5G Neutral Hosting

By

BORJA OTURA GARCIA

Department of Electrical and Electronic Engineering
UNIVERSITY OF BRISTOL

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of MASTER OF SCIENCE in the Faculty of Engineering.

NOVEMBER 2020

Word count: Twelve thousand eight hundred and eighteen

Abstract

The Neutral Host concept proposes a solution for the increase in cell density required by 5G to support the flexibility promised to support diverse use cases, such as enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC) and massive Machine Type Communications (mMTC). This work evaluates the state of the art and current associated technologies and proposes a change in the model of infrastructure sharing. A Neutral Host business model is proposed as well as an architecture that leverages on Network Function Virtualisation (NFV), Software Defined Networks (SDN), Multi-access Edge Computing (MEC) and Network Slicing to enable multi-level slicing and deployment automation in a shared infrastructure. An implementation of an automated EPC deployment relevant to such scenario is presented and results evaluated.

Dedication and acknowledgements

This dissertation is dedicated to Ana for her unconditional support, and to my friends at the University of Bristol for helping me approach the hurdles along the way.

AUTHOR'S DECLARATION

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: .....BORJA.OTURA.GARCIA..... DATE: .....10.DECEMBER.2020.....

TABLE OF CONTENTS

List of Figures

CHAPTER 1

INTRODUCTION

5G is the 5th generation of cellular networks. Figure 1.1 shows the evolution of cellular technologies from the 1st generation of analog communications, the introduction of digital technologies and text messaging service and later the first narrow-band internet connections in 2G, passing through the popularisation of mobile data services in 3G and real mobile broadband in 4G, to the currently in development 5G, where low latency, higher speed data rates and increased number of connected devices are the key features.

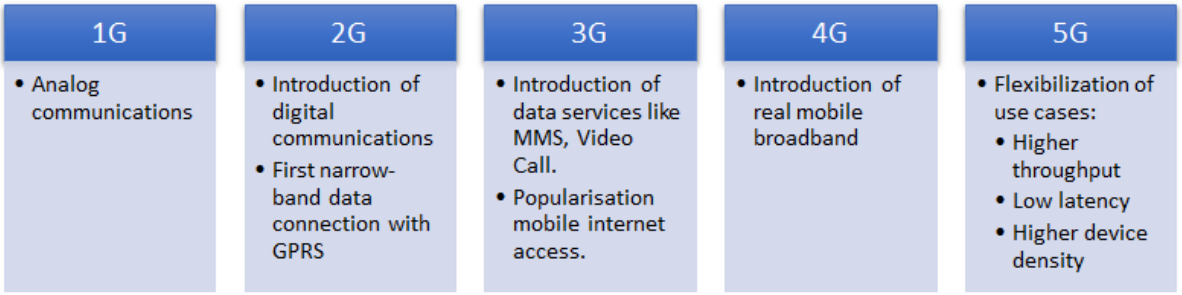

Figure 1.1: Mobile Networks Evolution to 5G

Unlike previous generations, the imminent deployment of 5G promises to provide an answer, not only for the requirements of mobile broadband consumers, but also for the Internet of Things connectivity as well as services requiring ultra-reliable and low latency communications such as autonomous vehicles. To support this, current networks will need to transform by deploying Multi-access Edge Computing (MEC) platforms over Network Function Virtualisation (NFV) infrastructures, leveraging the use of Software Defined Networking (SDN) technologies as well as appropriate Access Networks. This combination enables the creation of logical abstractions

of networks that can be subdivided into Network Slices, each with properties that meet the requirements of a specific service (i.e. high throughput, low latency, high number of connected devices). On the access side, 5G deployments, especially in the mmWave spectrum range (24GHz - 100GHz candidate for mobile applications) require an increase in the number of cells, either by the use of Small Cells or Cloud RAN implementations. This requirement creates current Mobile Network Operators (MNOs) a problem in the Site Acquisition process, specially in high density urban environments, and new formulas are required to achieve the desired coverage and service levels. Similarly, in rural areas where demand is limited, parallel single operator deployments may be challenging to justify from investment vs. return point of view.

The concept of Neutral Hosting proposes a solution to this problem. In a Neutral Host, a common infrastructure is shared so a single access site can serve the subscribers of multiple MNOs, thus reducing deployment costs and increasing efficiency. Local authorities are in a privileged position to become a Neutral Host as they own multiple assets spread across cities (lampposts, street cabinets, etc.) that would accelerate the deployment phases. In fact, we could consider these networks as a service offered by the Neutral Host to MNOs. Local authorities would benefit and justify the initial investment by guaranteeing the coverage to its citizens, the final users of the services.

There are, nonetheless, challenges that need to be addressed in order to design a model that can deliver these services with guarantees to the MNOs in their ability to continue offering the same or better service quality that they would if they deployed their own networks, while maintaining the network neutrality towards them. On the technical plane, some of these challenges include: the appropriate management of the radio spectrum shared resources, the integration among the MNOs slice in the Neutral Host and their own network seamlessly in the 5G context, and the ability of the Neutral Host to interact with the Operations and Business Support Systems (OSS/BSS) of the MNOs to manage the orchestration of services. Other challenges come from legal and regulatory perspective where spectrum license holder obligations need to be fulfilled, and new spectrum allocation policies, as well as security, integrated data management and privacy, may need to be considered.

CHAPTER 2

LITERATURE REVIEW

This chapter reviews the state of the art and existing literature around the 5G Neutral Host. First, a brief study of the technologies supporting 5G is introduced and then an assessment of the existing business models and related spectrum considerations is presented.

5G introduces into mobile networks the flexibility to provide communication services adaptable to different scenarios: enhanced mobile broadband (eMBB), massive IoT scenarios (MIoT) and ultra reliable low latency communications (URLLC), the three slice types specified by 3GPP [5]. This flexibility is supported on, and leverages five main technologies or concepts that are considered the basis of the 5G System:

- A new access technology, 5G New Radio (5GNR).
- Software Defined Networks
- Network Function Virtualisation
- Multi-Access Edge Computing
- Network Slicing

The introduction of a flexible numerology in the 5GNR interface that the 3GPP specified in its Release 15 [2] of the cellular standard enables the support for this variety of scenarios. However, it is assumed that not all scenarios will be deployed on every band in all configurations. Therefore, a thorough radio network planning to map the requirements in terms of capacity, performance and coverage demands for each type of service into the characteristics of different radio bands will be critical. While lower frequencies with better propagation properties would be adequate for MIoT use cases due to their propagation characteristics, the use of higher frequency bands like

mmWave will be required in urban environments to provide the necessary performance for eMBB scenarios, as well as URLLC where latency is critical. This fact, will drive an increase in the density of cells (referred to as Small Cells when they use low transmit power and have a limited footprint and range) operating the higher frequency bands. *Neokosmidis et al.* [30] describe how this increase in demand for available sites for cell deployment can create a market imbalance and propose the Neutral Host as a solution where an entity wholesales the network resources to third parties (i.e. the MNOs in this case), avoiding the need to deploy parallel infrastructures, specially in high density areas like cities. Already, back in 2012, *(Mobile infrastructure sharing (GSMA)* [21] analysis reported on the benefits of infrastructure sharing and its acceptance or even encouragement from the regulators. The analysis reports on different levels of infrastructure sharing, specially for 2G and 3G networks at the time. Some of the findings were that, although infrastructure sharing increased competition, an increasing number of infrastructure sharing agreements between operators were being signed, due in some cases to the lack of available sites in urban areas.

Most of the CAPEX required to build a mobile network is contributed by the Radio Access Network (RAN). The Neutral Host concept brings benefits in costs reduction (*Infrastructure Sharing: An Overview (GSMA)* [22]), spectrum efficiency and network flexibility (*Liang et al.*[27]). The adoption in 5G of Network Virtualisation technologies, Software Defined Networks and Network Slicing, makes the Neutral Host more relevant than ever before, as virtualisation of resources enable operators to better control their networks running on third party infrastructures. *Liang et al.* [27] describes virtualising mobile networks as "the process of abstracting, slicing, isolating, and sharing of mobile cellular networks". Mobile networks are composed of spectrum resources and infrastructure resources (i.e. Radio Access Networks [RAN], Core Networks [CN], and transport networks). The authors propose a business model identifying 3 roles: Service Providers (SPs), Mobile Virtual Network Operators (MVNOs), and Infrastructure Providers (InP), at matching levels with the Cloud Computing "Everything as a Service" (XaaS) model (*Duan et al.*[10]): Software as a Service (SaaS), Network as a Service (NaaS) and Infrastructure as a Service (IaaS) respectively. *Doyle et al.*[9] proposes a new value chain model for Communication Service Providers (CSPs) to create virtual networks composed using a pool of resources, including spectrum, owned or licensed to a particular Infrastructure Provider. A decoupling of infrastructure and spectrum is proposed, allowing the provision of the service through the most appropriate resource available. In the case of spectrum, as we will discuss further in this chapter, this vision enables incumbent license holders to lease part or all of its licensed spectrum to a Neutral Host that can help them monetise it more efficiently. There are, however, other resources like transport or computing resources which will be key to allow for the virtualisation of the infrastructure to enable efficient sharing.

In the case of RAN Virtualisation, there are multiple research studies that are focusing on virtualisation of radio resources from different perspectives. *Liang et al.*[27] identifies three types

of virtualisation of wireless resources, i.e. spectrum-level slicing, analogous to dynamic spectrum sharing, network-level slicing, commonly by virtualising the MAC scheduling function (*Zaki et al.* [39]), and flow-level slicing which would be equivalent to multiplexing end to end flows from different operators. *D'Oro et al.* [8] proposes a framework for CSPs to request reservation of scheduled radio resources from an Infrastructure Provider based on the operator's submitted intent, in terms of expected number of users and quality of service, however it does not tackle how the interconnection with the Core Network and end to end service is realised. *Schmidt et al.* [37] leverages the OpenAirInterface [33] opensource LTE implementation and extends FlexRAN Software Defined RAN platform presented in [18] to present FlexVRAN, demonstrating a RAN virtualisation platform capable of slicing heterogeneous RAN resources to provide multi-tenancy by, first, abstracting the heterogeneous resources into "functionally complete" logical base-stations, and then, abstracting the resources of the logical entity and offering them to multiple tenants in isolation.

Research efforts funded by the European Union's Horizon 2020 research and innovation programme, like *5GCity* [35] and *SESAME* [19] projects present respective architectures for realisation of network sharing and edge deployments. The presented platforms, however, limit the control over the shared resources by presenting the infrastructure at orchestration level and, the former, doesn't tackle the inter-connection with the CSPs wider network.

This work proposes a combination of the technologies that support 5G to enable a Neutral Host architecture that allow operators to integrate a slice of the infrastructure into their wider network, while maintain control over the virtual deployment. The following sections in this chapter give an overview of the related technologies to consider within a Neutral Host, as well as business and spectrum regulation considerations.

2.1 Related Technologies

2.1.1 Software Defined Networks (SDN)

Software Defined Networking (SDN) is a new approach to network architectures that aims to provide means for a more agile network management by leveraging application programming interfaces (API). SDN term was originally associated to the separation of Control Plane and User Plane of network devices but it is evolving in industry to refer widely to network automation and programmability. *Kreutz et al.* [26] present a comprehensive survey on the technologies and research challenges around the SDN topic.

One of the most important characteristics of SDN is the centralisation of network intelligence. The control logic is delegated to an SDN Controller which has visibility and authority over the whole controlled network. This control is exercised over the network devices through the controller's southbound API. The distributed network devices can then be simplified to focus on implementing the forwarding settings received by the controller. One of the most popular SDN

southbound protocols is OpenFlow [29]. The programmability of the network, with end to end visibility and authority can then be offered to software network applications via the controller's northbound API.

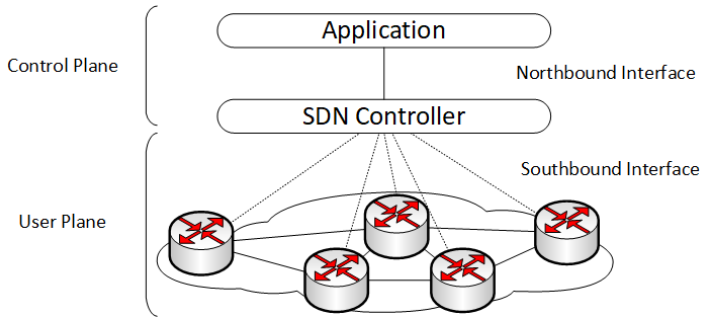

Figure 2.1: SDN Architecture

The term network virtualisation applies in SDN when multiple independent network abstractions utilise the same shared physical resources. In the scenario of a Neutral Host deployment, in order for the CSP to maintain the control over the deployment, it is not sufficient with the coexistence of multiple tenants on the Data plane, but also multiple Control Plane instances need to be able to present an abstracted view of the resources that form part of the logical network and provide the means for its control. This control needs to be carefully coordinated to guarantee isolation and avoid overlapping between the resources used by the different networks. *Sherwood et al.* [38] explain the concept of Network Virtualisation Hypervisors, in reference to computing hypervisors, and present FlowVisor, which acts as a proxy between network resources and the controllers of each slice providing isolation with transparency. *Blen et al.* [7] present a comprehensive survey and categorisation of different approaches to SDN hypervisors since.

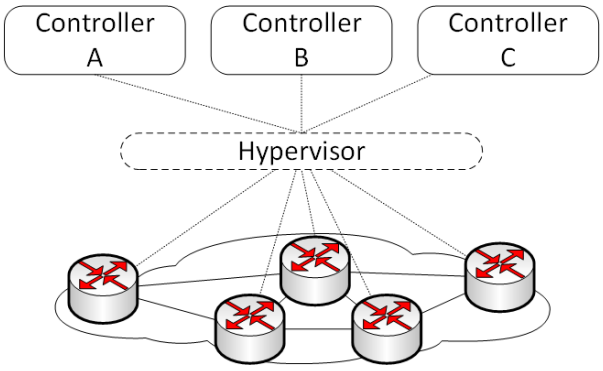

Figure 2.2: SDN Hypervisor

2.1.2 Network Function Virtualisation (NFV)

Network Function Virtualisation is a network architecture model proposed and specified by the European Telecommunications Standards Institute (ETSI). This model heavily relies on computing virtualisation models, like IaaS, and SDN to provide a platform for the deployment of networks composed of virtualised functions. ETSI NFV standard [13] proposes a framework to enable a network operator to deploy and manage networks composed of these virtual entities in a programmatic way. Inter-operability between different function vendors and the ability to deploy them on heterogeneous infrastructures in a programmatic way are the key aspects of the proposed framework.

The NFV framework is divided in 3 parts:

- Virtual Network Functions (VNF): Each of the software components that implement a certain network function.
- Network Function Virtualisation Infrastructure (NFVI): Virtualisation infrastructure including computing, storage and network resources that support the deployment of VNFs
- Network Function Orchestrator (NFVO): Management and Orchestration function responsible of the lyfecycle of the VNFs deployed over the NFVI.

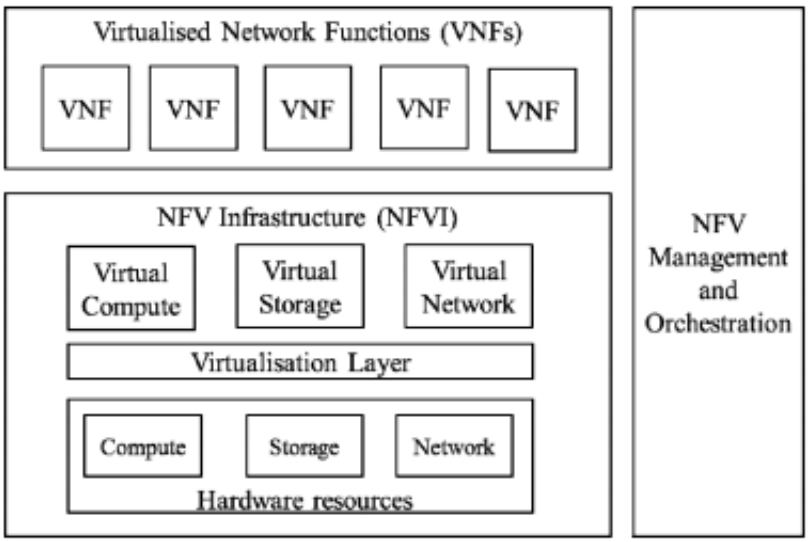

Figure 2.3: High-level NFV Framework [13]

For VNF specification, ETSI proposes VNF packages that are composed of images with the specific software that implements the relevant function, and a VNF Descriptor that specifies the capabilities of the function, interfaces, and other requirements such as CPU, Disk, RAM, or monitoring and scaling capabilities. ETSI specifies the rules for the creation of VNF Descriptors

based on TOSCA (Topology and Orchestration Specification for Cloud Applications) [34] and/or YANG (Yet Another Next Generation) [24] data modelling languages. These languages are also used to describe Physical Network Functions (PNFs), which are network functions deployed on dedicated hardware, but developed and modelled according to the NFV framework. VNFs and PNFs can then be combined together into Network Services (NS) which correspond to services that can be orchestrated by the NFVO.

