently.

In this document, multi-domain refers to combination of different kinds of connection-technology network domains. For example, it may be a RAN, DSL etc. in access; a fixed, wireless or mobile service provider network; as well as different technology domains, in transport networks such as carrier Ethernet, optical, MPLS, TE-tunnel etc. Often, a combination of technology domains is under the same administrator's control but may also belong to different administrative systems and may require cross-domain coordination.

The document covers generalized as well as resource guaranteed service scenarios that can benefit by applying Network Slicing principles as below in Figure 1

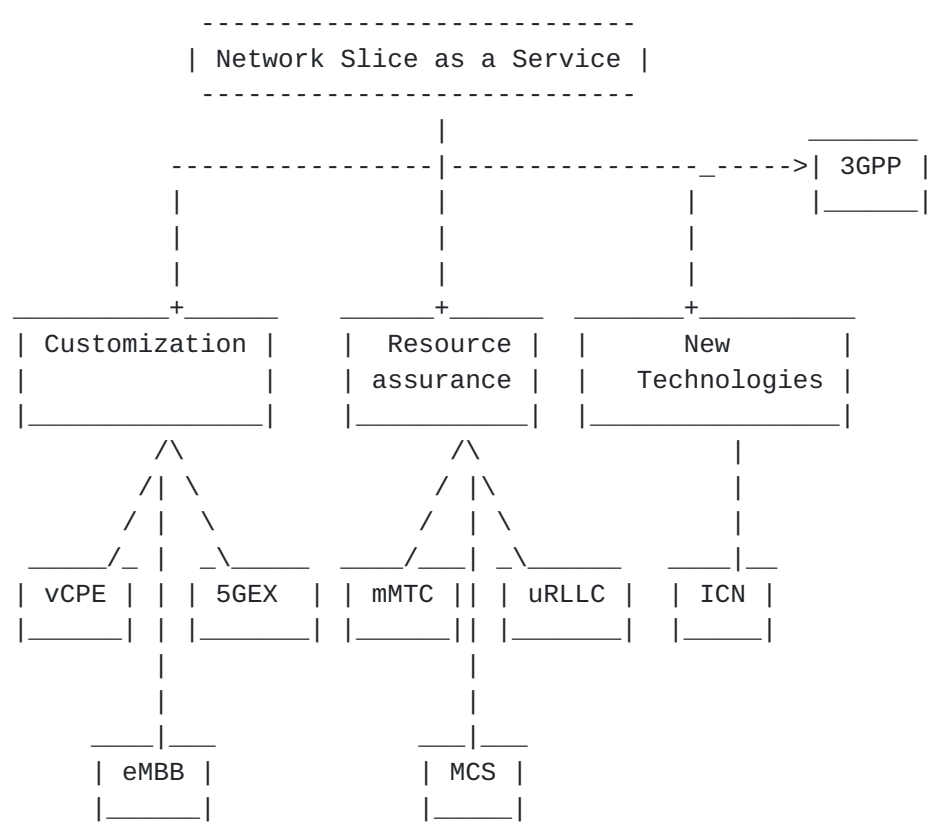

Figure 1: Use case organization in the document

The remaining document is organized as below:

- In Section 3, Network Slice as a Service(NSaaS) delivery model is described.

- Section 3.5, is a scenario for multi-domain network slice coordination.

- In Section 4, 3GPP architecture for 5G is discussed as a use case so that those requirements may be taken into consideration during slicing activities in IETF.

- Other use cases are discussed from 2 perspectives

  a. Existing scenarios: Several already deployed use cases that would further benefit operators when deployed through Network Slice paradigm are discussed in Section 5.

  b. Differentiated service scenarios: that must absolutely meet strict resource requirements, as if they use a dedicated

infrastructure. The example use cases are categorized in Section 6.

- o Section 7, has an example use case of cases where new technologies can be verified or deployed using network slicing concept.

- o In Section 8, the use case requirements are summarized which are inputs to the [I-D.qiang-netslices-gap-analysis].

3. A Generalized Network Slice as a Service

Network slicing instances share a common infrastructure, which provide flexible design of a logical network with specific network functions customized to support differentiated performance requirements of vertical industry through logical or physical system isolation and certain OAM tools.

Traditionally, vertical industries run their services in a shared network environment upon which infrastructure owners and service providers offer standalone network capabilities including connections, storage and etc. Network slicing paradigm enables supporting the requirements of a network slicing tenant to be met individually. Hence it is anticipated that this type of new business model where network slice instances are leased to industry verticals as a service (i.e. Network Slicing as a Service, NSaaS) may become a norm in the near future.

3.1. Resource Centric Service Concept

Network services specify a set of resource requirements to offer desired Quality of Experience (QoE) to it consumers, using features offered by the control and forwarding planes. Traditional service guarantees are associated with resource attributes such as throughput, packet loss, latency, network bandwidth/burst or other bit rates and security. In addition, redundancy and reliability are provided by the infrastructure to improve overall QoE. More recently, concepts such as edge computing allow opportunistic placement of services to meet stringent requirements of low latency and/or high bandwidth applications.

Clearly the description of service delivery is more diverse now than before and demands higher degree of resource engineering and agility. The motivation behind Network slicing paradigm is to enable new service deployments without having to build new network infrastructures or causing disruptions to already deployed services in the network. In this regard, there are two primary characteristics NS should satisfy, a) Strict demand for network resource, b) Network Customization.

3.2. Strict Resource Demand

Several services are sensitive to response times and/or amount of bandwidth, e.g. real time interactive multimedia, high bandwidth video feed or remote access to an enterprise network. Failure to meet these criteria lead to service degradation. Moreover, new industry verticals are evolving due to technological advancements in sensors, IoT, robotics and multi-media, along with new type of network interactions (both human-human or human-machine). These impose even stricter resource and connectivity requirements. The challenge lies in utilizing common network infrastructure and judiciously allocating available infrastructure resources.

3.3. Network Customization

To a network slice tenant, the ability to customize services dynamically is important. Customization gives control to the operator of a slice to create, provision and change network resources to suit their service demands. Customization enables decomposition of resources from an underlying network infrastructure and logically aggregate them as part of a slice. These customizations also include placement and logical connection of the network functions based on the service requirements.

3.4. NSaaS of Different Granularity

In order to meet various requirements from the network slice tenant, NSaaS should be provided with different granularities. Some typical examples of granularities that a provider may offer are as follows.

- Network Domain - Network slice instances of different networks i.e. access (wireless, fixed) network, transport network and core network.

- Access technologies - Network slice instances of different generations of cellular and fixed network technologies, i.e. 4G, WiFi, Passive Optical Network (PON) and DSL.

- SLA requirements - Network slice instances of different SLA requirements, i.e. low-latency network, legacy best-effort network and network with guaranteed-bandwidth.

- Vertical applications - Network slice instances of different industry verticals. i.e. manufacturing site, V2X, industrial IoT and smart city.

- OTT services - Network slice instances of different applications provided by OTT, i.e. messaging, payment, video streaming and gaming.

- Cross domain services - Network slice instances of different services across multi-provider domains such as l2, l3 VPN services.

During the realization of network slice instance, it is also very important that sub-instance of a more general one can be provided with a finer granularity. In practice, it is up to the provider to decide the granularity to lease the network slice instances.

The customization of different granularities of a network slice introduce many challenges, especially in terms of network management and orchestration. As a network slice provider (provider of end-to-end slice service), it is essential to have a comprehensive understanding of the network capability. This requires that network connectivity and resources can be exposed to the network slice tenants (as the differentiated services). Accordingly, network slice provider is able to orchestrate specific instances based on these exposed capabilities.