NFV Management and Orchestration principles allow for separation of the virtualised functions from the infrastructure they run on, by leveraging abstraction of the available resources (compute, storage and network) and the creation of common standardised interfaces to manage the lifecycle of VNFs and NS (i.e. Onboard, Instantiate, Scale, Update, Terminate) [14].

2.1.3 Multi-Access Edge Computing (MEC)

Multi-access Edge Computing, as defined by ETSI [17], "enables the implementation of MEC applications as software-only entities that run on top of a virtualisation infrastructure, which is located in or close to the network edge". This approach provides benefits in reduction of latency by bringing users closer to the accessed resources, as well as an improvement in network congestion by reducing the residence time (and 'mileage') in the network.

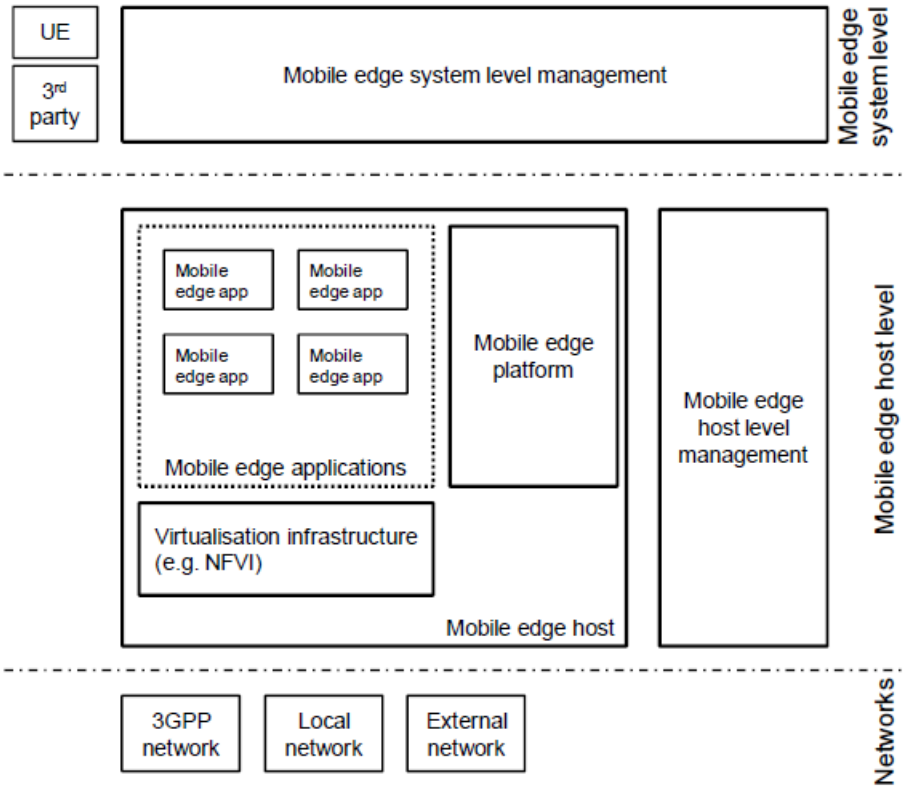

Figure 2.4: Mobile Edge Computing framework [17]

As shown in figure 2.4, ETSI proposes a reference framework [17] for the realisation of these benefits in a mobile network. This framework is composed of three main components:

1. MEC System level management. Its principal function is orchestration of the whole MEC System.

2. MEC Host is the local entity formed by:

    - MEC Platform: in charge of managing the MEC services available at the MEC host and making them available for consumption. These can be provided by the platform itself or by a third party MEC Application running in the MEC host.
    - MEC Applications: Applications that are instantiated on a MEC host.
    - Virtualisation infrastructure (NFVI): Virtualisation infrastructure supporting the MEC applications running on the host.

3. MEC Host Level Management. Manages the coordination between MEC platform, applications and infrastructure at a host level.

Some important services provided by the proposed MEC platform are:

1. Radio Network Information: Provides information about the radio conditions, measurement and statistics related to the User Plane and information related to the UEs associated with a MEC Host.

2. Location: Provides location information (i.e. geo-location, cellId,..) related to the UEs and radio nodes associated to the MEC Host.

3. Traffic Manager: Allows for shaping and bandwidth allocation of the traffic with the MEC applications.

This framework has been defined with an integrated vision with NFV where both standards inter-operate with one another and it can be directly implemented over a standard NFV infrastructure. This has led to MEC implementations in industry and research that do not follow the MEC architecture but, instead, simply leverage an NFV infrastructure located close to the edge, losing functionality provided by the MEC reference architecture, or providing it in a non standardised way. The authors of [23] [32] present LL-MEC (Low Latency MEC), an open-source, ETSI MEC standard based platform for mobile edge services. The platform creates an abstraction of the infrastructure resources, enabling the programmatic control at the edge for low latency services, and offers a framework for MEC applications to access exposed network information to these services and granting them the desired level of control.

2.1.4 Network Slicing

The term Network Slicing is based on the concept of virtualisation, which allows for physical resources to be shared as they are split into several virtual sets and allocated to different consumers in mutual isolation. Network Slicing is pivotal to 5G and how different use cases with specific traffic characteristics can coexist within a common infrastructure.

In 3GPP, and aligned with the proposal for 5G slicing from NGMN (Next Generation Mobile Networks) [31], the concept of Network Slicing is introduced from 5G (3GPP 5G System Architecture. TS 23.501 Release 15 [5]). A 5G slice is the combination of 5G virtual network functions and/or physical resources required to provide a specific service in isolation to other services provided over the same resources. A network slice is defined within the domain of a PLMN and is composed of a set of core (CN) Control and User Plane functions and an Access Network (AN) or N3IWF function in case of non-3GPP access. When an UE requests to attach to the network, it provides the 5G System with a list of up to 8 slices it wishes to connect to. Each slice is identified by a "Service/Slice Type" (SST) and "Slice Differentiator" (SD).

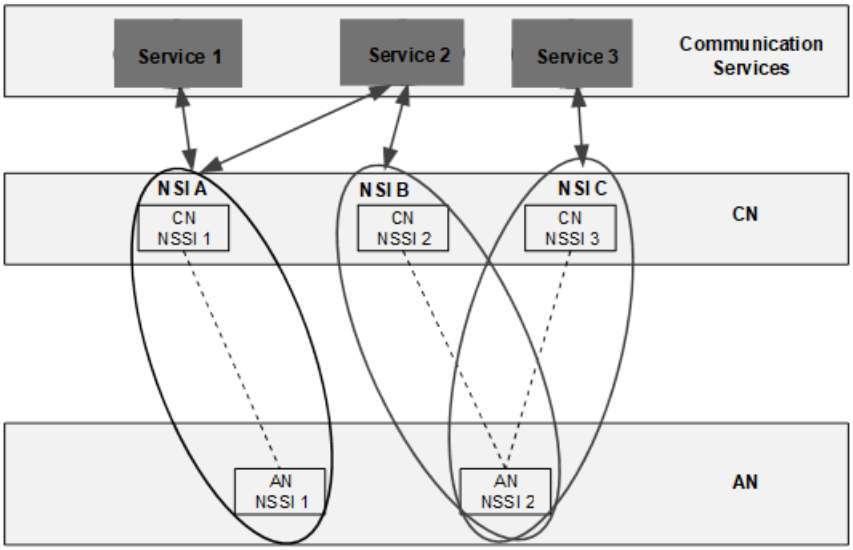

Figure 2.5: 3GPP Rel.15 End to End services provided by NSI(s) [4]

The 5G system uses these identifiers to obtain the details of the network function instances that compose the requested slice instance. Network Slice Instance (NSI) is defined by 3GPP TR.28.801 [4] as "a set of network functions and the resources for these network functions which are arranged and configured, forming a complete logical network to meet certain network characteristics". A communication service can consume one or several NSIs, by creating one or more PDU (Packet Data Unit) sessions, each associated to a single NSI. The resources can be grouped in and identified by Network Slice Subnet Instances (NSSI), which then can be combined to form an NSI (figure 2.5).

ETSI Report on Network Slicing Support with ETSI NFV Architecture Framework [15] explores and highlights the capabilities of SDN and NFV to provide multi-tenant support across several Infrastructure Providers. Figure 2.6 shows the relation between 5G slicing elements and NFV. In NFV, Network Slice and Network Slice Subnets are implemented indistinctly through Network Services.

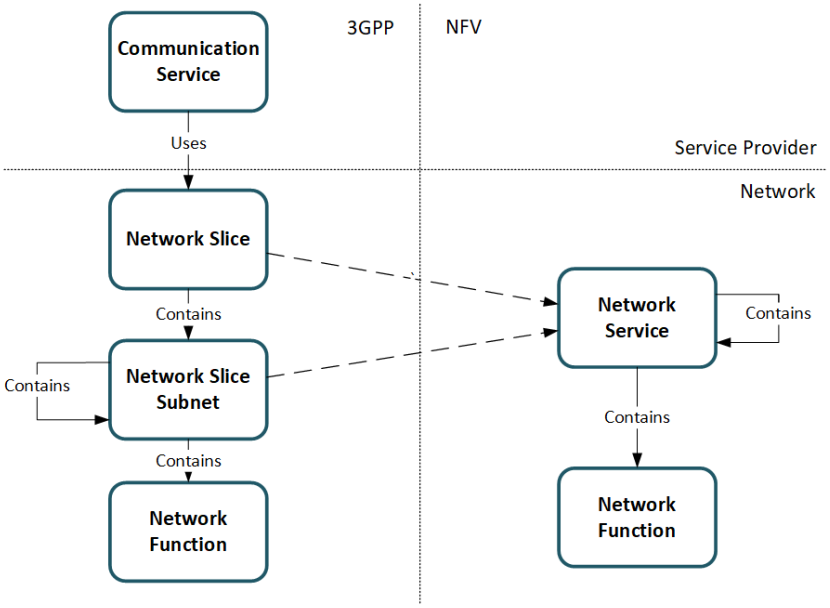

Figure 2.6: Mapping 3GPP Network slicing with NFV [15]

The concept of neutral hosting 5G networks, exploits the idea of multi-tenant NFVI, where the provider's infrastructure resources are sliced into several virtual sets of resources allocated to the operators respectively. This set of resources can then be used by the operator to deploy 3GPP functions as required to implement multiple 5G slices. This concept will be further detailed in chapter 3.

2.1.5 3GPP 5GS Architecture

The 5G architecture is specified in 3GPP TS 23.501 Release 15 [5]. It is specified as a Service Based Architecture, in the sense that the functions offer services that are accessible to other authorised functions, as opposed to a Reference Point Architecture where interfaces are specified between functions one to one.

The 5G System is composed of the following main Network Functions (NFs):

- User Equipment (UE)
- (Radio) Access Network ((R)AN): Either one or a combination of a 5G New Radio or a 4G radio, and/or a non 3GPP access network.

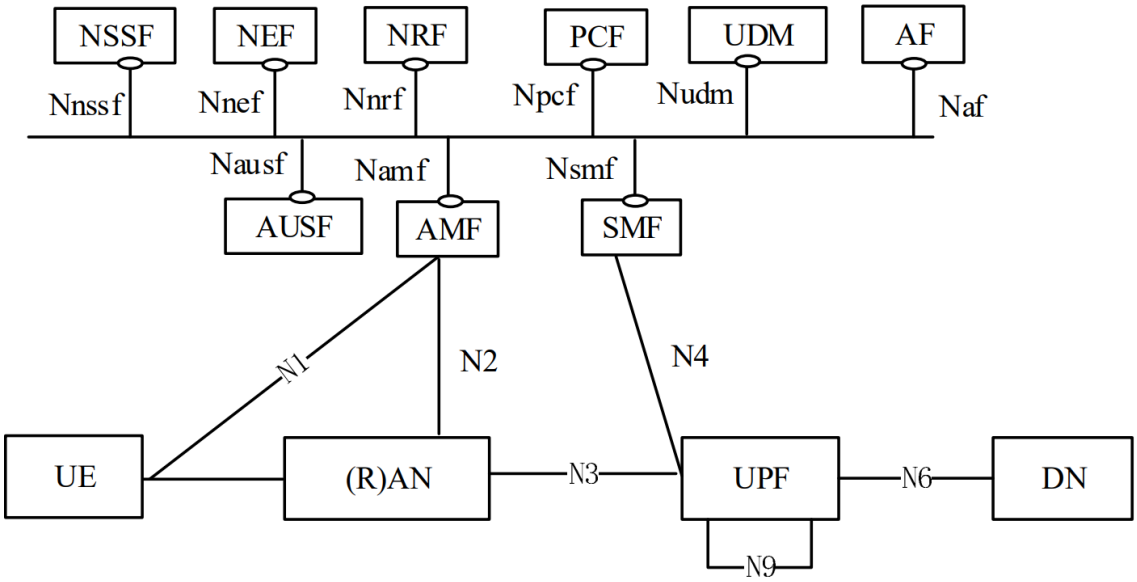

Figure 2.7: 5G System architecture [5]

- Access and Mobility Management Function (AMF): This key function terminates the Control Plane interfaces of both (R)AN and UEs, mainly supporting Authorisation and Authentication, UE Registration, Mobility and transport for Session Management messages to the SMF.
- Session Management Function (SMF): Provides Session Management for UEs, managing tunnels between (R)AN nodes and UPFs, allocation of IP addresses, reply to ARP requests, configuration of packet routing at the UPFs, as well as charging data collection, among others.
- User Plane Function (UPF): This function deals with the User Plane packets sent by the UEs through the (R)AN, based on SMF received configuration, QoS, enforcing policies, routing the packets to its destination Data Network.
- Policy Control Function (PCF): Provides SMF with the policies to be enforced on the User Plane.
- Authentication Server Function (AUSF): Supports access authentication.
- Unified Data Management (UDM): Supports the management of access authorization based on the UE's subscription as well as storing the functions currently serving a UE.
- Network Slice Selection Function (NSSF): This function supports management of allowed and configured slices for a UE.

- Network Repository Function (NRF): Discovers information about available network function instances and provides information about them to other functions when requested.
- Network Exposure Function (NEF): Securely exposes capabilities and events within the 3GPP network to external entities allowing for interaction with external applications
- Application Function (AF): An Application Function can communicate with the 5G Core to request actions on the UE traffic routing, policy applied, etc. It interfaces directly with other network functions or with the NEF if it is not part of the trusted domain.
- Data Network (DN): Networks made available to the UEs by the 5G System. This is referenced in within the system by a Data Network Name (DNN)

These are the main functions that support the 5G System. Other NFs are described in 3GPP TS 23.501 Release 15 [5], such as the Non-3GPP InterWorking Function (N3IWF) which adds support for non-3GPP Access Networks.

2.1.5.1 Network Sharing in 5G

Commercial deployments of previous 3GPP networks have focused on three main ways of sharing networks:

- Passive Sharing: Passive elements of the infrastructure are shared, like site real estate, tower mast space, power, etc.
- Active Sharing: Sharing of active electronic equipment, including antennae, transmitters and potentially spectrum depending on the specific agreement.
- National Roaming: The host operator allows other national operators or virtual operators (MVNO) to roam into its infrastructure.

There are three different approaches of active sharing that have been considered in legacy shared networks:

- Multi-Operator RAN (MORAN): Active elements of the RAN are shared, but the spectrum separation is maintained. The Core Networks remain totally separated. This type of sharing is not standardised by 3GPP specifications.
- Multi-Operator CN (MOCN): Spectrum and active elements of the RAN are shared. A single logical cell is radiated over a common spectrum and subscribers of host and guest operators are allowed to connect. The Core Networks remain totally separated.
- Gateway CN (GWCN): A further extension of the MOCN scenario. In this case, the core network control plane anchor (i.e. MME in LTE) is also shared while the user plane and other core control plane functions remain independent.

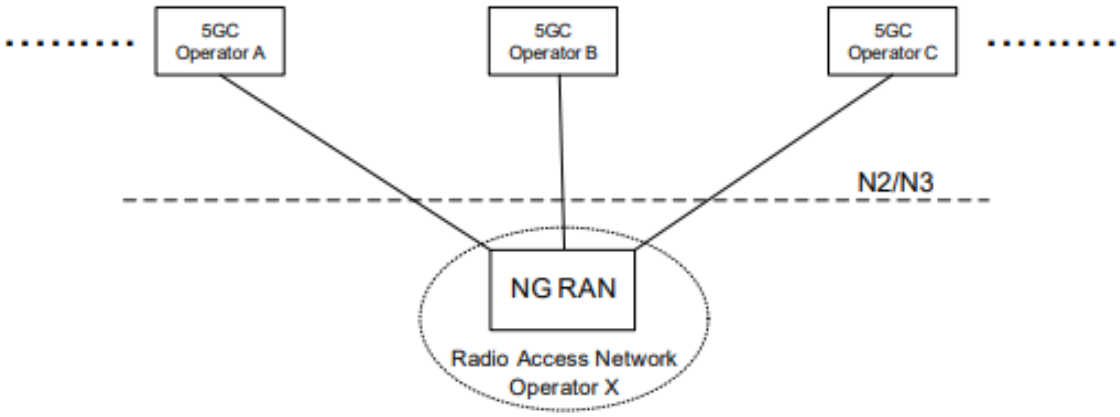

Figure 2.8: A 5G Multi-Operator Core Network (5G MOCN) in which multiple CNs are connected to the same NG-RAN [5]

As per 5G, only the MOCN model (figure 2.8) has been standardised from release 15. The introduction of Network Slicing and the capabilities of NFV to support multiple tenants offer, however, an extension to the infrastructure sharing possibilities like the one presented in this work.

2.1.5.2 MEC in 3GPP 5G Specification

The 5G system is capable of allowing users to benefit from accessing resources near the edge of the network, reducing latency and releasing pressure from transport networks.

From 3GPP TS 23.501 Release 15 [5], there are several ways this can be achieved, depending on the service requirements:

- UPF Re-selection: Change the UPF(s) that serve a PDU session to terminate in the required DN.

- Local Routing and Traffic Steering: Selected traffic is diverted to the local network by the User Plane. This can be done either by inserting an Uplink Classifier (ULCL) that selects between multiple PDU Session anchor points for a single PDU sessions, or a branching point in the case of IPv6 multi-homing PDU sessions.

- Applying the 5G System's Session and Service Continuity feature to allow for application/UE mobility.

- Using information from other NS (i.e. AF, PCF) in the system to modify the user plane selection and routing.

- Local Area Data Network (LADN): A DN can be accessible as an LADN under the LADN Service Area. An LADN Service Area contains a list of Tracking Areas where the LADN DNN is available for a DNN.

2.2 Business model and Regulatory considerations

This section explores the Neutral Host scenario justification from the business and regulatory perspective. First, we will look at how the network sharing model fits in the current business ecosystem from the main actors point of view, and second, we will explore the regulatory aspects that need to be considered in such scenario.

2.2.1 Business Model

The outpacing in growth of Digital-Native companies has favoured the trend among CSPs to move from merely providing connectivity to offering further end-to-end digital services like multimedia content distribution, IP voice and messaging, or other services focused on specific enterprise use cases or transforming into platform providers for 3rd party services [28].

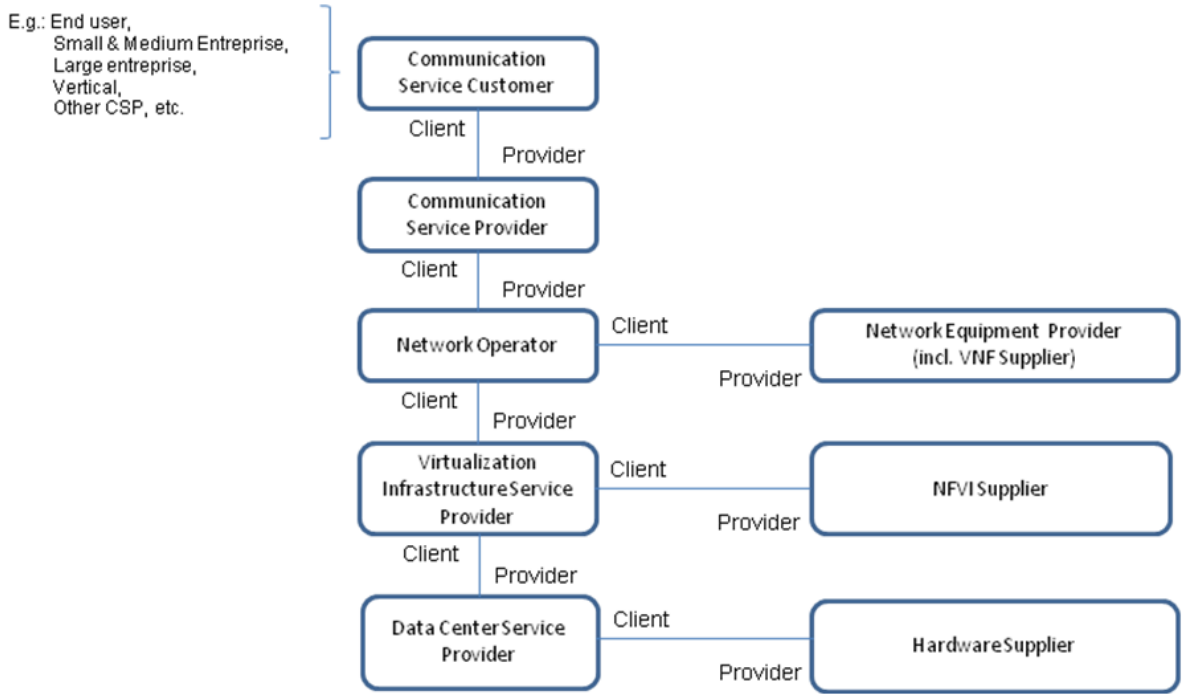

Figure 2.9: 5G Business roles [4]

This trend may generate a shift in the business strategy focus of CSPs. In the model presented by 3GPP TR 28.801 "Study on management and orchestration of network slicing for next generation network" [4] shown in Figure 2.9, Mobile Network Operators currently perform either the

Communication Service Provider (CSP) and Network Operator (NOP) role, or only the NOP role, wholesaling the network services to other CSPs, i.e. Mobile Virtual Network Operators (MVNOs). A third option would be to consume the services of 3rd party NOPs that provide services to multiple CSPs in specific geographic locations, such as rural areas, industrial premises, enterprises, local communities, etc.. These local NOPs may be promoted or funded by organisations with interests specific to such areas, i.e. local authorities, enterprises or communities. The proposed model is a win-win scenario where the NOPs fulfils the necessities of the local organisations, while reducing the capital expenditure (CapEx) and operating expenditures (OpEx) of deploying the new 5G networks.

DBS Group [36] estimates the benefits on Return On Invested Capital (ROIC) for Telcos from 12% to 15% when sharing or leasing the 5G network as opposed to owning it. The cost savings derived, could be invested on transforming into a model based on differentiation by digital services offerings, as the current differentiation value based in network performance or availability would be reduced when using a common infrastructure.

From the implementation point of view, DBS Group report cites sources that estimate up to 40% in asset savings and a cash flow improved on up to 31% when deploying a shared resources network.

The consortium behind 5GCity project previously mentioned in this chapter, proposes a business model for Neutral Hosts around analogous players as those in the 3GPP 5G value chain. A special mention is made towards the owners of spectrum, as a key resource for deploying mobile networks. MNOs have traditionally been the owners of radio-electric spectrum. 5Gcity, however, identifies other three scenarios, i.e. NH, NH + MNO or 3rd party ownership, evaluating each scenario, and highlighting the added complexity due to lack of proper regulation in terms of spectrum sharing and fair monetisation. 5GCity model for Neutral Host is based on the wholesaling of access and computing resources, through the platform developed by the project. The authors identify several potentially viable charging schemes, i.e. monthly subscription or dynamic charging per use of the resources.

2.2.2 Spectrum Licensing

One critical aspect of the Mobile Networks Neutral Host, is the inherent need for available spectrum to provide service equivalent in quality or better than the CSPs' own deployments. This section discusses the practicalities and regulatory considerations around spectrum licensing and availability to the Neutral Host.

There are two main ways in which the ever increasing requirements for mobile data communication can be accommodated, either by increasing the amount of spectrum dedicated to this use, or by increasing the efficiency in which this spectrum is utilised. In the UK, regulated by the Wireless Telegraphy Act 2006, RF transmitting equipment can only operate if authorised by a license or if it is explicitly exempt. The body that manages the spectrum for optimal utilisation

is the National Regulatory Authority (NRA), Ofcom, in the case of the UK. Ofcom's position is to study a combined approach to spectrum management for 5G and beyond, where strategies to increase the efficiency of available spectrum, like geographically limited licenses or Dynamic Spectrum Access (DSA), can complement the new 5G bands allocation plan.

Ofcom's current frequency band allocation model for cellular networks is by auction. In 2019, the UK's NRA stated the intention to explore further methods to encourage innovation and reduce entry barriers for new users by introducing two ways in which spectrum licenses can be applied for. Shared Access licensing provisions four frequency bands, for which commercially available equipment currently exist, for shared use. However, when we think about the Neutral Host, these bands are explicitly not allowed for national mobile broadband use. Local Access licensing, instead, is designed to reuse the frequency bands that are currently allocated to Mobile Operators, allowing new users to apply for authorisation to use a certain band at a specific location where it is underutilised. Ofcom has also stated their intention to explore automated tools for management of spectrum, like Automated Frequency Coordination databases [6].

As highlighted by the TM Forum [28], there will will be a big demand for location specific applications in the B2B market that could benefit from such licensing schemes. Although the two aforementioned new licensing schemes are not designed with a Neutral Host for national mobile operators in mind, it is a welcomed first approach in the direction towards a more efficiently managed spectrum. Similar approach could be taken in the future to allow for Neutral Host deployments to be licensed locally on certain bands.

Until new regulation allows for this scenario, current incumbents could potentially lease their licenses to improve the monetisation efficiency of their allocated spectrum. Regulation within the UK, allows for spectrum license trading in two forms, i.e. transfer and lease. The main difference between the two being that in the case of transfer, the original licensee gives up on its rights and obligations over the spectrum and Ofcom issues a new license to the new operator. In the case of leasing, the rights and obligations remain with the original licensee authorising the leaseholder by to use the spectrum by agreement. Ofcom is not involved in the leasing process.

CSPs leasing out part of their licensed spectrum to the Neutral Host, limited to geographical locations, seems to be an interesting approach for the creation of pools of available resources that can be more efficiently utilised, in a similar way as Virtual Machines can make more efficient use of computing resources by sharing hardware. Detailed, bespoke agreements could be drawn between the parts to, for example, guarantee that priority is given to contributors of spectrum to the pool up to the amount of contributed resources in situations of high utilisation, while still being able to access more resources than contributed while they are not occupied. *Giupponi et al.* [20] presented a business model based on similar inter-operator agreements and found that it mutually benefits operators, in the short-term by increased revenues for operators with lower market shares, and in the longer term in better user experience and reduced churn (subscribers porting to other operators) for operators with larger subscriber base. *Jorswieck*

et al.[25] demonstrates how tight scheduling coordination in spectrum sharing can result in a higher spectrum efficiency in terms of throughput and capacity. The Neutral Host could exercise the medium access scheduling role based on agreed rules.

CHAPTER 3

NEUTRAL HOST

A Neutral Host is a network solution that enables several tenants (e.g. CSPs) to access and exploit shared resources based on an agreement with the infrastructure owner, allowing them to create, operate, maintain and monitor a network slice of the physical infrastructure and seamlessly integrate it into its wider network if required.

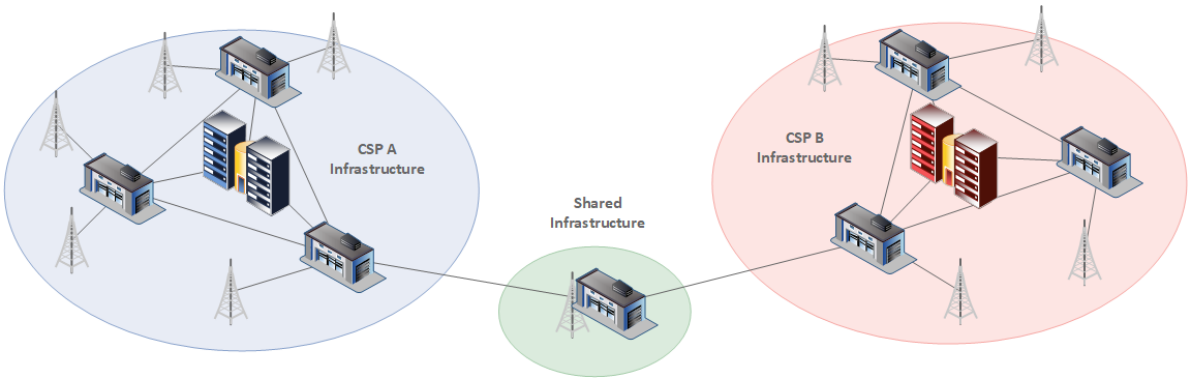

Figure 3.1: Infrastructure sharing

A Neutral Host system is described in this chapter. First, we will study the business model and identify the services that the Neutral Host is required to provide in a 5G scenario. Next, we will focus on the automation implications in 5G, as well as 4G network. Finally, an enabling system architecture is described.

3.1 Business Model

The approach of using shared networks can result on a Federated Network composed of the CSP own resources that is complemented by tenancies on 3rd party infrastructures when it is indicated. This could be due to business strategy, balance between deployment cost vs. expected return, and regulation, among other constrains.

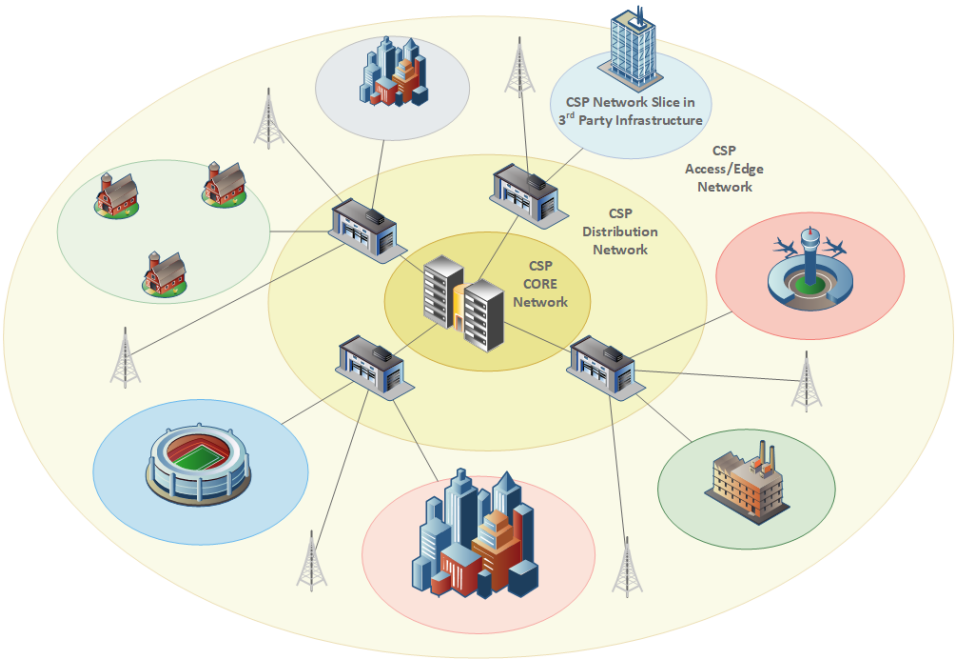

Figure 3.2: Federated Network

The higher frequency bands planned for 5G above 26 Ghz will drive an increase in the density of radios required to cover a particular area. The deployment and operation cost to run this new infrastructure could be reduced if entities such as local authorities, enterprises, large venues and/or industrial premises deployed their own infrastructure and leased the available resources partly or fully to CSPs. From the infrastructure owner's perspective, there is currently a strong interest in private 5G networks. The possibility of recovering some of the deployment cost by leasing infrastructure could encourage the investment in Neutral Host. Also, for local authorities, it can be a great strategy to foster local economy and attract investment in local development, as well as improve the citizens' connectivity and help reduce the digital divide.

The strategy of network sharing is not new to CSPs. Network sharing agreements have been signed in the past between CSPs to save costs. However, leaving aside the virtual MNO (MVNO) approach, these have consisted mainly in RAN Sharing, either passive sharing, when the parties share sites, masts, or passive equipment like antennae, feeders, etc. or active sharing, when the base station equipment is shared, normally using MORAN (Multi-Operator RAN) or less commonly MOCN (Multi-Operator Core Network) features.