3.5. Service customization across multi-provider multi-domains as NSaaS

L2 and L3 connectivity services can be deployed in a multi-provider multi-domain scenario and, in the SDN era, this implies the decoupling of network resources for different service provider and domain orchestrators. The allocation of network resources within the domain of each service provider, involved by the end-to-end service, can be defined as a network slice.

Within a single domain, provider is aware of the entire topology and its own resource availability and has complete control over those resources. However, in a multi domain scenario, the overall knowledge of the resources and topologies cannot be made across providers. Therefore, the exchange of information across these providers have to be enabled, as shown in Figure 2, inspired by [I-D.bernardos-nfvrg-multidomain] and [I-D.ietf-opsawg-service-model-explained].

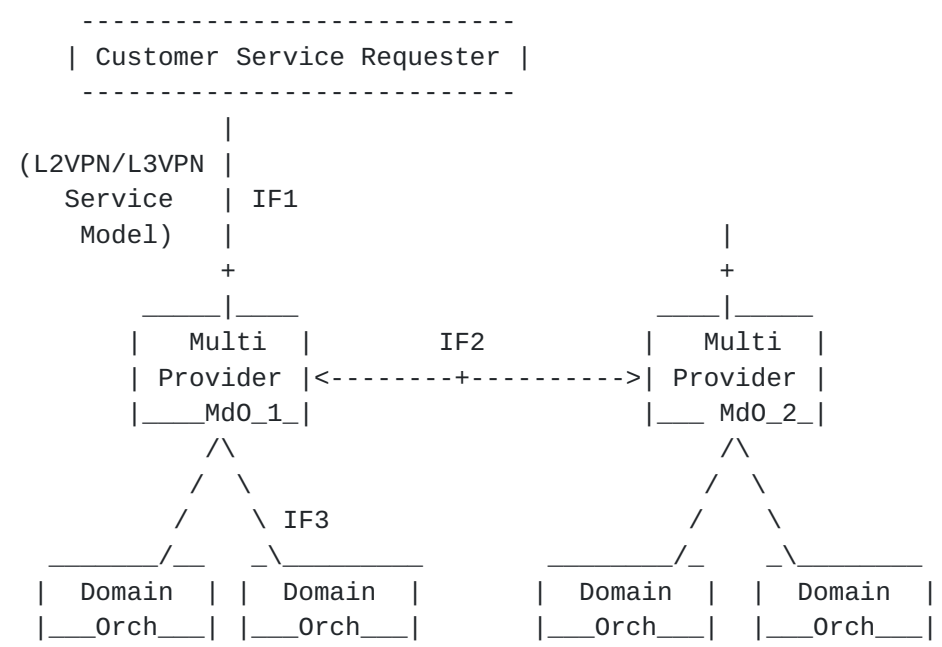

Figure 2: Multi-domain, multi-provider connectivity services

The Figure 2 shows a multi provider MdO (MP-MdO) exposing an interface 1 (IF1) to the tenant, interface 2 (IF2) to other multi provider MdO (multi domain orchestrator) and an interface 3 (IF3) to individual domain orchestrators. IF1 is exposed to the tenant who could request his specific services and/or slices to be deployed. IF2 is between the orchestrators and is a key interface to enable multi-provider operation. IF3 focuses on abstracting the technology or vendor dependent implementation details to support orchestration in each network domain (see [!@I-D.bernardos-nfvrg-multidomain] for details). The coordination alternatives between MP-MdOs are: * Bilateral Cascading: providers can have long-lasting business agreements only with their direct neighbors. * Full Mesh between MP-MdOs: Providers can have long-lasting business agreement with any provider (neighboring or remote).

This reference architecture is the main focus of the 5GEx European Project.

Among applications, L2VPN and L3VPN wholesale end-to-end services in a multi-provider and multi-domain scenario needs the following characteristics for network slice management

- An automatic activation test and verification functionality (by customer or orchestrator).

- Interface to modify parameters of L2VPN or L3VPN service such as bandwidth or path redundancy.

Looking at Figure 2, the customer needs a new L2 end-to-end service between CPEs across two domains (MP-MdO1 and MP-MdO2). As MP-MdO1 receives the service request, it is deployed as a network slice. In this regards MP-Md01 has prior knowledge of topology and resource across domains in some form, it then splits the service request into a slice across each of the involved domain. Once service is set up: MP-MdO1 allocates resources for the slice on SP1 domain while MP-MdO2 allocates on SP2 domain respectively.

[I-D.ietf-l2sm-l2vpn-service-model] and [RFC8049] can describe IF1 For L2 and L3 end-to-end services respectively. The ability to map such services as network slice will be considerable opportunity for dynamic cross-domain operations.

4. Network Slicing in 3GPP Mobile Network

Network Slicing is a core capability of the currently under development 3GPP 5G phase 1 mobile system, as it makes it possible for different service verticals, such as IoT and broadband applications, to be deployed over a common shared infrastructure. More details can be found in [TS_3GPP.23.501], [TS_3GPP.23.502], [TR_3GPP.38.801], [TR_3GPP.33.899] and [TS_3GPP.28.500].

3GPP is currently defining its own solution for network slicing. An IETF effort in this field may, however, still be complementary in the long run as IETF focuses on the IP infrastructure and protocols which are generally out of scope of 3GPP. Challenges relevant to the IETF include isolation between network slices, supporting sharing network functions between several slices, building slices recursively from smaller slice subnets, implementing slicing across different domains for roaming, etc.

4.1. Network Slices in 3GPP Systems

In 3GPP systems a network slice is a complete logical network which provides telecommunication services and network capabilities. Distinct Radio Access Network (RAN) slices and core network slices interwork to provide mobile connectivity. A device may access multiple NS simultaneously through a single RAN. 3GPP defines slice IDs (NSSAI) composed of a Slice Service Type (SST) and a Slice Differentiator (SD). SST refers to an expected network behavior in terms of features and services (e.g. specialized for broadband or massive IoT), while SD helps distinguishing among several NS instances.

Figure 3 describes the general layout of Network Slicing in mobile networks. A core network slice includes, a Session Management Function (SMF), which manages PDU sessions, and a User Plane Function (UPF). Some functions such as the Access and Mobility management Function (AMF) are common and shared between multiple RAN and core network slices.

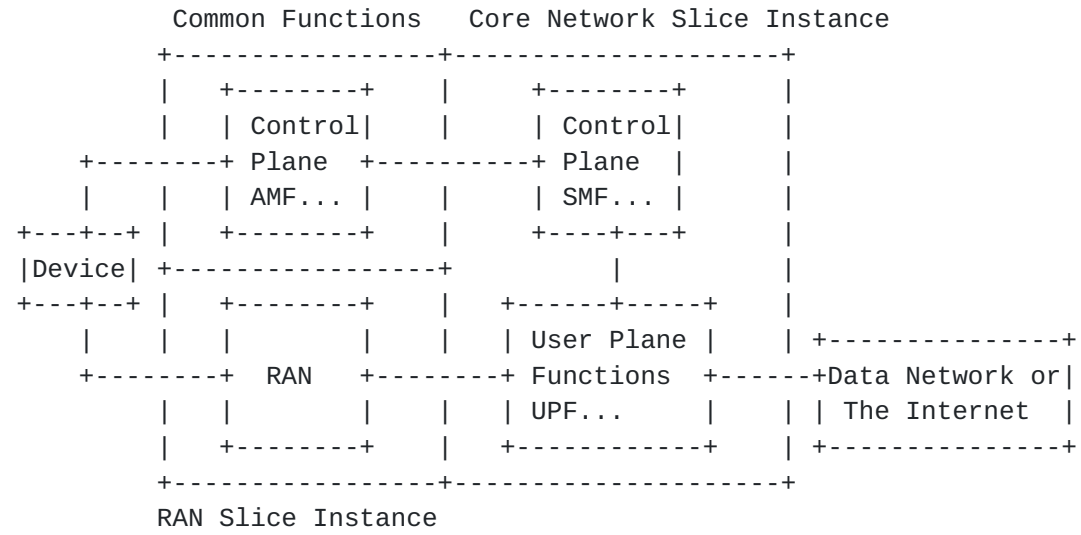

Figure 3: 3GPP Network Slices

4.2. Creating, Managing and Operating 3GPP Network Slices

To create a network slice instance, mobile network operators define "Network Slice Subnets" into OSS/BSS management system. NS subnets are NS components including NFs and reserved network resources. OSS/BSS communicates with the orchestrator, which, through the rest of the NFV-MANO system, configures compute and network elements to create, compose and activate slices.

Mobile network operators can modify the configuration of a RAN or core network slice, while it is in use. To support this, the operator needs to measure QoS/SLA data for hosted network services, and associate results with the relevant network slice. Example of operations include increase or decrease network capacity or compute capacity of NFs; update the configuration of NFs; add, replace or remove a NFs or a Network Slice Subnet.

Slice selection occurs in 2 phases: first, common functions (including AMF) and available network slices are pre-selected when the device registers with the network. Later on, the network dynamically selects network slices when a device initiates

communication, based on a slice ID associated with the application (on the device) that requests a new flow.

5. Role of Virtualization in Network slicing

Virtualization is a key enabler of network slices; Many network services can be easily deployed using components of NFV framework like network functions, hardware decoupling and resource placement [#?NFVSLICE]. When deployed as a network slice, the resources associated with virtualized network services are managed uniformly by network slice provider. One such use case is described below.

5.1. Virtualized Customer Premise Equipment

A CPE is an equipment that connects the customer premises to the provider's network. A CPE may either be a layer-2 or a layer-3 device (the routing gateway) performing different network functions depending on the access technology (DSL modem, PON modem, etc.). Any services provided such as Internet access, IPTV, VoIP, etc. or network functions for example, local NAT, local DHCP, IGMP proxy-routing, PPP sessions, routing, etc. are also part of CPE. The installation of different on-premise devices, entails a high cost for service providers in terms of both initial installation and operational support, since they are typically responsible for the end-to-end service.

Traditional CPE deployments are service provider network functions installed on customer site to provide above mentioned functionalities along with remote site connectivity. Communication Service provider (CSP) is responsible for management and administration of connections and state with proper policy, bandwidth, security and QoS requirements.

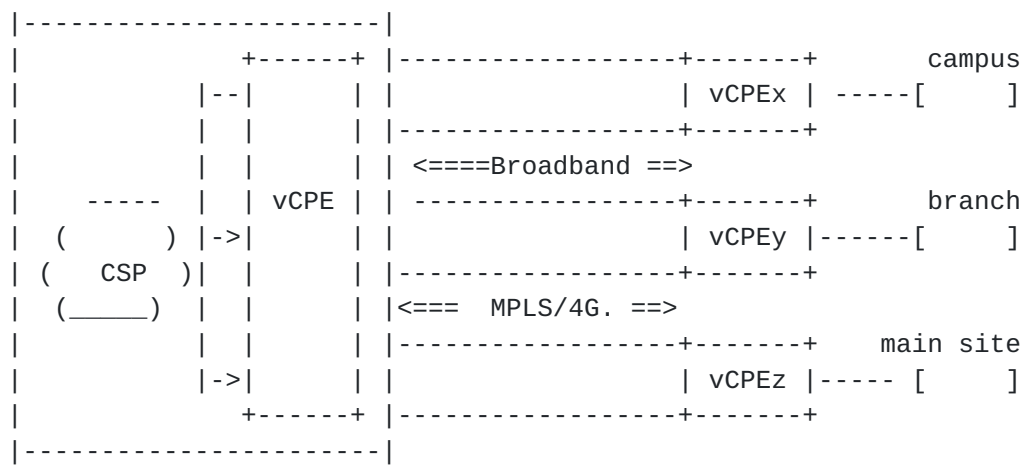

Figure 4: Virtualized CPE with distributed architecture

Figure 4 shows a virtualized architecture in which many functions are moved to CSP's cloud simplifying CPE on premises tremendously. Additional details of deployment architecture models are captured in [I-D.pularikkal-virtual-cpe] where full dissemination of data path and control plane functions is described. The figure shows vCPEx, vCPEy, vCPEz are virtualized CPEs on multiple sites of a specific customer, there may be set of different network functions in each x, y and z CPE. The vCPE instance in CSP cloud is integrated to each site performing service chains of network functions and resource allocations specific for ingress and egress path of each site.

A vCPE is a well-known concept[VCPEBBF] which when combined with WAN technologies provides end to end visibility and reachability to remote sites. However, there is no standard approach to connectivity or management of various CPE functions. Using network slicing, a greater level of agility can be achieved, with each customer dynamically managing its own network with the assistance of network slicing framework.

The benefit of self-managing a vCPE network slice is the capability to move network functions on premise of to the cloud. An obvious use case will be customer initiated gradual migration of network functions from a site to CSP cloud.

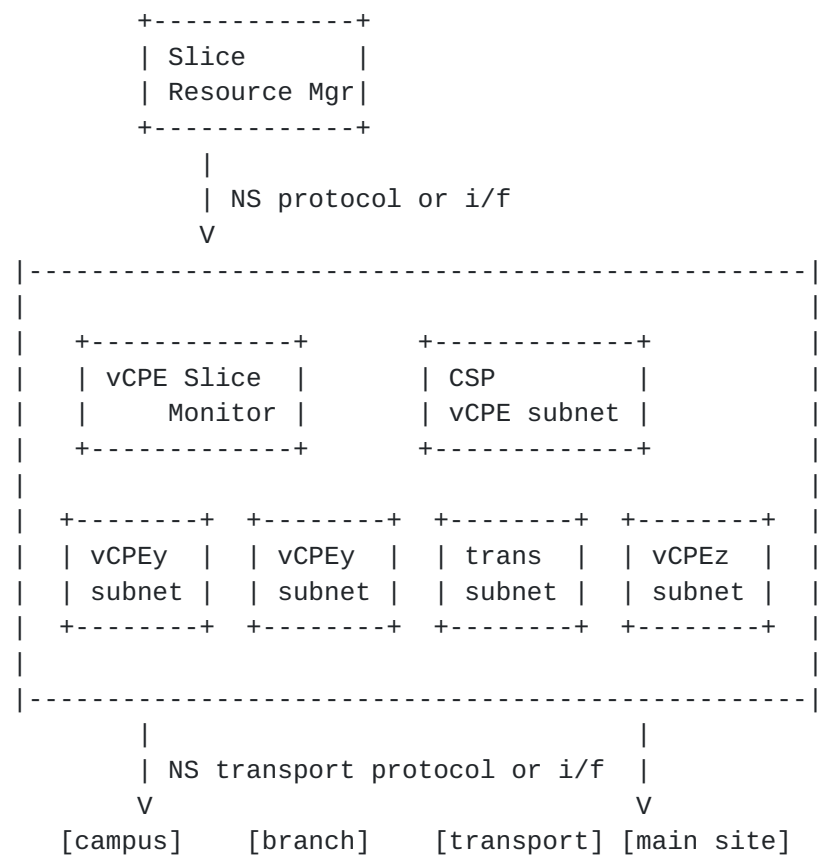

Figure 5: vCPE as a Network Slice

In Figure 5, a slice for vCPE is shown. Using slice subnet approach, each vCPE site instance may be considered as an abstracted subnet, along with the WAN transport as another subnet. The network functions are chained in a distributed fashion between site vCPEs and CSP vCPE subnet. A monitoring function interfaces with CSP's global slice manager for resource management. A south-bound interface through network slice transport protocol, realizes these functions on the infrastructure.