In the case of 5G, and due to the exploitation of edge computing features to achieve the claimed performance improvements like reduced latency, new sharing options should be considered. Leveraging on NFV and SDN, radio sites (specially aggregation sites) will transform into small datacentres that are great candidates for sharing by means of virtualisation techniques. This transformation of RAN sites into edge datacentres will also enable new forms of active RAN sharing, based on virtualised RAN. This is a critical change from previous sharing scenarios, as it gives tenants increased flexibility and control over the deployed network while still saving costs of new infrastructure deployment.

As pointed out in cited literature, the main revenue streams from the Neutral Host come from the wholesaling of infrastructure. A charging scheme consisting on a basic tenancy fee and added dynamic charges per usage seems suitable. These dynamic charges could combine charges on traffic utilisation from the access layer and the current charging scheme of public cloud services.

Spectrum licensing is a critical topic in the Neutral Host discussion. Current spectrum licence holders are the very same tenants that would require accessing it from the Neutral Host. CSPs can monetise more efficiently their spectrum by contributing part of it to a pool that would be exploited by the Neutral Host at a certain location. This is could potentially be managed via an Automated Frequency Coordination database (a.k.a Spectrum Access System or Licensed Shared Access Controller). Agreements between the CSPs and the Infrastructure Provider would need to be formulated so spectrum licensees have a corresponding deduction on their usage charges when contributing spectrum. A different approach would be for spectrum to be made available locally by regulators and licensed directly to the Neutral Host. Regulatory bodies need to evolve and adapt their regulations to promote these innovative scenarios.

The proposed model differs from other presented models in that the tenant slice in the Neutral Host can become an integrated extension of the tenant wider network, rather than an isolated deployment, while maintaining a high degree of tenant control over the deployed slice.

3.1.1 Neutral Host Services

Based on the technologies involved in a 5G network, described on section 2.1, a CSP will be interested in 4 main services to be provided by 3rd party resources:

- **Access** to the network in the local area: Radio equipment needs to be deployed to cover the area served by the Neutral Host.

- **Processing** power close to the edge of the network: an NFV infrastructure will be required to provide edge services.

- Underlying **Network Resources**: This network integrates the NFVI and RAN together, as well as providing a gateway to external networks.

- Access to **Management Interfaces** from where a CSP can programmatically control its slice.

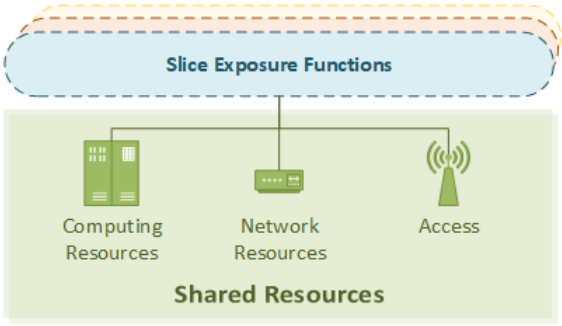

Figure 3.3: Neutral Host Services

These services dictate the requirements for the Neutral Host architecture and enable a CSP to integrate 3rd party infrastructure into its own network while retaining the control of its slice.

3.1.2 Slice definition in the Neutral Host context

A 5G Service provider interested in a tenancy on the Neutral Host infrastructure will most likely require to splice its slice in the Neutral Host into its wider network and maintain the ability to offer slices to its own users.

For this reason, an End to End (E2E) slice model that combines those of 3GPP 5G System, NFV, MEC, SDN domains described in 2.1.4 and, in a customised manner, one that includes every resource made available for sharing is required to be designed for the Neutral Host system.

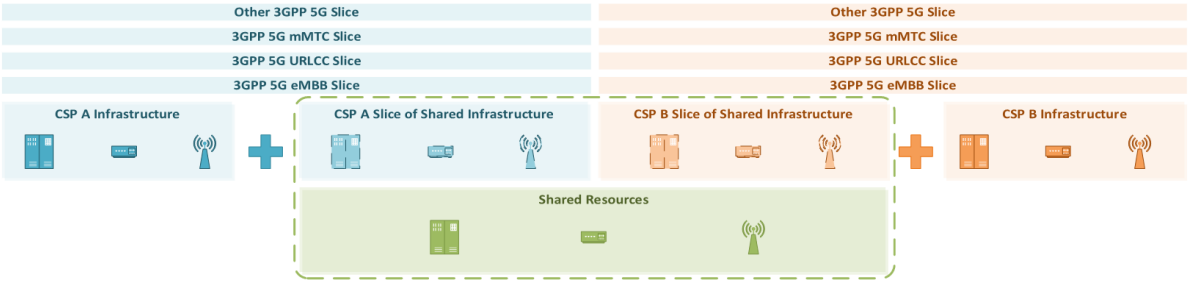

Figure 3.4: Neutral Host E2E Slicing

Starting from the top, CSP customers will be the final users in the system. They will, through the CSP Operations and Business Support Systems (OSS/BSS), manage and orchestrate a service request of a 3GPP 5G slice that expands across the whole network available to the CSP.

The service to the user may be deployed over the CSP own cloud infrastructure, over the infrastructure of a third party provider, or a combination of both. This would be the case when the user selects to deploy a service on a location where the CSP service is provided by a Neutral

Host. This fact should, however, be transparent for the user, who does not need awareness of the third party involved. This transparency translates into a requirement for the CSP to have total visibility and control over their slice on the Neutral Host infrastructure.

For the slicing model at the Neutral Host, and in order to abstract the operator from the sliced MEC Host, this work proposes the slicing of the NFV infrastructure and the underlying SDN network and RAN infrastructure to enable the deployment of a MEC platform per hosted operator if desired (Figure 3.5).

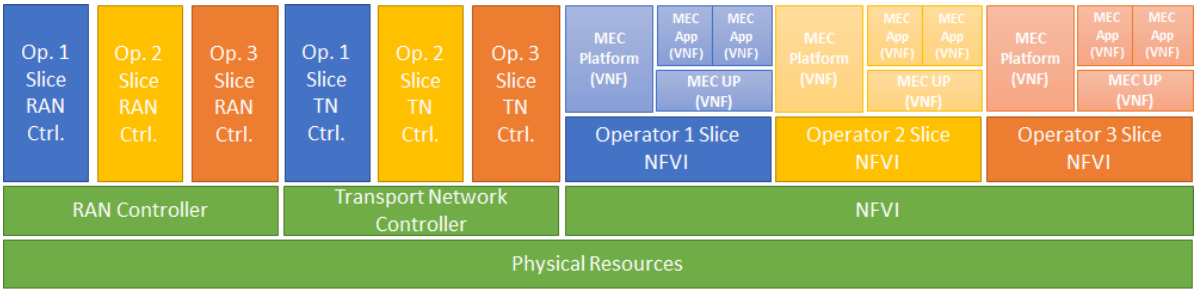

Figure 3.5: Neutral Host NFV Slicing for MEC

3.2 Automation

Arguably, one of the biggest gains obtained from the use of NFV and SDN in 5G is the ability to automate the deployment, instantiation, scaling and deletion of networks and their functions, specially useful to manage network slices. This capability needs to be maintained from the home network, across into the Neutral Host. As a consequence, the Neutral Host needs to provide the necessary interfaces for the guest to keep hold of this capability.

More importantly, coordination is required when automating the deployment of functions. The new functions need to be able to integrate with the wider network and these need to available for discovery.

In this section, 5G support for automated deployment of functions on a Neutral Host network is explained, as well as a proposal for a 4G implementation with automated configuration support.

3.2.1 5G Network deployment Automation

Release 15 of 3GPP standard for 5G [3] natively supports the automation of network function deployment. This feature is supported by the NRF and its service based interface Nnrf. A NF implementation can trigger the registration of the new instance, update of the registered information, notification about the status, or de-registration of its NF profile (NF type, the FQDN or IP address of its interfaces and other information specific to the service it provides) by interacting with the service provided by this interface.

Consequently, authorised NFs can query the NRF to discover services offered by other NFs, as well as subscribe/unsubscribe for notifications about services that can be consumed and information about the NF that provide it.

This is particularly useful when deploying in an NFV infrastructure, a NF can be packaged as a VNF. When an instance of this VNF is created, the NF can trigger the registration with the NRF as part of day-1 operations (phase for configuration and registration of the VNF application).

In the context of Neutral Host, when a CSP needs to deploy a service at the edge of the network, the VNF(s) providing this service can be packaged with an UPF into a NS, and this be instantiated on demand into the slice of the operator within the Neutral Host infrastructure. The UPF can, on day-1 operations, register itself into the NRF of the CSP as the PDU Session Anchor for a specific DNN within the TAC service area (i.e. LADN). This is represented in Figure 3.6.

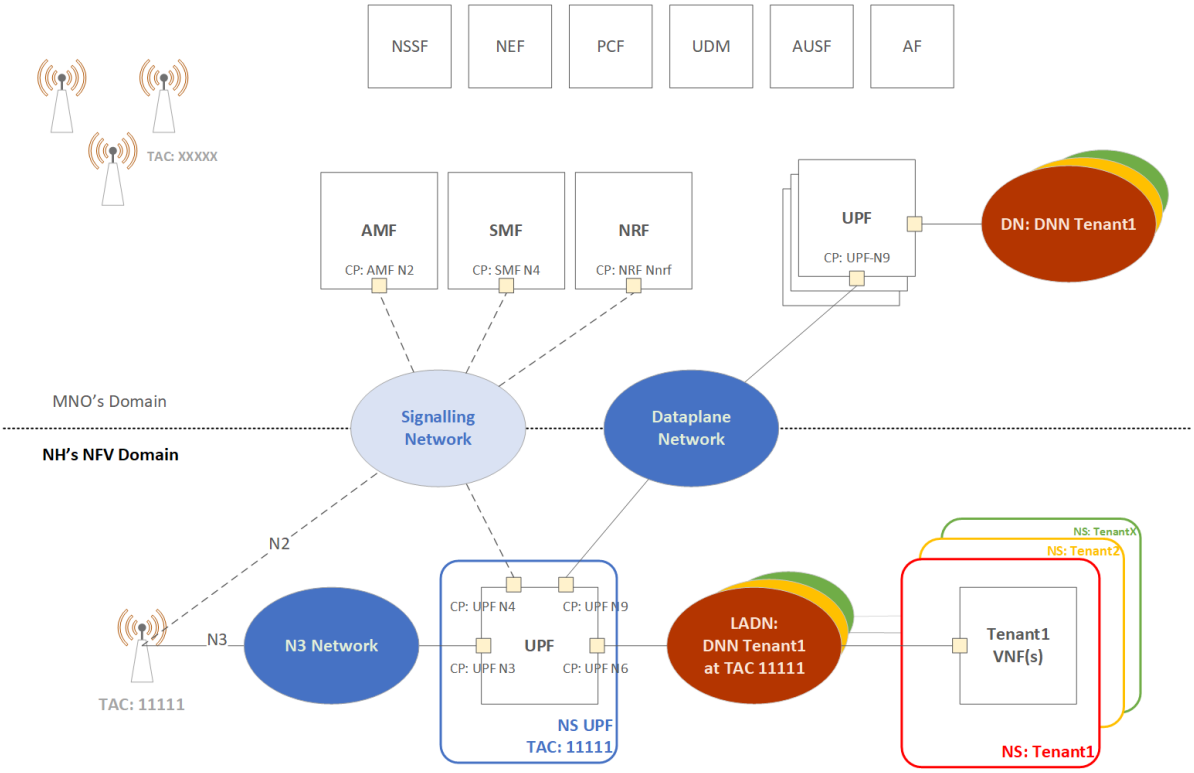

Figure 3.6: 5G-CN Automation

3.2.2 LTE Edge Network deployment Automation

For this work, the scenario considered consists in the deployment of the necessary elements to allow for data sessions from UEs, within the service area of the Neutral Host, to terminate locally into a PDN that provides a service at the edge of the network. To this effect, we will focus on the Distributed SGW-PGW scenario for MEC in 4G described in section A.1.

SGW and PGW are the two main functions required to provide this service. A SGW is needed as the anchor point for the UEs user plane through the eNodeBs on the Neutral Host infrastructure. As we will see, the SGWs are associated to the Tracking Areas (i.e. a group of neighbouring cells identified by a Tracking Area Code (TAC)) they serve. A PGW terminates the PDU sessions from the UE into the PDN specified by the APN. In the Neutral Host deployment scenario, different implementations of PGW and economics of resources will dictate the best strategy between the deployment of a single PGW to serve several APNs or a dedicated PGW to serve each APN deployed. In this work, we will consider the dedicated PGW per APN scenario. Also, for simplicity, we will consider that all the Neutral Host eNodeBs belong to the same TAC and that only one SGW is required to cover the whole Neutral Host infrastructure.

In the 4G EPS, service discovery is supported by DNS procedures as described in 3GPP TS 29.303 [1], although some implementations may use a different method to select the functions for a specific service. In summary, DNS may be used in the EPS to derive the IP address of a PGW serving a specific APN and, similarly, the IP address of the SGW serving a specific TAC can also be obtained. The specification supports the selection of PGW and SGW that are either co-located or close in the topology, as well as prioritisation based on the records order on the DNS registry.

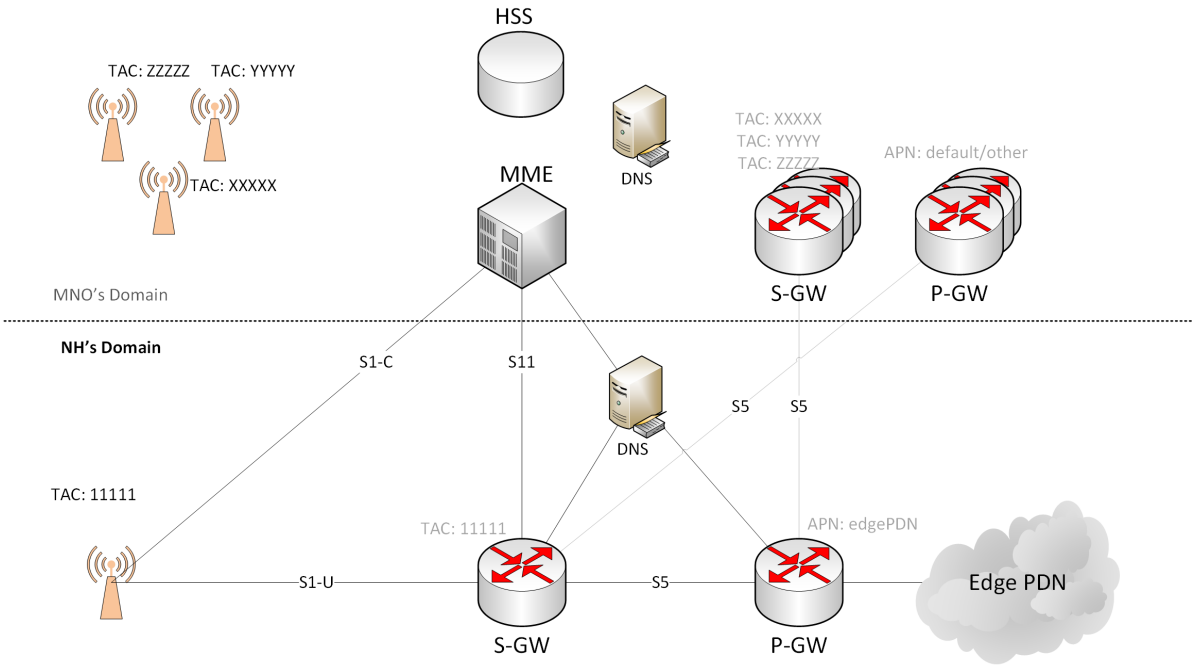

Figure 3.7: EPC deployment at the Neutral Host as edge of the network

Given the importance of DNS in the selection of functions, the deployment of a dedicated DNS server local to the Neutral Host is proposed, and this DNS server needs to be made reachable from the operator's network in order to allow the discovery of these functions. There are, however, no specified procedures by which a new network function can be registered for discovery. Therefore,

the proposed automated model needs to be designed so any new function instance (SGW/PGW) triggers an update on the DNS server to register the function for discovery. The entity requesting the instantiation to the NFVO, either needs to perform the registration of the function on the DNS, or provide enough information as instance parameters for the function to be able to perform it by itself. In this work, the server IP address, port and authentication credentials are passed on to the instance, which then performs the registration on the DNS server.