5.2. Enhanced Broadband

Today, video consumes the largest amount of bandwidth over the Internet. As the higher resolution formats enter mainstream, even more bandwidth will be needed to stream 4K/8K/360 degree formats. For example, connected Virtual Reality(VR)/Augmented Reality(AR) is the future use case of eMBB services. Notably, media processing for AR/VR will require in-network processing functions and high latencies between components could lead to downgrade of user experience. Therefore, an AR/VR stream requires a special infrastructure that differs from best-effort network.

A purpose-built network slice for eMBB streaming shall ensure to minimize processing overheads, it may be done by placement of network functions closer to subscribers. Resource scaling for eMBB should be dynamic because bandwidth is expensive and such vertical service operators may not want to pay for unutilized bandwidth. Therefore, slices should be able to monitor, negotiate and adjust the scale for both bandwidth and service functions. Latency guarantees vary from general services, therefore, as a first step, monitoring for quality of service is needed and more advanced operation would involve recovery and reparation of paths.

A typical eMBB slice Figure 6 from a network operator is a performance oriented service customization. An eMBB service slice template will allow a tenant to request or specify

(1) CDN components (as service functions)

* Regional network locations of CDN, encoders etc.

* Location of acquired content.

* Describes transport constraints for its own distribution network comprising of connectivity between content acquisition and Fan-out points.

(2) An interface to subscriber database perhaps as a network function, from multiple access network types (cellular, fixed).

(3) Live performance monitoring and resource negotiation loop.

(4) A well-coordinated network slice protocol that enables resource allocation across different network domains.

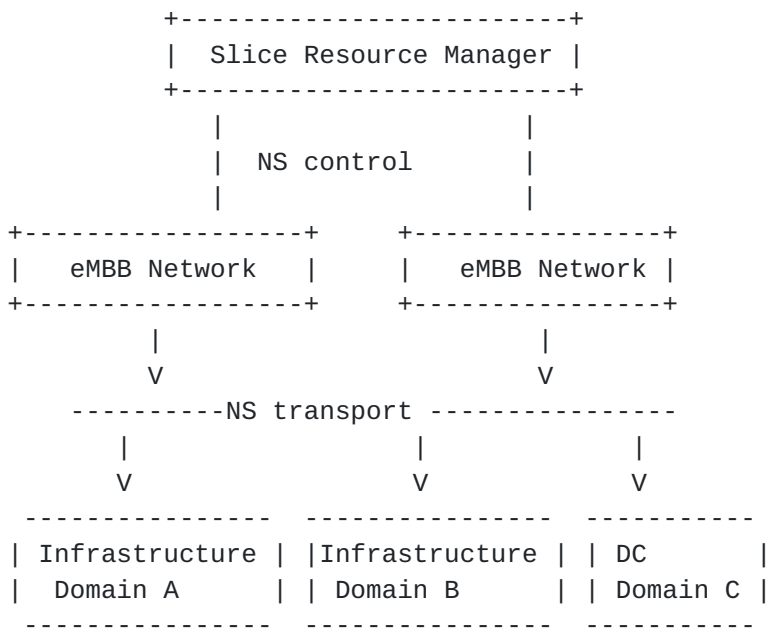

Figure 6: Transport provider network operator view.

6. Services with Resource Assurance

6.1. Massive Machine to Machine Communication

Sensor networks are widely deployed in industries such as agriculture, environmental monitoring and manufacturing. The general workflow of wireless sensor network is provided in Figure 7.

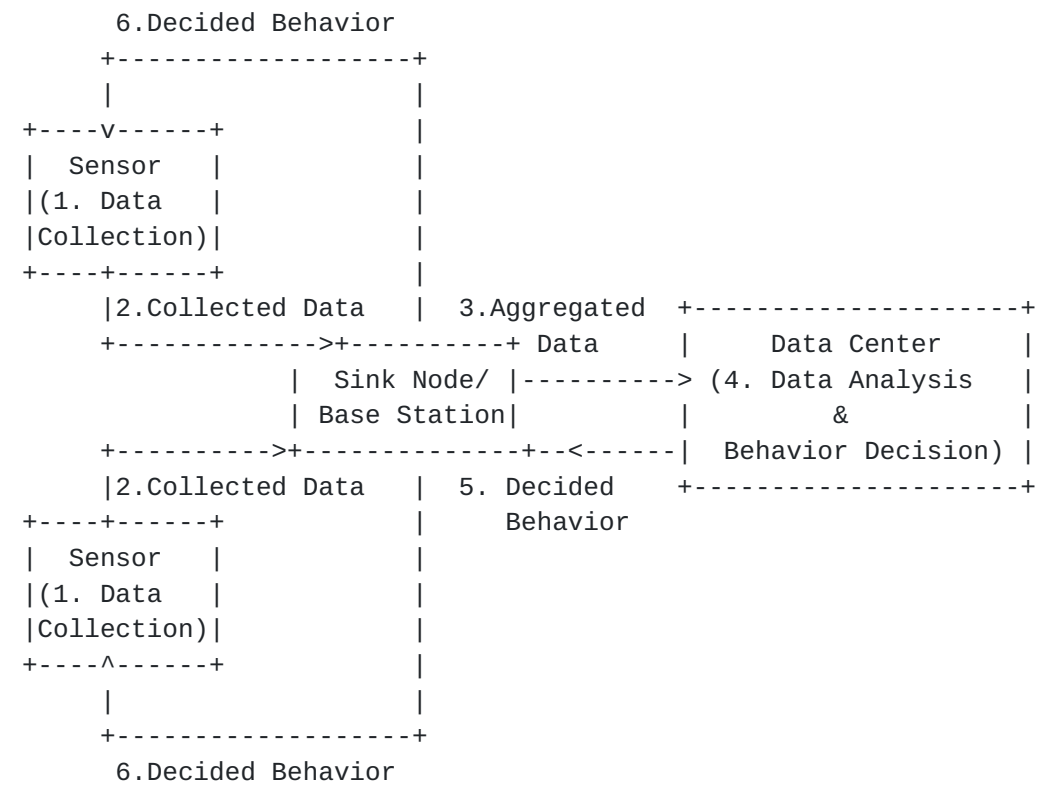

Figure 7: Workflow of wireless sensor network

Figure 7 shows, control of sensor data & behavior at scale, requiring wide area coverage and power constrained communication. A few new types of scenarios that require unique infrastructure are:

- Smart city networks: an integration of several public infrastructures together through M2M communications. For example Automatic metering (for gas, energy, water, etc.), environment monitoring (for pollution, temperature, humidity, etc.), traffic signal control etc.