Three steps are identified in the deployment process, assuming the interconnection between the NH and MNO domains has already been managed and secured. Note some of these steps can be optional, if we consider a CSP picking the required services from different Neutral Hosts:

1. **Reconfigure network resources**: The underlying network needs to be reconfigured programmatically as required before or after each of these steps to accommodate for new configurations and creating the links required to connect the new functions together.

2. **Reconfigure eNodeBs**: There are several configuration options, as described in chapter 2, depending on the level of sharing. For this work we will consider the MOCN scenario: Reconfigure cells to add a Public Land Mobile Network ID (PLMN ID), which uniquely identifies a network globally, to the set of broadcast networks and establish S1 interfaces to MNO's EPS. At this stage, there is "access only" service from the Neutral Host, using the MNO's core network.

3. **Deploy Local DNS Server**: This DNS server will register the services of MNO's functions deployed in the Neutral Host.

4. **Deploy SGW**: To be used as the local anchor to the eNodeBs part of the Neutral Host configured TAC.

5. **Deploy PGWs**: At this stage, successive PGWs can be deployed to serve the respective APNs, creating a local PDN network and connecting to it via its SGi interface.

6. **Deployment of PDN VNFs**: These are the VNFs that offer the end service to mobile subscribers requesting access via a specific APN.

Considering the previous steps, we can identify the equivalent to, using 5G terminology, three Network Slices Subnets that can be deployed independently to allow for flexibility in the automation. These three identified services need therefore to be mapped into Network Services.:

1. **Local DNS**:

Figure 3.8: DNS Network Service

- **Description**: Provides the name service within a PLMN for the Neutral Host domain in support to the MME gateway selection function. It listens for announcements of updates on the availability of the functions under its domain and updates its database accordingly.
- **Interfaces**:
  - *CP DNS*: For simplicity, we can consider a single interface that provides DNS Service and listens for updates on available functions.
- **Primitives**:
  - *initial_setup*:
    - **Description**: Executed as NFV day-1 operation, configures the DNS application for service readiness and starts the application.
    - **Parameters**:
    - *MCC:* Mobile Country Code, part of the PLMN ID, identifying the country of the served network.
    - *MNC:* Mobile Network Code, part of the PLMN ID, identifying the served network within an MCC.
  - *start*:
    - **Description**: Support primitive for NFV day-2 operations (phase for VNF maintenance). Starts the DNS application if it is stopped.
    - **Parameters**: None.
  - *restart*:
    - **Description**: Support primitive for NFV day-2 operations. Restarts the running DNS application
    - **Parameters**: None.
  - *stop*:

        * **Description**: Support primitive for NFV day-2 operations. Stops the running DNS application.
        * **Parameters**: None.
    - *status*:
        * **Description**: Support primitive for NFV day-2 operations. Queries the status of the DNS application.
        * **Parameters**: None.

2. **SGW**:

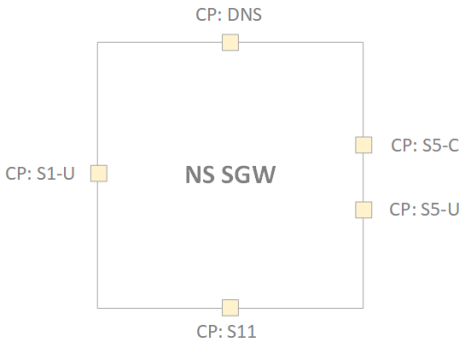

Figure 3.9: SGW Network Service

- **Description**: Performs the SGW function for a TAC within a PLMN.
- **Interfaces**:
    - *CP S1-U*: Interface with the eNodeBs S1 user plane. Terminates Radio Access Bearer from UEs (E-RAB).
    - *CP S11*: Interface with MME S11 for management of EPS Bearers.
    - *CP S5-C*: Interface with PGWs S5 control plane for managemente of user plane S5 Bearers.
    - *CP S5-U*: Interface with PGWs S5 user plane. Terminates S5 Bearers.
    - *CP DNS*: Interface with the DNS function for registration, update and de-registration of the function.
- **Primitives**:
    - *initial_setup*:
        * **Description**: Executed as NFV day-1 operation, configures the SGW application for service readiness, starts the application and registers the function on the DNS.
        * **Parameters**:

- *MCC:* Mobile Country Code, part of the PLMN ID, identifying the country of the served network.
- *MNC:* Mobile Network Code, part of the PLMN ID, identifying the served network within an MCC.
- *TAC:* Served TAC.
- *Function Server IP:* IP address where the DNS function is available.
- *Function Server Port:* Port where the DNS function is available.
- *Credentials:* Credentials to be used for authentication with the DNS.

– *start*:

* **Description**: Support primitive for NFV day-2 operations. Starts the SGW application if it is stopped and updates the status with the DNS server.
* **Parameters**: None.

– *restart*:

* **Description**: Support primitive for NFV day-2 operations. Restarts the running SGW application and updates the status with the DNS server.
* **Parameters**: None.

– *stop*:

* **Description**: Support primitive for NFV day-2 operations. Stops the running SGW application and updates the status with the DNS server.
* **Parameters**: None.

– *status*:

* **Description**: Support primitive for NFV day-2 operations. Queries the status of the SGW application.
* **Parameters**: None.

3. **PGW**:

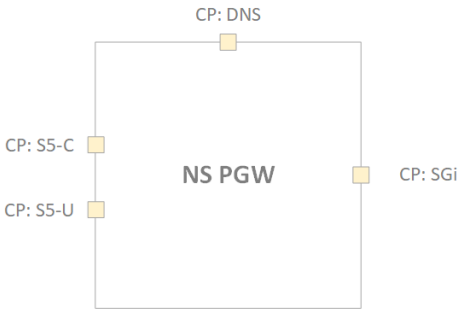

Figure 3.10: PGW Network Service

- **Description**: Performs the PGW function for an APN within a PLMN.
- **Interfaces**:
  - *CP SGi*: For simplicity, we can consider a single interface that provides DNS Service and listens for updates on available functions.
  - *CP S5-C*: Interface with SGWs S5 control plane for management of user plane S5 Bearers.
  - *CP S5-U*: Interface with SGWs S5 user plane. Terminates S5 Bearers.
  - *CP DNS*: Interface with the DNS function for registration, update and de-registration of the function.
- **Primitives**:
  - *initial_setup*:
    - **Description**: Executed as NFV day-1 operation, configures the SGW application for service readiness, starts the application and registers the function on the DNS.
    - **Parameters**:
      - *MCC:* Mobile Country Code, part of the PLMN ID, identifying the country of the served network.
      - *MNC:* Mobile Network Code, part of the PLMN ID, identifying the served network within an MCC.
      - *APN:* Served APN.
      - *UEPOOL:* Pool of IP address for allocation to UE PDU Sessions.
      - *DNS:* IP addresses of the DNS to be configured at the UE.
      - *Function Server IP:* IP address where the DNS function is available.
      - *Function Server Port:* Port where the DNS function is available.
      - *Credentials:* Credentials to be used for authentication with the DNS.
  - *start*:
    - **Description**: Support primitive for NFV day-2 operations. Starts the PGW application if it is stopped and updates the status with the DNS server.
    - **Parameters**: None.
  - *restart*:
    - **Description**: Support primitive for NFV day-2 operations. Restarts the running PGW application and updates the status with the DNS server.
    - **Parameters**: None.
  - *stop*:
    - **Description**: Support primitive for NFV day-2 operations. Stops the running PGW application and updates the status with the DNS server.

* **Parameters**: None.

– *status*:

* **Description**: Support primitive for NFV day-2 operations. Queries the status of the PGW application.
* **Parameters**: None.

These building blocks allow a CSP to flexibly extend its 4G functions, using a 3rd party NFV infrastructure. Figure 3.11 shows a scenario where the aforementioned Network Services are used in combination and how they interconnect to provide the required service. The NFV Orchestration plays a crucial role in coordinating this interconnection.

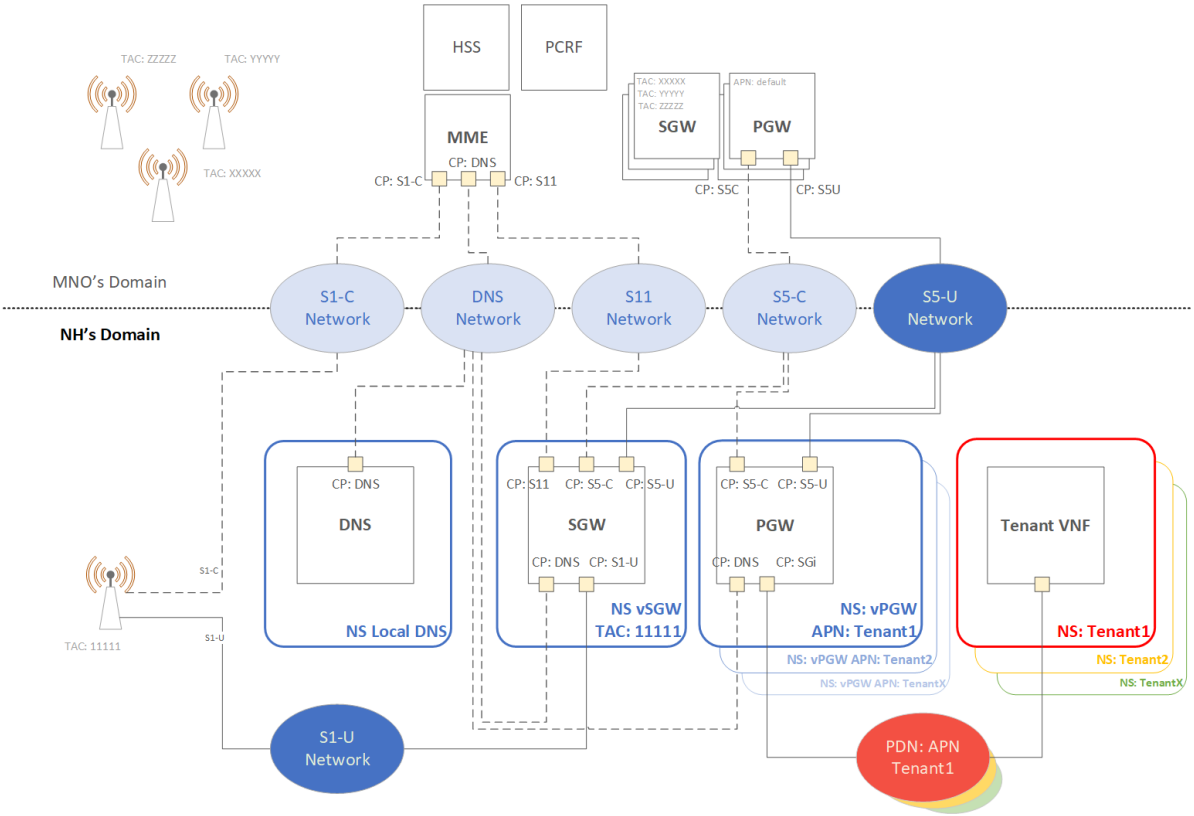

Figure 3.11: EPC Network Services integration

3.3 Architecture

Based on the services, slicing and automation requirements previously described we can propose an architecture to serve as a framework for implementation of a Neutral Host.

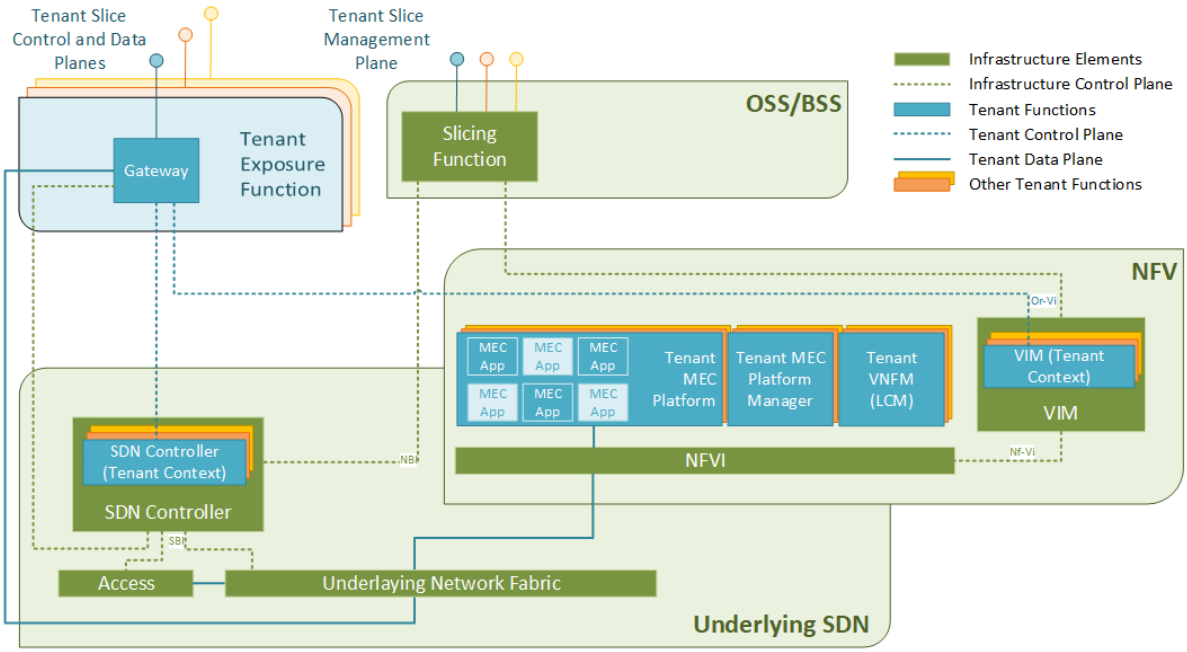

Figure 3.12: NH Framework Architecture

Figure 3.12 shows how the underlying access, network fabric, and NFV infrastructure serve as the base that sustains the rest of the system. The proposed architecture extends ETSI NFV and MEC architectures (Section 2.1.2 and Section 2.1.3) with an infrastructure slicing function that incorporates together the NFV and underlying SDN domains.

The role of the Slicing Function is to present an integrated view of the available resources for selection, managing the life-cycle of the created slices, maintaining a database with information of the different tenants and their slice record containing the selected resources and applicable policies, as well as centralising the requests of slice realisation to the SDN controller and VIM.

SDN Controller and VIM implement the required slice at request of the slice manager, configuring the resources and applying the slice policies, to then group the resulting Tenant Context and exposing to the Tenant for control of the slice.

From the CSP point of view, as a tenant of the neutral host, an interface to the Slice Function for slice management purposes is presented by the Neutral Host OSS/BSS. The reality of the resources being shared is transparent at the level of VIM and SDN Northbound Interfaces, which are presented to the CSP along with its Data Plane, via the Tenant Exposure Function that acts as a gateway to the CSP's own network.

3.4 Chapter summary

This chapter has presented the Neutral Host concept, as the main contribution of this work, by presenting a business model on which it is supported, describing the main resources that will be relevant in this scenario, and presenting a multi-level solution to solve slicing requirements of multiple tenants on a shared infrastructure. After evaluating the automation requirements of 4G and 5G networks, an enabling architecture that realises it has been presented.

Next chapter will demonstrate a 4G automation scenario using NFV and SDN techniques, as it could leverage such deployment.

CHAPTER 4

PRACTICAL IMPLEMENTATION OF AN AUTOMATED EPC

This chapter describes the scenario created for the demonstration of an automated 4G network deployment in a virtualised Neutral Host scenario. This automation deployment assumes the context within a slice provided by the Neutral Host. Two use cases were implemented, which correspond to the automated deployment of two Network Services, namely, SGW and PGW. For simplicity of the deployment, the number of interfaces of each NS and VNF was compacted as shown in Figure 4.1.

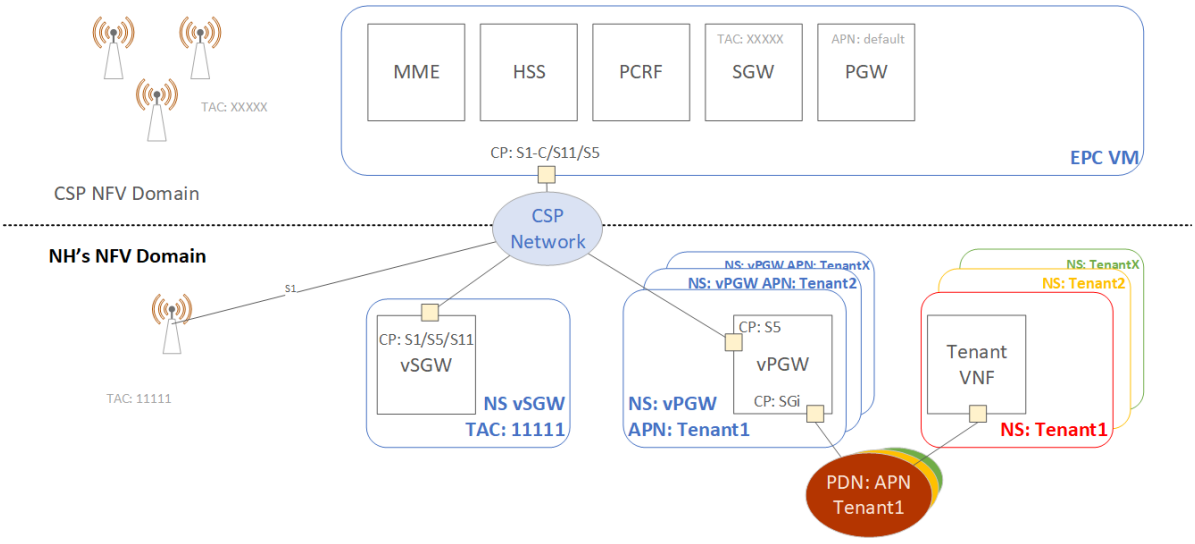

Figure 4.1: 4G Automation Scenario

4.1 Infrastructure Overview

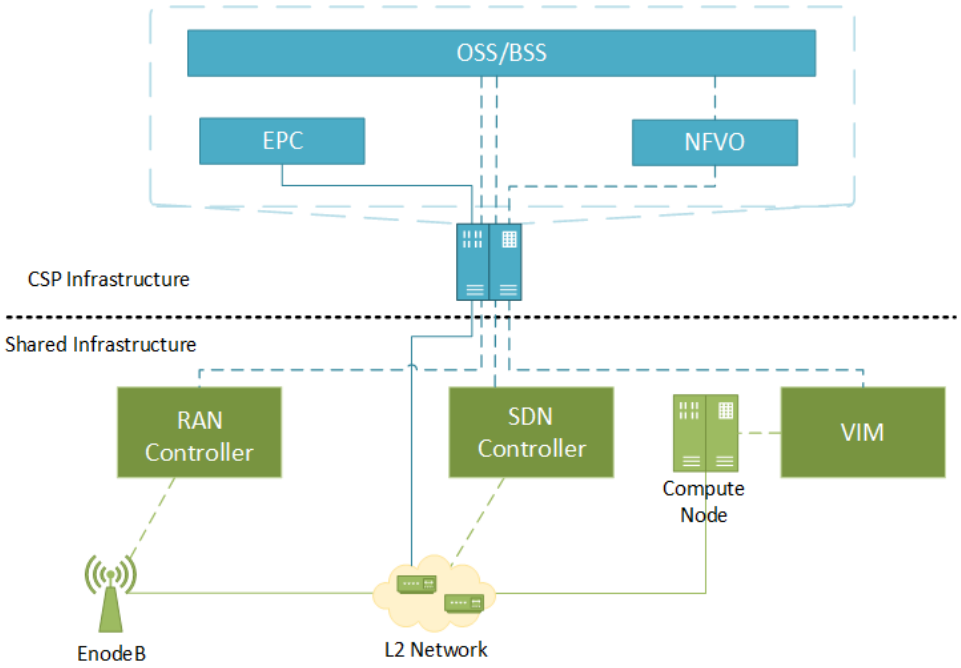

Figure 4.2: Infrastructure Environment

The implemented testbed is shown in Figure 4.2. Two virtualisation infrastructures were implemented. The first one serves the purpose of hosting the elements that correspond to the CSP domain and simulates its own infrastructure. In this domain we find the core elements of the EPC, i.e. MME, HSS and PCRF, the NFV Orchestrator, and the OSS/BSS logic that triggers the scenario deployments. The second NFVI, together with an eNodeB and SDN enabled network, forms the Neutral Host shared infrastructure. Openstack deployments were used as the VIM in both domains and ETSI Open Source Mano selected as the orchestrator, at the CSP domain.

On the shared infrastructure side, two RAN setups were evaluated. First, a NOKIA Airscale 4G eNodeB was used as the shared radio resource. This device was managed by a software agent that provisions the required configuration to serve multiple PLMNs using 3GPP MOCN feature. And then, same configuration was done, substituting the software agent by a FlexRAN controller and the eNodeB by an OpenAirInterface eNodeB. The connection between the eNodeB and the compute node was realised by a flat network on which Openstack Neutron as the SDN controller provisions isolated networks for each tenant. This isolation is provided by the use of VLANs in the implemented scenario.

4.2 Virtual EPC

An open source EPC implementation is available at `https://open5gs.org/`. Open5gs implements the basic functions of an EPC compliant with 3GPP Standard Release 14.

Each element of the EPC is implemented in a different service that can be managed as a compact EPC or in a standalone manner which matched the requirements of the implementation.

- *MME:* open5gs-mmed
- *SGW:* open5gs-sgwd
- *PGW:* open5gs-pgwd
- *HSS:* open5gs-hssd
- *PCRF:* open5gs-pcrfd

For this work, the EPC software was enhanced with a Command Line Interface (CLI) agent based in python, able to receive commands that modify the configuration of the different EPC components, as well as managing the running state of each service.

Open5gs implementation of the EPC does not use the DNS procedures to announce and discover new services. Instead, the list of services available in the network are written onto the MME configuration file *mme.yaml* directly. The service discovery functionality is added and implemented using the CLI agent. The following commands are available on the CLI agent:

- ***cli.py manage:***
  - *Description:* This function can be used to manage the running status of the different services.
  - *Parameters:*
    - *Action:* Choice between "START", "STOP", "RESTART", "ENABLE" and "DISABLE" as per Ubuntu *systemctl* available instructions.
    - *Element:* Choice between "MME","SGW","PGW","HSS" and "PCRF".
- ***cli.py mme_setup:***
  - *Description:* Writes the initial MME configuration in *mme.yaml*.
  - *Parameters:*
    - *MCC:* Mobile Country Code of the served network.
    - *MNC:* Mobile Network Code of the served network.
    - *MME_CODE:* MME Code as per 3GPP Rel. 14 specification.
    - *MME_GID:* MME Group ID as per 3GPP Rel. 14 specification.

    - *NAME:* Name of the Mobile Network.
    - *GTPC:* Name of the device to be configured for S11 interface.
    - *S1AP:* Name of the device to be configured for S1 interface.

- ***cli.py mme_tac:***
  - *Description:* Creates, Updates or Deletes a TAC from the MME configuration of available functions in *mme.yaml*.
  - *Parameters:*
    - *Action:* Choice between "CREATE", "UPDATE", "DELETE".
    - *MCC:* Mobile Country Code of the served network.
    - *MNC:* Mobile Network Code of the served network.
    - *TAC:* Tracking Area Code to be configured.
    - *SGW:* SGW that serves the specified TAC.

- ***cli.py mme_apn:***
  - *Description:* Creates, Updates or Deletes a APN from the MME configuration of available functions in *mme.yaml*.
  - *Parameters:*
    - *Action:* Choice between "CREATE", "UPDATE", "DELETE".
    - *APN:* Access Point Name to be configured.
    - *PGW:* PGW that serves the specified TAC.

- ***cli.py sgw_setup:***
  - *Description:* Writes the initial SGW configuration in *sgw.yaml* and sends an announcement of the new configured SGW function and the served TAC to an indicated server using the provided credentials.
  - *Parameters:*
    - *MCC:* Mobile Country Code of the served network.
    - *MNC:* Mobile Network Code of the served network.
    - *TAC:* Tracking Area Code to be configured.
    - *GTPC:* Name of the device to be configured for GTPC traffic, i.e. S11 and S5-C interfaces.
    - *GTPU:* Name of the device to be configured for GTPU traffic, i.e. S1-U and S5-U interfaces.
    - *SERVER_ADDR:* IP address of the server listening for announcements of new functions for discovery.

    - *SERVER_PORT:* Port number of the server listening for announcements of new functions for discovery.
    - *USERNAME:* Username credential for authentication on the server.
    - *PASSWORD:* Password credential for authentication on the server.

- ***cli.py pgw_setup:***
  - *Description:* Writes the initial PGW configuration in *pgw.yaml* and sends an announcement of the new configured PGW function and the served APN to an indicated server using the provided credentials.
  - *Parameters:*
    - *MCC:* Mobile Country Code of the served network.
    - *MNC:* Mobile Network Code of the served network.
    - *APN:* Tracking Area Code to be configured.
    - *GTPC:* Name of the device to be configured for GTPC traffic, i.e. S5-C interface.
    - *GTPU:* Name of the device to be configured for GTPU traffic, i.e. S5-U interface.
    - *SERVER_ADDR:* IP address of the server listening for announcements of new functions for discovery.
    - *SERVER_PORT:* Port number of the server listening for announcements of new functions for discovery.
    - *USERNAME:* Username credential for authentication on the server.
    - *PASSWORD:* Password credential for authentication on the server.
    - *PCRF_FQDN:* FQDN of the serving PCRF.
    - *PCRF_ADDR:* IP Address of the serving PCRF.
    - *REALM:* Realm configured for Diameter with PCRF.
    - *UE_POOL:* Pool of IP address for assignment to UEs connecting via this APN.
    - *DNS:* DNS for configuration on UEs connecting via this APN.

- ***cli.py pcrf_setup:***
  - *Description:* Writes the initial PCRF configuration in *pcrf.yaml* and initialises the required certificates.
  - *Parameters:*
    - *IFACE:* Interface over which the PCRF Service will run.
    - *FQDN:* FQDN of the PCRF Service.
    - *REALM:* Realm configured for Diameter with PGWs.

- ***cli.py pcrf_peer:***

  - *Description:* Manages the list of Diameter Peers.
  - *Parameters:*
    * *ACTION:* Choice between CREATE, UPDATE, DELETE.
    * *FQDN:* FQDN of the Diameter Peer object of the ACTION.
    * *ADDR:* Address of the Diameter Peer object of the ACTION.

The EPC software and the CLI Agent was pre-installed on an Ubuntu 18.04 image and then added into the VNF packages of the different EPC functions, i.e. SGW and PGW.

Current version of the CLI Agent is implemented to expect commands executed through SSH using port 22 for direct compatibility with Juju Proxy Charms [11], used by OSM to perform VNF configuration and lifecycle management. In this case, Juju Proxy Charms was observed to increase the VNF instantiation time, due to the need of creating a Linux container and install the required Juju software components to perform the Proxy Charm function. In parallel, a simpler version of the VNFs was implemented, using Cloud-Init to also trigger the VNF day-1 operations instead, reducing the time required for bringing the relevant function into service.

Each VNF package is created containing the following main files:

- *vEPC_*<function>*_vnfd.yaml:* Descriptor of the VNF as per OSM YANG Information Model [12]

- *base_open5gs.qcow:* Virtual EPC VM Image file containing Open5GS software and the CLI Agent.

- *Charm files [Optional]:* Generated and compiled using the *charm* command and libraries provided by Canonical.

- *cloud_config [Optional]:* Cloud-Init file containing the instantiation parameters for the VNF. This file contains placeholders for parameters that are passed on to the NFV Orchestrator at instantiation time, rather than being contained in the VNF Package, with the purpose of customising the required VNF with instance specific values.

Figure 4.3 shows a representation of the implemented network services. The corresponding NS and VNF descriptors, as well as the *cloud_config* files are shown in Appendix B.

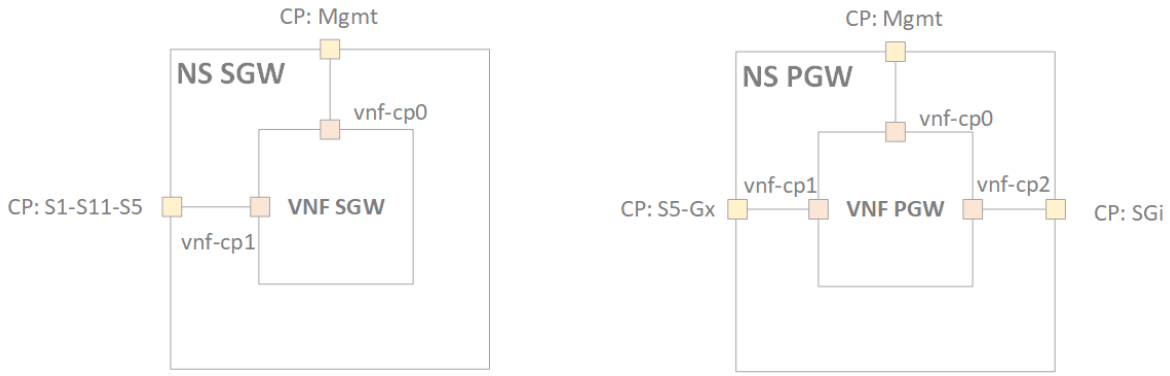

Figure 4.3: Demo Network Services

4.3 Use Cases Workflows

This section describes the workflows of both use cases implemented and deployed in the described testbed.

4.3.1 TAC Integration workflow

TAC integration is realized by the sequence described in figure 4.4. The user in the CSP domain, request the integration of a TAC in the shared infrastructure domain through its organization OSS/BSS. The OSS/BSS then triggers a sequence of requests to realize this configuration. The system requests the eNodeBs that form the specific TAC to add configuration for a new PLMN, indicating the IP address of the MME that will terminate the S1 interfaces. In parallel, a request to Openstack neutron is placed, to create a network that allows the communication between the S1, S5 and S11 interfaces between the eNodeB, MME, SGW and PGW. Once the network has been created, the sequence continues by OSS/BSS requesting OSM to deploy a SGW NS using the indicated parameters on the recently created network. OSM then triggers the creation of the requried SGW VM on the shared infrastructure VIM. Once day 0 and day 1 operations are finished, the EPC is ready to accept S1 connections from eNodeBs in this TAC, and service is therefore established.

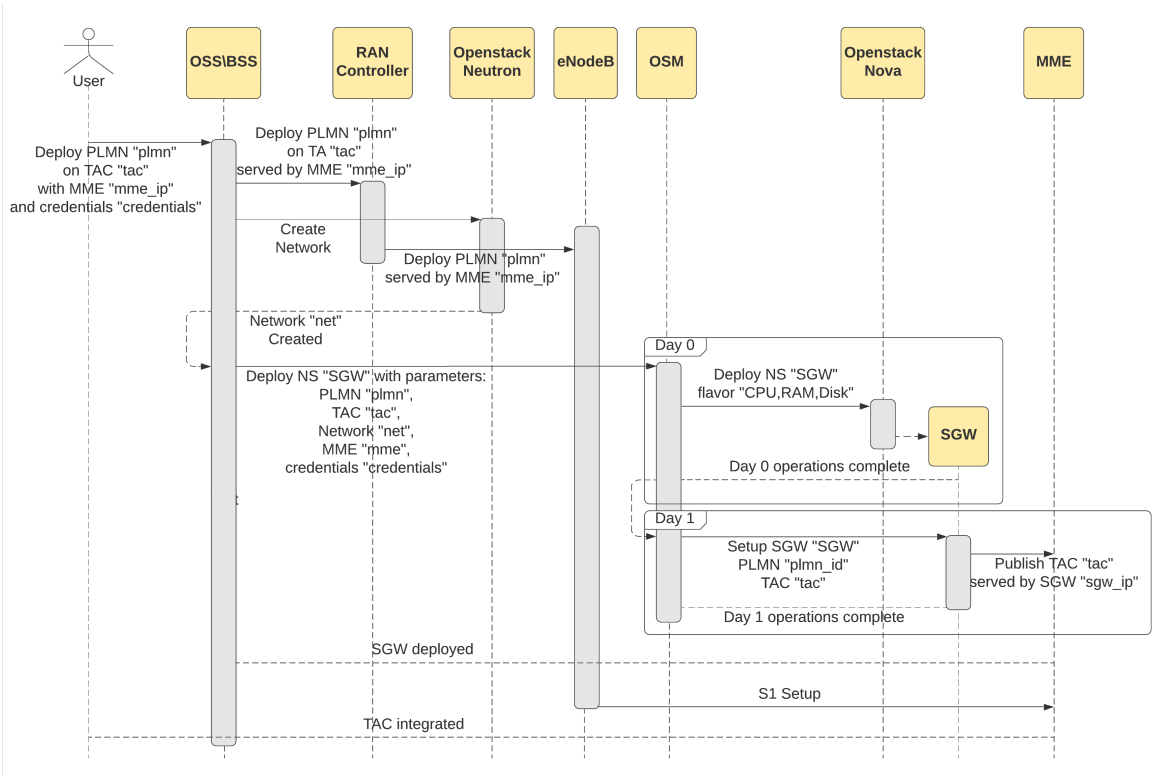

Figure 4.4: Demo SGW Sequence Diagram

4.3.2 APN Deployment workflow

An APN deployment is realised by the deployment of a PGW NS as described in figure 4.5. The TAC is assumed to have been integrated previously on this scenario. The user in the CSP domain, request the deployment of an APN in the shared infrastructure domain through its organisation OSS/BSS. The OSS/BSS then triggers a sequence of requests to realise this configuration. In this scenario, the network for communication with the EPC has already been created previously. Instead the SGi network needs to be created by a request to Openstack neutron. Once the network has been created, the sequence continues by OSS/BSS requesting OSM to deploy a PGW NS using the indicated parameters, the existing EPC network and the recently created SGi network. OSM then triggers the creation of the required PGW VM on the shared infrastructure VIM. Once day 0 and day 1 operations are finished, the EPC is ready to accept connections from users requesting access to the PDN served by this APN.