- E-health communications that remote monitor the physical conditions (e.g., heart rate, pulse, blood pressure etc.), and accordingly take necessary measures remotely. E-health communication network must be secure, reliable and fast but small-size of data exchange.

mMTC Type Slices involves potentially a large number of small and power-constrained devices, therefore, resource allocation at scale is of particular importance in mMTC type slices. Furthermore, different kind of IoT devices may exhibit delay sensitivity in industry operations etc. The mMTC type slices should be conscious of requirements of scale, variable data pattern, and energy efficient communications.

6.2. Ultra-reliable Low Latency Communication

In uRLLC scenarios, data loss is not acceptable. Both data and control planes may require significant enhancements to transmission or information distribution protocols. [TR_3GPP_38.913] specifies access network user plane latency as 1ms and reliability factor of 99.999% for transmission of a packet of size 32 bytes. The slices of this type must be ensured that shared infrastructure absolutely does not cause any adverse effects.

In the following sections three new uRLLC scenarios are described.

(1) Industrial operation: Operations in remote sites usually need combined support of cellular and transport network. Operational accuracy is characterized by

* Requires high-quality communication links between the control site.

* Low latency and low jitter in communication path

* Closed control loop (Sensor -Controller - Actuator) as shown in Figure 8, a typical control cycle time where network is involved should be below 10ms [Tactile-Internet].

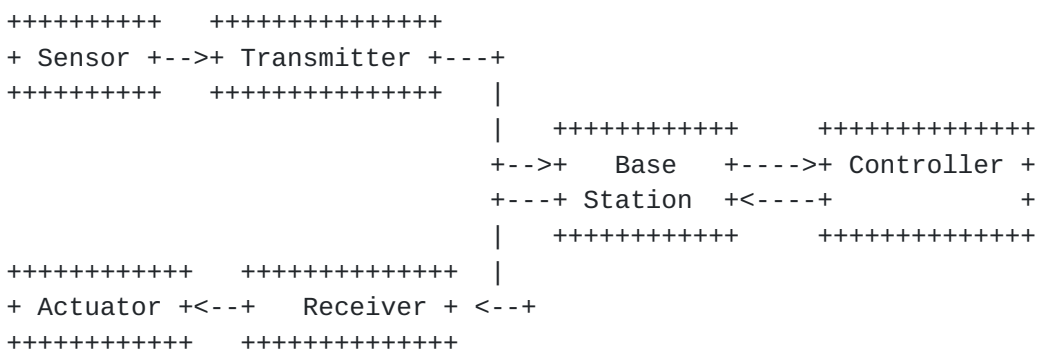

Figure 8: Industrial closed control loop

(2) Remote surgery enables surgeons to perform critical specialized medical procedures remotely, providing accurate control and haptic feedback.

A uRLLC network slice only accepts service specific traffic and must not receive any other type of traffic to avoid negative impact on the service operation. Capabilities required by uRLLC service provider include

- Locations of the access nodes for terminals (devices, vehicles) to the transport network and locations of the controller to construct its own network topology within the network slice. In high mobility scenario such as automotive verticals, the dynamic topology adjustments are required without loss of data.

- Each service vertical has different performance requirements in terms of latency, reliability and data rate etc., therefore, the uRLLC network slice should allow customization for these parameters.

- A uRLLC service provider should be able to registers self with access rights to resource monitoring and negotiation loop.

A network slice provider offers a uRLLC Slice with the following considerations

- Should support/provide specific data and control planes protocols with significant enhancements for deterministic latency and reliability (e.g. DetNet[I-D.dt-detnet-dp-sol] in data plane).

- Allow uRLLC service operator to access user admission and authentication to its network slice in advance.

- The network coverage for a uRLLC service provisioning may be limited to a confined area, either indoor or outdoor, network operator needs to be able to coordinate resource allocation across different access types and network domains.

A high-level Figure 9, shows a URLLC slice provider and service view of the network. The monitoring of resources is done in the context of performance. A performance degradation would require resource adjustment. As shown in Figure 9, in one possible sliced model will have its own customizer that uses internal performance observing logic with in its slice by coordinating with different subnets/ domains using southbound NS transport protocol and transfers this information to operator via a northbound NS protocol for resource adjustment.

It is implied that domains maybe different access technologies and need for a common performance metric propagation and resource allocation is important for a uRLLC slice to function properly.

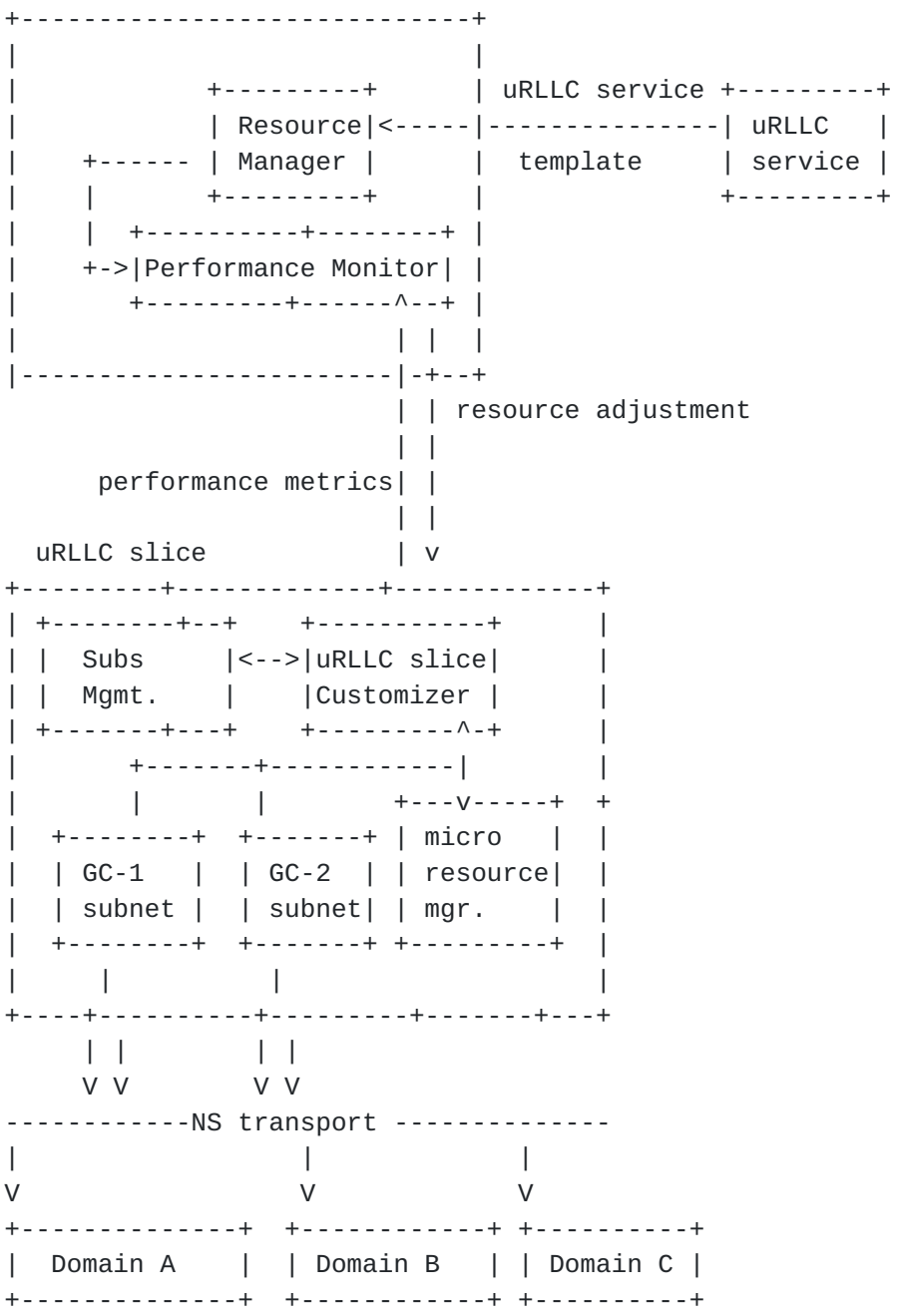

Figure 9: Reference for uRLLC Network Slice.