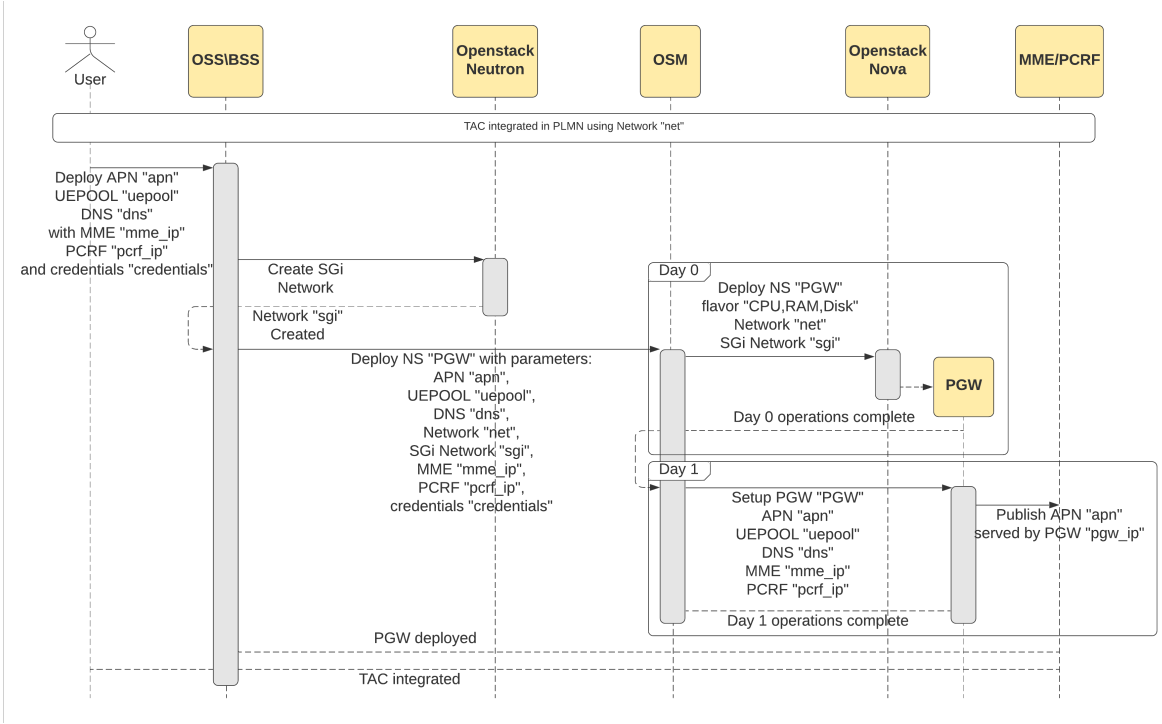

Figure 4.5: Demo PGW Sequence Diagram

4.4 Demo Results

A series of 30 tests for each scenario was performed and the results can be seen in figure 4.6. The TAC scenario was executed twice, first with the Nokia commercial basestation, and second with the FlexRAN open-source controller and an OpenAirInterface eNodeB emulator. On the left side, the VNF deployment time for each test can be appreciated for both use cases while, the right side, shows the breakdown of the total time for each test and use case, highlighting the average time and 99% confidence interval.

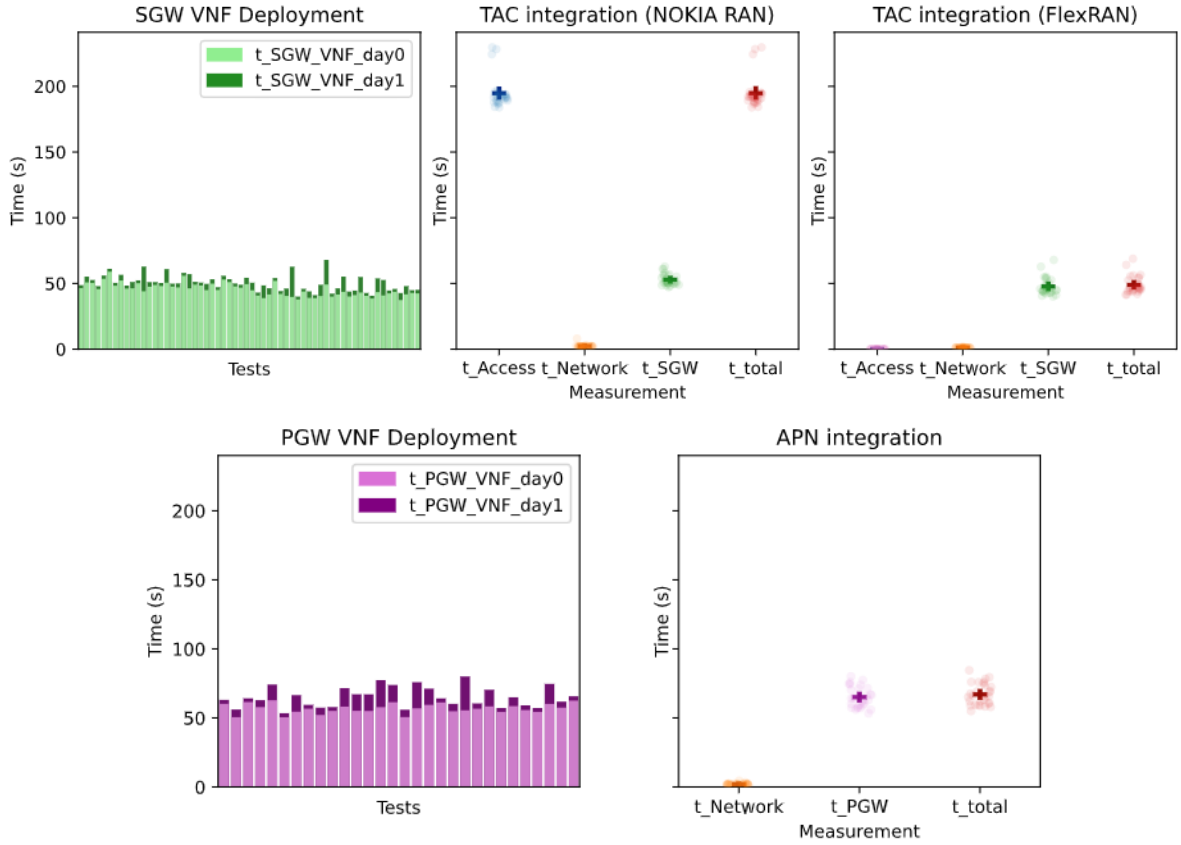

Figure 4.6: Demo Results

The total time to integrate a new TAC into the network corresponds to the maximum between the time necessary to reconfigure the access equipment, and the sum of the times to reconfigure the backhaul network and to deploy an SGW. In the case of a new APN integration, the total time is the sum of the times to create an SGi network and to deploy a PGW.

$$t_{TAC} = max\{t_{Access}, t_{Network} + t_{SGW}\}$$

$$t_{APN} = t_{Network} + t_{PGW}$$

Similarly, the time required to deploy a SGW or a PGW VNF is the sum of the times to perform Day 0 and Day 1 operations.

$$t_{SGW} = t_{SGW\_VNF\_day\_0} + t_{SGW\_VNF\_day\_1}$$

$$t_{PGW} = t_{PGW\_VNF\_day0} + t_{PGW\_VNF\_day1}$$

In the new TAC integration scenario, it can be identified that the limiting factor in this case is the amount of time required to reconfigure the access network when using the Nokia Airscale device. This is due to the current architecture of the commercial eNodeB, which requires a hardware reset to make effective the new configuration. Contrasting, the FlexRAN/OpenAirInterface RAN enables the reduction of this time to negligible values, when compared to the SGW VNF deployment time. In the case of a new APN integration, given that the access network does not need to be reconfigured, the total time is also primarily contributed by PGW VNF deployment time.

It is important to note that, obviously, specific implementations of VNFs will have significant impact in the performance of these deployment scenarios. We can observe from the results that most of the VNF instantiation time is contributed by day 0 operations due to the lightweight nature of the particular EPC software implementation. The expectation is that the ratio between day 0 time and day 1 time is flipped when using richer implementations as the application setup time may increase while day0 operations time may stay within similar ranges. This can be considered as an important factor to measure the quality and performance of a given VNF package against the provided functionality.

The limited deviation between the samples at 99% confidence is attributed to the static nature of the test environment and future works will explore the evaluation under loaded scenarios.

4.5 Chapter summary

This chapter has presented an implementation of two scenarios of 4G automation relevant to a Neutral Host deployment, i.e. TAC Integration and APN Deployment, and the infrastructure and software implemented for demonstration have been described. The results from this demonstration show how the automation of deployment of EPC functions allows for minimal deployment times in a virtualised deployment while maintaining maximum degree of flexibility. This agility will translate in operational gains when integrating Neutral Host networks and also allows for faster maintenance response times on contingency scenarios.

CHAPTER 5

CONCLUSION

After the initial review of the various technologies and latest literature on the state of the art presented in chapter 2, the main contributions of this work have been presented in chapters 3 and 4. First, the business model of a 5G Neutral Host has been presented, a new scenario of access sites as small, shared, edge datacentres proposed, and the services to be provided by a Neutral Host identified. These services are based on a proposed federated deployment strategy for CSPs that consume the services of 3rd party infrastructure providers. Then, to realise this strategy, a multi-level slicing model that leverages the capabilities of NFV, SDN and RAN Sharing was proposed. These technologies are combined, enabling infrastructure owners to offer platforms that CSPs can take advantage of when deploying 5G services that require MEC resources. Next, 5G and 4G automated network deployment scenarios were presented as use cases of this model. After that, a Neutral Host architecture capable of offering these services was introduced. Finally, a practical demonstration of an automated EPC deployment has been described and the results discussed.

We can conclude that the new technologies supporting 5G make possible a new infrastructure sharing model for public networks and Neutral Host. The traditional active sharing models where operators deployed, operated and maintained radio equipment that provides service to further operators and simply hands the traffic off to them at a demarcated transport interconnection point, can now be extended to small edge datacentres where CSPs can deploy their own virtualised functions. NFV Orchestration and SDN allow CSPs to maintain tight control over deployment, operation and optimisation, even allowing them to choose different software vendors than their competitors, with the desired ration of offered features vs. achieved performance, and multi level slicing allows resources to be shared in mutual isolation while retaining the capability to serve multiple tenants.

This new deployment model is supported by a novel business model where operators compose end to end networks by interconnection of multiple federated domains by leveraging the cloud *Infrastructure as a Service* model and extending it with Access network in the co-localised geographical area.

Further work around this topic can be focused on several areas:

- Interconnection: In this work the Neutral Host network has been considered as sharing a predefined transport demarcation point for both Control Plane and Data Plane. Further study can be carried out to define methods that automate this interconnection by leveraging what could be a national grid of Neutral Host infrastructures. This could be an extension of the IP Exchange services used for roaming today.

- Slicing: This work has focused on the deployment of slices from the CN point of view. As described in chapter 2 multiple research studies are being undertaken in the area of RAN Virtualisation and RAN Slicing. In future works, it is important to study the integration of end to end CN and RAN slices within a Neutral Host deployment. Future addition to the OSS of the Neutral Host is a spectrum brokering system to apply the agreed policies to the radio interface. Such system could dynamically offset the amount of radio resource blocks utilised by the tenant against the amount of spectrum contributed, as an assistance for the Infrastructure Provider to calculate the fees, as well as to help the licensees monetise the spectrum. This could be achieved in a similar fashion as how an Automated Frequency Coordination system operates. Scenarios where a CSP is under-occupying its resources can be foreseen and other tenants could choose to pay the former for the use of these resources.

- Virtualisation: Further study is required on the best dimensioning practices for the deployment of a shared virtualisation infrastructure that also incorporates access resources. Furthermore, the described infrastructure is based on VM virtualisation. There is a current trend to evolve NFV to cloud-native applications based on orchestrated containers. An evolution of the presented architecture could study the practicalities of offering a *Container-as-a-Service* (CaaS) model that would sit midway between IaaS and PaaS models.

- Radio Network Planning and Optimisation: Study needs to be carried out on the implications of the Neutral Host and federated network model in radio network planning and optimisation for mobility and load balancing scenarios between between Neutral Host and public network.

APPENDIX A

APPENDIX A: 3GPP 4G EPS ARCHITECTURE

This section describes the main components and basic operation of an elementary 4G System. It is composed of the following elements:

- *eNodeB*: Radio base-station for User Equipment (UE) access.
- *MME*: Performs session management functions as well as mobility for the UEs connecting to the network.
- *HSS*: Subscriber database containing the UE profiles and performs UE authentication.
- *SGW*: Data Session anchor from the RAN. Terminates the S1-U interface.
- *PGW*: Data Session anchor towards the Data Network. Provides SGi interface towards the Data network.

Other functions like the PCRF support the system to enforce traffic policy on the data-plane dynamically.

Figure A.1 shows the basic diagram of a functional EPC. UEs accessing the network request authentication to the HSS via the MME. The MME then selects the SGW based on load or closeness to the access and request for an EPS bearer to be created for the APN provided by the UE. The SGW then identifies the PGW that serves such APN and requests an S5 Bearer to be created for the UE traffic. On completion the SGW completes the EPS Bearer by establishing an S1-U bearer towards the eNodeB serving the user.

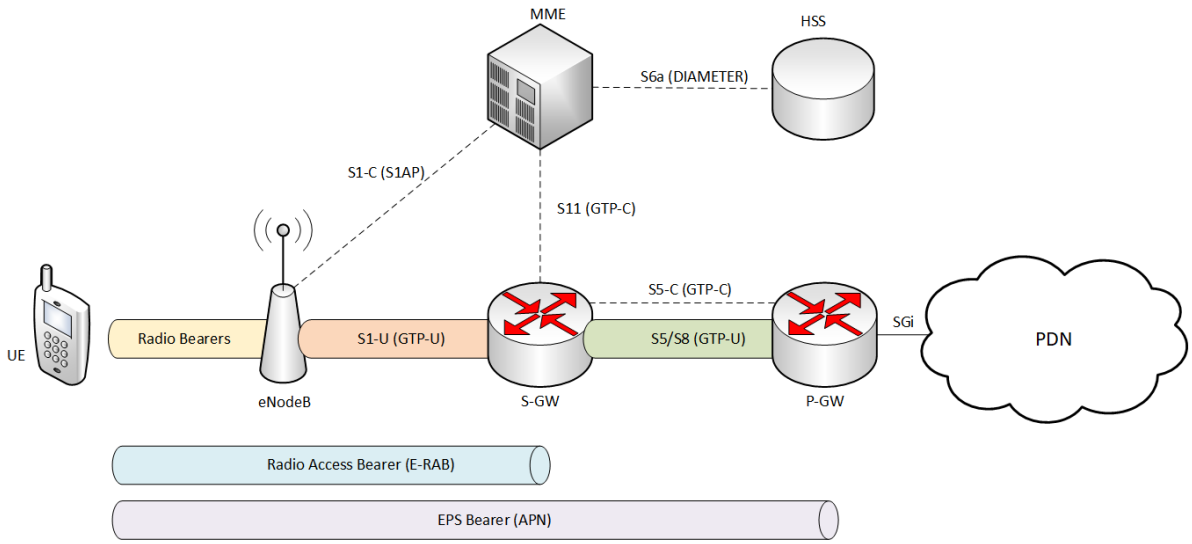

Figure A.1: EPS

A.1 MEC in 4G

ETSI Whitepaper *"MEC Deployments in 4G and Evolution Towards 5G"* [16] studies the different scenarios in which the EPS can leverage a MEC deployment:

- *Distributed EPC*: The complete EPC is deployed at the edge, including the HSS. This architecture is useful in Emergency or Mission Critical communications scenarios.
- *Bump in the wire*: In order to discriminate traffic that is intended to/from the MEC Applications, the User Plane function of the MEC is placed either at the eNodeB, before the traffic is encapsulated into the GTP-U tunnel towards the SGW, or somewher along the route in the S1-U interface, performing the task of managing the traffic in and out of the tunnel.
- *Distributed SGW-PGW*: In this scenario, a SGW and PGW are deployed at the edge of the network and the MEC platform sits at PGW's SGi interface, allowing for discrimination of edge traffic based on APN.
- *SGW-LocalBreakOut*: This is a hybrid scenario that allows operators to even discriminate between the traffic that belongs to the same APN as this is done at the SGW with Local Break Out functionality. In this scenario, only the SGW is deployed at the edge, on the MEC Platform.