6.3. Critical Communications

Critical communications are associated with emergency situations. Often referred to as mission critical, the communication has to be reliable and non-disruptive. Different scenarios of critical communications relate to public safety responders (e.g. fire fighters, paramedics), military, utility or commercial applications,

mainly using reliable voice or short data messaging over wireless communication systems.

Next-generation public safety communications are planned to be built with enhanced broadband voice, data and video communications services beyond narrowband LMR with broadband LTE networks for high speed data (ref 22.179 and FirstNet).

3GPP defined on-network critical communication can be established both via (a) over the network infrastructure to manage the call, (b) off-network, where the terminals communicate directly to each other. In the network slicing context, over the network, involves transport networks for an always available, reliable, and zero packet loss quality of traffic support to meet critical services requirements.

Maintaining a separate broadband infrastructure for critical communications incurs a heavy deployment cost. Especially, as the coverage of this separate network has to be extended to large-scale nationwide geographies and remain interoperable is too expensive. As new communication technologies emerge, public safety systems will have to bear the state of the art adoption cost. A separate infrastructure lacks flexibility to add new value-added services or to take advantage of available commercial services.

While shared infrastructure, brings out challenges of these kind:

(1) Reliable support: Of basic mission critical services: Such as loss of information in voice communication is not acceptable in emergency services, if common infrastructure is to be used, it must assure no loss of information.

(2) Zero congestion: It is not acceptable for critical calls to be delayed at call setup times or be subjected to any other congestion scenarios.

Having the Mission Critical Service (MCS) as a network slice benefit from the following:

- Insertion and authorization of subscribers in a group communication: In a critical infrastructure, the subscriber authentication may be done earlier at the entry point automatically through slice selection functional entity.

- Pre-allocated QoS Class Identifiers (QCIs): Generally, QCIs are requested on per session basis which could slow down overall call control setup and is undesirable for emergency services. When operating in a slice, these resources maybe reserved ahead of time in a coarse-grained manner instead of per session.

MCS network slices are relatively straight forward as it only concerns with guaranteed bit rate (GBR) on per media basis and management of groups. From transport they should be able to request transport services based on GBR for reliable communication. A reference network slice in Figure 10 below, shows a mission critical (MC) organization providing service agreement through a network slice template with resource specification. The MCS slice sets up different subnetworks of different subscriber groups and manages its membership. These subnets are realized into the infrastructure across different domains through a network slice transport mechanism. The MCS must be capable of active resource monitoring to prevent congestions to ever occur as well as request additional transport resources in case of emergency event occurrence.

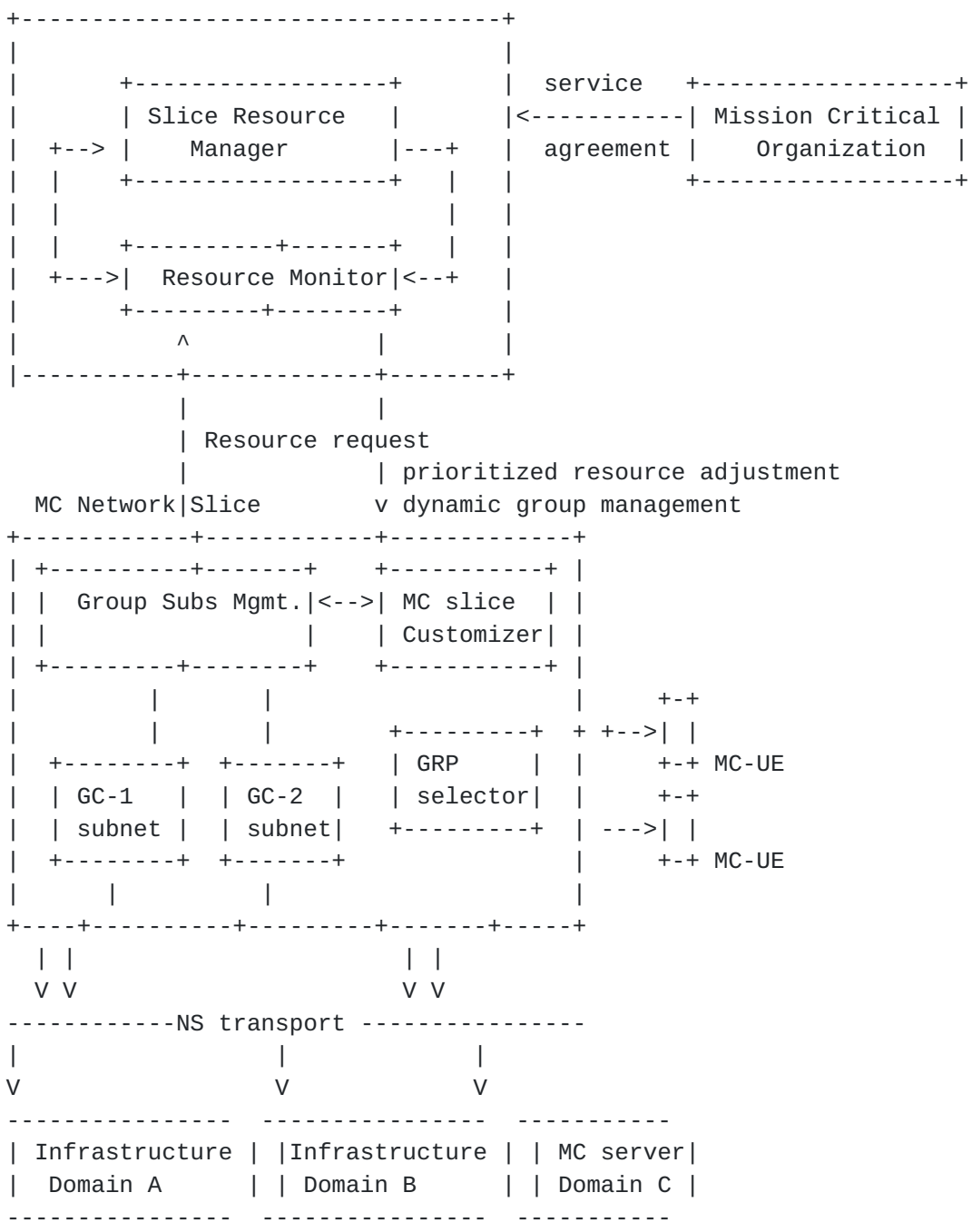

Figure 10: Reference for Mission Critical Network Slice.

7. Network Infrastructure for new technologies

7.1. ICN as a Network Slice

ICN as in Information-Centric Networking is a culmination of multiple future Internet research efforts in various parts of the world, now being pursued under IRTF's research task group called [ICNRG].

Information-Centric Networking (ICN) addresses Internet's network architectural design gaps based on evolving applications requirements and end user behavior that is significantly different from what IP was designed for - which was optimized for host-to-host communication paradigm. ICN is a non-IP paradigm based on name-based routing and offers many desirable networking features to applications such as naming, security, caching, mobility, multicasting and computing in a manner different from traditional host-centric communication model. ICN's name-based abstraction to application minimizes bootstrap configuration from the network, making it suitable to several communication modalities such as multi-point-to-multi-point, AR/VR, D2D and Ad hoc communication.