APPENDIX B

Appendix B: OSM NS and VNF Descriptors

B.1 SGW VNF Descriptor

```
#vEPC_SGW_vnfd.yaml
vnfd:vnfd-catalog:
vnfd:
-   id: vEPC_SGW_vnfd
    name: vEPC_SGW_vnfd
    short-name: vEPC_SGW_vnfd
    description: Virtual SGW based on Open5Gs, enhanced with CLI agent to
    support automated deployment.
    vendor: UoB
    version: '1.0'

    mgmt-interface:
        cp: vnf-cp0

    vdu:
    -   id: vEPC_SGW_vnfd-vSGW
        name: vEPC_SGW_vnfd-vSGW
        description: vEPC_SGW_vnfd-vSGW
        count: 1

        vm-flavor:
```

```
            vcpu-count: 4
            memory-mb: 4096
            storage-gb: 20

        image: 'base_open5gs'

        cloud-init-file: 'cloud_config'

        interface:
        -   name: ens3
            type: EXTERNAL
            virtual-interface:
                type: PARAVIRT
            external-connection-point-ref: vnf-cp0
            mgmt-interface: true
        -   name: ens4
            type: EXTERNAL
            virtual-interface:
                type: PARAVIRT
            external-connection-point-ref: vnf-cp1

        vdu-configuration:
            juju:
                charm: vepc

            initial-config-primitive:
            -   name: config
                parameter:
                -   name: ssh-hostname
                    value: <rw_mgmt_ip>
                -   name: ssh-username
                    value: ubuntu
                -   name: ssh-password
                    value: ubuntu
                seq: '1'

            -   name: sgw-setup
                parameter:
```

```
                -   name: gtpc_dev
                    value: <gtpc_dev>
                -   name: gtpu_dev
                    value: <gtpu_dev>
                seq: '2'

            -   name: service-publish
                parameter:
                -   name: element
                    value: sgw
                -   name: mcc
                    value: <mcc>
                -   name: mnc
                    value: <mnc>
                -   name: tac
                    value: <tac>
                -   name: addr
                    value: <addr>
                -   name: port
                    value: <port>
                -   name: username
                    value: <username>
                -   name: password
                    value: <password>
                seq: '3'

    connection-point:
    -   name: vnf-cp0
    -   name: vnf-cp1
```

B.2 SGW NS Descriptor

```
#vEPC_SGW_nsd.yaml
nsd:nsd-catalog:
nsd:
-   id: vEPC_SGW_nsd
    name: vEPC_SGW_nsd
    short-name: vEPC_SGW_nsd
```

```
    description: Virtual SGW based on Open5Gs, enhanced with CLI agent to
    support automated deployment.
    vendor: UoB
    version: '1.0'

    constituent-vnfd:
    -   member-vnf-index: 1
        vnfd-id-ref: vEPC_SGW_vnfd

    vld:
    -   id: vEPC_SGW_nsd_vld0
        name: management
        short-name: management
        type: ELAN
        mgmt-network: 'true'
        vim-network-name: 'mgmt'
        vnfd-connection-point-ref:
        -   member-vnf-index-ref: 1
            vnfd-id-ref: vEPC_SGW_vnfd
            vnfd-connection-point-ref: vnf-cp0

    -   id: vEPC_SGW_nsd_vld1
        name: vEPC_SGW_nsd_vld1
        short-name: vEPC_SGW_nsd_vld1
        type: ELAN
        vnfd-connection-point-ref:
        -   member-vnf-index-ref: 1
            vnfd-id-ref: vEPC_SGW_vnfd
            vnfd-connection-point-ref: vnf-cp1
```

B.3 SGW Cloud-Init Config File

```
#cloud-config
timezone: Europe/London
hostname: sgw-{{mcc}}{{mnc}}-{{tac}}-uob
runcmd:
- echo "127.0.0.1 sgw-{{mcc}}{{mnc}}-{{tac}}-uob" | sudo tee -a /etc/hosts
- sudo python3 /usr/local/nh-vepc-api/cli.py sgw_setup --mcc {{mcc}}
```

```
    --mnc {{mnc}} --tac {{tac}} --gtpc {{gtpc}} --gtpu {{gtpu}}
    --server_addr {{server_addr}} --server_port 22 --username {{username}}
    --password {{password}}
output: { all: '| tee -a /var/log/cloud-init-output.log' }
```

B.4 PGW VNF Descriptor

```
#vEPC_PGW_vnfd.yaml
vnfd:vnfd-catalog:
vnfd:
-   id: vEPC_PGW_vnfd
    name: vEPC_PGW_vnfd
    short-name: vEPC_PGW_vnfd
    description: Virtual SGW based on Open5Gs, enhanced with CLI agent to
    support automated deployment.
    vendor: UoB
    version: '1.0'

    mgmt-interface:
        cp: vnf-cp0

    vdu:
    -   id: vEPC_PGW_vnfd-vPGW
        name: vEPC_PGW_vnfd-vPGW
        description: vEPC_PGW_vnfd-vPGW
        count: 1

        vm-flavor:
            vcpu-count: 4
            memory-mb: 4096
            storage-gb: 20

        image: 'base_open5gs'

        cloud-init-file: 'cloud_config'

        interface:
        -   name: ens3
```

```
32              type: EXTERNAL
33              virtual-interface:
34                  type: PARAVIRT
35              external-connection-point-ref: vnf-cp0
36              mgmt-interface: true
37          -   name: ens4
38              type: EXTERNAL
39              virtual-interface:
40                  type: PARAVIRT
41              external-connection-point-ref: vnf-cp1
42          -   name: ens5
43              type: EXTERNAL
44              virtual-interface:
45                  type: PARAVIRT
46              external-connection-point-ref: vnf-cp2
47
48          vdu-configuration:
49              juju:
50                  charm: vepc
51
52              initial-config-primitive:
53              -   name: config
54                  parameter:
55                  -   name: ssh-hostname
56                      value: <rw_mgmt_ip>
57                  -   name: ssh-username
58                      value: ubuntu
59                  -   name: ssh-password
60                      value: ubuntu
61                  seq: '1'
62
63              -   name: pgw-setup
64                  parameter:
65                  -   name: gtpc_dev
66                      value: <gtpc_dev>
67                  -   name: gtpu_dev
68                      value: <gtpu_dev>
69                  -   name: sgi_dev
```

```
70                  value: <sgi_dev>
71              -   name: uepool
72                  value: <uepool>
73              -   name: dns1
74                  value: <dns1>
75              -   name: dns2
76                  value: <dns2>
77              seq: '2'
78
79          -   name: service-publish
80              parameter:
81              -   name: element
82                  value: pgw
83              -   name: mcc
84                  value: <mcc>
85              -   name: mnc
86                  value: <mnc>
87              -   name: tac
88                  value: <tac>
89              -   name: apn
90                  value: <apn>
91              -   name: addr
92                  value: <addr>
93              -   name: port
94                  value: <port>
95              -   name: username
96                  value: <username>
97              -   name: password
98                  value: <password>
99              seq: '3'
100
101     connection-point:
102     -   name: vnf-cp0
103     -   name: vnf-cp1
104     -   name: vnf-cp2
```

B.5 PGW NS Descriptor

```
#vEPC_PGW_nsd.yaml
nsd:nsd-catalog:
nsd:
-   id: vEPC_PGW_nsd
    name: vEPC_PGW_nsd
    short-name: vEPC_PGW_nsd
    description: Generated by OSM package generator
    vendor: UoB
    version: '1.0'

    constituent-vnfd:
    -   member-vnf-index: 1
        vnfd-id-ref: vEPC_PGW_vnfd

    vld:
    -   id: vEPC_PGW_nsd_vld0
        name: management
        short-name: management
        type: ELAN
        mgmt-network: 'true'
        vim-network-name: 'mgmt'
        vnfd-connection-point-ref:
        -   member-vnf-index-ref: 1
            vnfd-id-ref: vEPC_PGW_vnfd
            vnfd-connection-point-ref: vnf-cp0

    -   id: vEPC_PGW_nsd_vld1
        name: vEPC_PGW_nsd_vld1
        short-name: vEPC_PGW_nsd_vld1
        type: ELAN
        vnfd-connection-point-ref:
        -   member-vnf-index-ref: 1
            vnfd-id-ref: vEPC_PGW_vnfd
            vnfd-connection-point-ref: vnf-cp1

    -   id: vEPC_PGW_nsd_vld2
        name: vEPC_PGW_nsd_vld2
```

```
        short-name: vEPC_PGW_nsd_vld2
        type: ELAN
        vnfd-connection-point-ref:
        -   member-vnf-index-ref: 1
            vnfd-id-ref: vEPC_PGW_vnfd
            vnfd-connection-point-ref: vnf-cp2
```

B.6 PGW Cloud-Init Config File

```
#cloud-config
timezone: Europe/London
hostname: pgw-{{mcc}}{{mnc}}-{{apn}}-uob
write_files:
  - path: /etc/sysctl.conf
    content: |
        net.ipv4.ip_forward=1
runcmd:
  - echo "127.0.0.1 pgw-{{mcc}}{{mnc}}-{{apn}}-uob" | sudo tee -a /etc/hosts
  - sudo sysctl -p /etc/sysctl.conf
  - sudo python3 /usr/local/nh-vepc-api/cli.py pgw_setup --mcc {{mcc}}
    --mnc {{mnc}} --apn {{apn}} --gtpc {{gtpc}} --gtpu {{gtpu}
    --ue_pool {{ue_pool}} --dns {{dns1}} {{dns2}} --realm {{realm}}
    --pcrf_fqdn {{pcrf_fqdn}} --pcrf_addr {{server_addr}}
    --server_addr {{server_addr}} --server_port 22 --username {{username}}
    --password {{password}}
output: { all: '| tee -a /var/log/cloud-init-output.log' }
```

BIBLIOGRAPHY

[1] 3GPP.
Domain name system procedures; stage 3, *TS 29.303 Release 15*, 2019.

[2] 3GPP.
Nr; physical channels and modulation, *TS 38.211 Release 15*, 2019.

[3] 3GPP.
Procedures for the 5g system (5gs) (5GS), *TS 23.502 Release 15*, 2019.

[4] 3GPP.
Study on management and orchestration of network slicing for next generation network, *TS 28.801 Release 15*, 2019.

[5] 3GPP.
System architecture for the 5g system (5GS), *TS 23.501 Release 15*, 2019.

[6] Dynamic Spectrum Alliance.
Online resources, 2020.

[7] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer.
Survey on network virtualization hypervisors for software defined networking.
IEEE Communications Surveys Tutorials, 18(1):655–685, 2016.

[8] S. D'Oro, F. Restuccia, and T. Melodia.
Toward operator-to-waveform 5g radio access network slicing.
IEEE Communications Magazine, 58(4):18–23, 2020.

[9] L. Doyle, J. Kibiłda, T. K. Forde, and L. DaSilva.
Spectrum without bounds, networks without borders.
Proceedings of the IEEE, 102(3):351–365, March 2014.

[10] Y. Duan, G. Fu, N. Zhou, X. Sun, N. C. Narendra, and B. Hu.
Everything as a service (xaas) on the cloud: Origins, current and future trends.
In *2015 IEEE 8th International Conference on Cloud Computing*, pages 621–628, June 2015.

[11] ETSI.
Creating your own vnf charm, OSM.

[12] ETSI.
Osm information model.

[13] ETSI.
Network functions virtualisation (nfv); architectural framework, ETSI GS NFV 002, 2014.

[14] ETSI.
Network functions virtualisation (nfv); management and orchestration, ETSI GS NFV MAN 001, 2014.

[15] ETSI.
Network functions virtualisation (nfv) release 3; evolution and ecosystem; report on network slicing support with etsi nfv architecture framework, ETSI GR NFV-EVE 012, 2017.

[16] ETSI.
Mec deployments in 4g and evolution towards 5g, ETSI White Paper No. 24, 2018.

[17] ETSI.
Multi-access edge computing (MEC); framework and reference architecture, ETSI GS MEC 003, 2019.

[18] Xenofon Foukas, Navid Nikaein, Mohamed M. Kassem, Mahesh K. Marina, and Kimon Kontovasilis.
Flexran: A flexible and programmable platform for software-defined radio access networks.
In *Proceedings of the 12th International on Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '16, page 427–441, New York, NY, USA, 2016. Association for Computing Machinery.

[19] I. Giannoulakis, G. Xylouris, E. Kafetzakis, A. Kourtis, J. O. Fajardo, P. S. Khodashenas, A. Albanese, H. Mouratidis, and V. Vassilakis.
System architecture and deployment scenarios for sesame: Small cells coodination for multi-tenancy and edge services.
In *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, pages 447–452, June 2016.

[20] L. Giupponi, R. Agusti, J. Perez-Romero, and O. Sallent.
Inter-operator agreements based on qos metrics for improved revenue and spectrum efficiency.
Electronics Letters, 44(4):303–304, 2008.

[21] GSMA.
Mobile infrastructure sharing, 2012.

[22] GSMA.
Infrastructure sharing: An overview, 2019.

[23] Anta Huang and Navid Nikaein.
Demo: Ll-mec a sdn-based mec platform.
In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, MobiCom '17, page 483–485, New York, NY, USA, 2017. Association for Computing Machinery.

[24] Internet Engineering Task Force (IETF).
The yang 1.1 data modelling language, 2016.

[25] E. A. Jorswieck, L. Badia, T. Fahldieck, E. Karipidis, and J. Luo.
Spectrum sharing improves the network efficiency for cellular operators.
IEEE Communications Magazine, 52(3):129–136, March 2014.

[26] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig.
Software-defined networking: A comprehensive survey.
Proceedings of the IEEE, 103(1):14–76, 2015.

[27] C. Liang and F. R. Yu.
Wireless virtualization for next generation mobile cellular networks.
IEEE Wireless Communications, 22(1):61–69, February 2015.

[28] Mark Newman, Chief Analyst, TM Forum.
5G future business models for monetization, 2019.

[29] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner.
Openflow: Enabling innovation in campus networks.
SIGCOMM Comput. Commun. Rev., 38(2):69–74, March 2008.

[30] Ioannis Neokosmidis, Theodoros Rokkas, Dimitrios Xydias, and Maria Rita Spada.
Regulatory considerations in the 5g era: The 5gcity neutral host case.
In John MacIntyre, Ilias Maglogiannis, Lazaros Iliadis, and Elias Pimenidis, editors, *Artificial Intelligence Applications and Innovations*, pages 111–120, Cham, 2019. Springer International Publishing.

[31] NGMN Alliance.
5G white paper, 2015.

[32] N. Nikaein, X. Vasilakos, and A. Huang.
Ll-mec: Enabling low latency edge applications.

In *2018 IEEE 7th International Conference on Cloud Networking (CloudNet)*, pages 1–7, 2018.

[33] Navid Nikaein, Mahesh K. Marina, Saravana Manickam, Alex Dawson, Raymond Knopp, and Christian Bonnet.
Openairinterface: A flexible platform for 5g research.
SIGCOMM Comput. Commun. Rev., 44(5):33–38, October 2014.

[34] Organisation for the Advancement of Structured Information Standards ("OASIS").
TOSCA technical committee, 2016.

[35] 5GCity H2020 project.
Online resources, 2019.

[36] DBS Group Research.
The push for 5g: Shaking up the landscape, 2017.

[37] R. Schmidt, C. Chang, and N. Nikaein.
Flexvran: A flexible controller for virtualized ran over heterogeneous deployments.
In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–7, 2019.

[38] Rob Sherwood, Glen Gibb, Kok-Kiong Yap, Guido Appenzeller, Martin Casado, Nick McKeown, and Guru Parulkar.
FlowVisor: A network virtualization layer.
page 15.

[39] Yasir Zaki, Liang Zhao, Carmelita Goerg, and Andreas Timm-Giel.
LTE mobile network virtualization.
16(4):424–432.