7.2. New Verticals - ICN based service delivery

Services over ICN slices can take advantage of its features such as:

(1) In ICN, applications, services and content are addressed using names, hence end host resolution services like DNS can be avoided, this achieves name resolution to edge content or services without incurring additional RTT delays.

(2) Service flows will be offered mobility and multicasting support, as the networking is session-less and optimized towards efficient movement of named data or networking named services and host level communication.

(3) Services can be deployed at the very edges with ease as ICN routers are compute friendly, this is because states in the forwarding table can be that of either content or service resources.

(4) Further saving bandwidth in the upstream link through opportunistic caching is an inherent feature of ICN, this also leads to energy efficient networking.

When offered as a programmable and customizable logical network slice, ICN based services can be offered as a network slice in parallel with traditional IP based services. ICN can be realized as a slice [_5GICN_] based on the choice of data plane resource offered by the operators in different domains of the network such as the access, core network or main data centers. While the same resources can be used to support services over IP, proper resource isolation shall allow it to co-exist with ICN slices as well. ICN slices can be offered over a network slicing framework built upon a programmable pool of software and/or hardware based data plane resources.

7.2.1. Required Characteristics

In ICN, applications use Interest/Data or Get/Put abstractions over named resources resolved by ICN's routing plane. An ICN slice shall be a programmable ICN-domain, in which content learning and distribution will be done using existing or new ICN aware distributed routing logic or through centralized application controllers. As a result, it should be possible to deploy software or hardware based network functions such as ICN routers and content producers and distributors that serve and speak ICN protocols, or enabled through service gateways at the edges of the network. Just as multiple service instances can be part of a slice, an ICN slices can multiplex heterogeneous services; on the other hand an ICN slice can be as granular as a single service instance too. The latter approach has implications with respect to consumer privacy, access control of name data objects, and granularity of mobility handling [_5GICN_].

A basic ICN slice can be manifested as a resource isolated logical network while sharing resources with other connectivity or IP based service slices. An ICN slice relies on programmability and virtualization framework to manage the service slices, to allow maximum flexibility through ICN aware logically centralized control plane for ICN service and slice management.

- Through a network slice template -ICN service providing entity could specify specific locations (edge of network domains) to deploy ICN-routers or other ICN-NFs (ICN aware network functions). Its service definition varies with the type of service.

- Application driven connectivity between ICN network elements in all segments and create an ICN based virtual topology.

- Mechanisms to deliver ICN user traffic over the infrastructure such as overlay or, ICN NFs can be tightly integrated with the RAN such as the eNodeB or implicitly using traffic classification function at the edge and tunneled to ICN User Plane Function (UPF).

- In addition, bandwidth and other network resources may be requested from the underlay depending on its capability of providing deterministic or statistically guarantees.

How multiple services will be deployed within an ICN aware slice may or may not be exposed to the network operator, depending on if the ICN slices are natively managed by it or a by other service providers.

8. Overall Use Case Analysis

The discussion in above use cases can be summarized as following in terms of the requirements for network slicing framework.

8.1. Requirements Reference

The following functional requirements are derived from discussions in above sections. They are described in details in [I-D.qiang-netslices-gap-analysis] document.

The differentiated services described in this document demonstrate several common functionalities. Therefore, a homogeneous approach towards deployment and management is absolutely necessary.

8.2. Mapping Common characteristics to Requirements

(1) Resource Reservation: Compute and network resources are reserved as part of initial creation and subsequently during the maintenance of a slice. For example, a service may initially reserve resources for its own control plane, and then later it may reserve user plane flows for applications on demand. Reference use cases: Differentiated services discussed in section "Services with Resource Assurance". A network slice aware infrastructure shall be able to support mechanisms for elastic scaling (up/down) of resources and their non-disruptive provisioning.

(2) Resource Assurance: A network slice aware infrastructure allows operators to allocate part of the network resources to meet stringent resource characteristics. Scenarios in both Section 5 and Section 6 require on demand and dynamic adjustments. It may not be possible to achieve this using centralize or API approach with finer granularity of resources participating in constrained path computation.

(3) Multi-dimensional service vertical: Network slicing supports dynamic multi-services, multi-tenancy and the means for backing vertical market players.

(4) Multi-domain coordination: Multi-domain refers to different technology related network domains. For example, it may be RAN, DSL etc., mobile core network, ISP or different domains in transport networks such as carrier Ethernet, MPLS, TE-tunnel etc. Often, they are under same administrator's control but may require coordination across different administrations. Furthoremore, capabilities of each domain must be known in order to validate if a slice can be created or not. All scenarios

mentioned require multi-domain coordination to connect and administer different subnets.

(5) Operational Isolation: A network slice represents logical group of network resources, functions and corresponding configurations separating its behavior and hence operation from the underlying physical network. Each network slice may have its own operator that sees this slice as a complete network (i.e. with router instances, policies, programmability, placement of virtual network functions according to traffic patterns etc.) and can manage as its own network.

(6) Transparency: Network slicing does not change the functionality of a scenario; It only facilitates creation of an isolated, an independently run infrastructure for that use case over a common network. Transparency promotes inter-operability and a common resource specification enables it.

(7) Reliability: It is an important resource attribute in the type of service verticals described above. Many services verticals cannot deliver functionality unless the network is reliable (See remote industry operation, remote surgery and other uRLLC applications). In this regard, monitoring probes are needed of each network slice and resources associated with it.

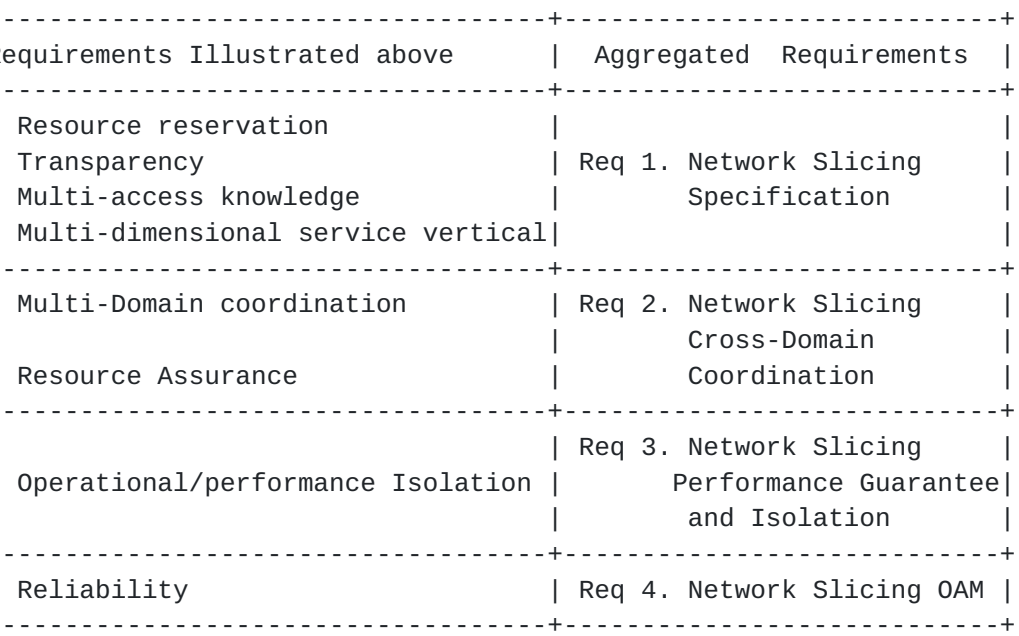

Figure 11: Mapping Common Characteristics to Requirements

NSaaS is a key for network operators to deploy network slices. Having standard means to realize these use cases, enables (a)

different usecases to be uniformly understood by a network slice provider, and (b) similar use cases to be understood in a similar fashion by different network slice providers. Both these cases should allow common mechanisms to map and allocate network slices over the network infrastructure.

Due to the availability of diverse technologies in control and data planes; the first step should be a top-down means to realize a slice with a common technology independent information model. It may describe a resource-centric slice with connectivity, storage, and compute resources, network functions, and operational requirements, that further get mapped to infrastructure resources and capabilities for run-time operations and monitoring. This model may be used by an orchestrator onboarding function for creating instances of network slice services and distributing to network infrastructure providers.

9. Conclusion

A service should typically need a network slice for one of those reasons:

(1) The service cannot provide optimal experience on a best-effort network.

(2) It is inefficient and expensive to build a separate infrastructure.

The separation from a generalized network, should allow new services to use newer or different protocols in network, transport and management layer/plane for that service (as in the case of ICN, mMTC, uRLL). The goal of Network slices is to offer enriched service verticals with very different network capability and performance demands but also simplify from the traditional service delivery models.

There is need for a uniform framework for end to end network slicing specifications that spans across multiple technology domains and can drive extensions in those technolgy-areas for support of Network slices.

10. Security Considerations

The security considerations apply to each kind of slice. In addition general security considerations of underlying infrastructure whether isolated communication with in a slice apply for links using wireless technologies.

11. IANA Considerations

There are no IANA actions requested at this time.

12. Acknowledgements

Note, the 5GEX L2VPN and L3VPN usecase is an independent contribution by authors and is not endorsed by 5GEX. Many thanks to the following reviewers for providing details for several use cases and for helping with the review of the document.

Stewart Bryant (stewart.bryant@gmail.com), Hannu Flinck (hannu.flinck@nokia-bell-labs.com), Med Boucadair (mohamed.boucadair@orange.com), Dong Jie (dong.jie@huawei.com).

13. References

13.1. Normative References

[I-D.bernardos-nfvrg-multidomain]
Bernardos, C., Contreras, L., Vaishnavi, I., and R. Szabo, "Multi-domain Network Virtualization", draft-bernardos-nfvrg-multidomain-03 (work in progress), September 2017.

[I-D.dt-detnet-dp-sol]
Korhonen, J., Andersson, L., Jiang, Y., Finn, N., Varga, B., Farkas, J., Bernardos, C., Mizrahi, T., and L. Berger, "DetNet Data Plane Encapsulation", draft-dt-detnet-dp-sol-02 (work in progress), September 2017.

[I-D.geng-netslices-architecture]
67, 4., Dong, J., Bryant, S., kiran.makhijani@huawei.com, k., Galis, A., Foy, X., and S. Kuklinski, "Network Slicing Architecture", draft-geng-netslices-architecture-02 (work in progress), July 2017.

[I-D.ietf-l2sm-l2vpn-service-model]
Wen, B., Fioccola, G., Xie, C., and L. Jalil, "A YANG Data Model for L2VPN Service Delivery", draft-ietf-l2sm-l2vpn-service-model-03 (work in progress), September 2017.

[I-D.ietf-opsawg-service-model-explained]
Wu, Q., LIU, W., and A. Farrel, "Service Models Explained", draft-ietf-opsawg-service-model-explained-05 (work in progress), October 2017.

[I-D.pularikkal-virtual-cpe]
Pularikkal, B., Fu, Q., Hui, D., Sundaram, G., and S. Gundavelli, "Virtual CPE Deployment Considerations", draft-pularikkal-virtual-cpe-02 (work in progress), February 2017.

[I-D.qiang-netslices-gap-analysis]
Qiang, L., Martinez-Julia, P., 67, 4., Dong, J., kiran.makhijani@huawei.com, k., Galis, A., Hares, S., and S. Slawomir, "Gap Analysis for Transport Network Slicing", draft-qiang-netslices-gap-analysis-01 (work in progress), July 2017.

[RFC8049] Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8049, DOI 10.17487/RFC8049, February 2017, <https://www.rfc-editor.org/info/rfc8049>.

13.2. Informative References

[_5GICN_] IEEE Communication, "Delivering ICN Services in 5G using Network Slicing. 'Asit Chakraborti, Syed Obaid Amin, Aytac Azgin, Ravi Ravindran, G.Q.Wang'", May 2017, <https://arxiv.org/abs/1610.01182>.

[ICNRG] IRTF, "ICN Routing Group", November 2016, <https://irtf.org/icnrg>.

[Tactile-Internet]
ITU-T, "Technology Watch Report, The Tactile Internet", August 2014, <https://www.itu.int/oth/T2301000023/en>.

[TR_3GPP.33.899]
3GPP, "Study on the security aspects of the next generation system", 3GPP TR 33.899 0.6.0, November 2016, <http://www.3gpp.org/ftp/Specs/html-info/33899.htm>.

[TR_3GPP.38.801]
3GPP, "Study on new radio access technology Radio access architecture and interfaces", 3GPP TR 38.801 1.0.0, March 2017, <http://www.3gpp.org/ftp/Specs/html-info/38801.htm>.

[TR_3GPP_38.913]
3GPP, "Study on scenarios and requirements for next generation access technologies", 3GPP TR 38.913 14.2.0, March 2017, <http://www.3gpp.org/ftp/Specs/archive/38_series/38.913>.

[TS_3GPP.23.501]
3GPP, "System Architecture for the 5G System", 3GPP TS 23.501 0.2.0, February 2017, <http://www.3gpp.org/ftp/Specs/html-info/23501.htm>.

[TS_3GPP.23.502]
3GPP, "Procedures for the 5G System", 3GPP TS 23.502 0.2.0, February 2017, <http://www.3gpp.org/ftp/Specs/html-info/23502.htm>.

[TS_3GPP.28.500]
3GPP, "Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions", 3GPP TS 28.500 1.3.0, 11 2016, <http://www.3gpp.org/ftp/Specs/html-info/28500.htm>.

[VCPEBBF] Broadband Forum, "TR-345 Broadband Network Gateway and Network Function Virtualization", Dec 2016, <https://www.broadband-forum.org/technical/download/TR-345.pdf>.

Authors' Addresses

Kiran Makhijani
Huawei Technologies
2890 Central Expressway
Santa Clara CA 95050
USA

Email: kiran.makhijani@huawei.com

Jun Qin
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095

Email: qinjun4@huawei.com

Ravi Ravindran
Huawei Technologies
2890 Central Expressway
Santa Clara CA 95050
USA

Email: ravi.ravindran@huawei.com

Liang Geng
China Mobile
Beijing 100095
China

Email: gengliang@chinamobile.com

Li Qiang
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: qiangli3@huawei.com

Shuping Peng
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: pengshuping@huawei.com

Xavier de Foy
InterDigital Inc.
1000 Sherbrooke West
Montreal
Canada

Email: Xavier.Defoy@InterDigital.com

Akbar Rahman
InterDigital Inc.
1000 Sherbrooke West
Montreal
Canada

Email: Akbar.Rahman@InterDigital.com

Alex Galis
University College London
London
U.K.

Email: a.galis@ucl.ac.uk

Giuseppe Fioccola
Telecom Italia
Italy

Email: giuseppe.fioccola@telecomitalia.it