Deliverable D2.1

5G-VINNI Solution facility sites High Level Design (HLD) - v1
Norway Facility Site Annex
(Release 4)

Editor:	Pål Grønsund
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	N/A
Actual delivery date:	30th Jun 2020 (M30)
Suggested readers:	Telecom professionals
Version:	1.0
Total number of pages:	184
Keywords:	5G, Solution Design, High Level Design, RAN, Mobile Core, Transport, Orchestration, MANO, Satellite, Edge Cloud, Security, Slicing, Services, ICT-17, ICT-19

Abstract

Description of network services for the 5G-VINNI Norway Facility site. Includes configuration of Infrastructure, RAN, Core, MANO and E2E Service Orchestration components and of the interconnections among them. Used as a reference for the orchestration and testing activities. Description of the cross-facility site services and interconnection requirements and configurations.

[End of abstract]

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 815279.

Impressum

Full project title	5G Verticals Innovation Infrastructure
Project acronym	5G-VINNI
Number and title of work-package	WP2 5G-VINNI End-to-End Facility Implementation and Infrastructure Integration
Number and title of task(s)	T2.1 Mapping of the Reference Architecture to Facility sites
Document title	5G-VINNI Solution facility sites High Level Design (HLD) – v1 – Norway Facility Site Annex – (Release 4)
Editor: Name, company	Pål Grønsund, Telenor
Work-package leader: Name, company	Terje Rød, Ericsson

Copyright notice

Executive summary

This document is an annex to 5G-VINNI Deliverable 2.1. This document is the High Level Design (HLD) document for the Norway facility site in 5G-VINNI. It describes the Release 4.

List of authors

Company	Author
Nokia	Adnan Khan, Duncan Silvey, Antonios Dimitriadis, Tirthankar Gosh
Ericsson	Dominik Zoric, Hrvoje Marinovic, Jano Pitter
Telenor	Pål Grønsund, Andres Gonzalez, Kashif Mahmood, Stefan Heck
Huawei	Geir Nevjen, Eivind Mikkelsen, Chen Peiyao
Cisco	Hana Baccouch

Table of Contents

List of figures

List of tables

Abbreviations

5G	Fifth Generation (mobile/cellular networks)
5G-VINNI	5G Verticals INNovation Infrastructure
AC	Alternating Current
AKA	Authentication and Key Agreement protocol
AMBR	Aggregate Maximum Bit Rate
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
APN	Access Point Name
AUSF	Authentication Server Function
AV	Authentication Vector
AVRS	Accelerated Virtual Routing and Switching
BE	Back End
BFD	Bidirectional Forwarding Detection
BGP	Boarder Gateway Protocol
CBAM	CloudBand Application Manager
CBND	CloudBand Network Director
CDR	Charging Data Record
CGNAT	Carrier Grade NAT
CN	Core Network
CP	Control Plane
CPRI	Common Public Radio Interface
CPU	Central Processing Unit
CSP	Communication Service Provider
CSR	Cell Site Router
DC	Datacenter
DC	Direct Current
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPDK	Data Plane Development Kit
E2E	End to End
eCPRI	Enhanced CPRI
EDA	Ericsson Dynamic Activation
EMS	Element Management System
eNB	evolved NodeB
EPC	Evolved Packet Core
EPG	Evolved Packet Gateway
ESM	EPC Subscription Manager
ETSI	European Telecommunications Standard Institute
EVR	Ericsson Virtual Router
FE	Front End
FMC	Fixed Mobile Convergence
FSB	File Server Board
gNB	gNodeB (g=Next Generation)
GPB	General Processor Board
GPRS	General Packet Radio System
GRE	Generic Routing Encapsulation
GSC	Global Session Controller
GTP	GPRS Tunnelling Protocol

gUE	g User Equipment (g=Next Generation)
GW	Gateway
HLD	High Level Design
HLR	Home Location Register
HOT	Heat Orchestration Template
HSS	Home Subscriber Server
iLOM	Integrated Lights Out Manager
IP	Internet Protocol
IPOS	IP Operating System
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
LLD	Low Level Design
LTE	Long Term Evolution
MANO	Management and Orchestration
MEC	Mobile Edge Computing, Multi-access Edge Computing
MGMT	Management
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
NAT	Network Address Translation
NCB	Node Controller Board
NCIR	Nokia Cloud Infrastructure Real-time
NDCS	Nokia Data Center Solution
NFS	Network File System
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVO	Network Function Virtualization Orchestrator
NR	New Radio
NRF	Network Repository Function
NSA	Non Stand Alone
NSSF	Network Slice Selection Function
NTP	Network Time Protocol
NVMe	Non Volatile Memory Express
O&M	Operations and Maintenance
OAM	Operations, Administration and Maintenance
OCP	Open Compute Project
OOB	Out Of Band
OS	Operating System
OSPF	Open Shortest Path First
OVS	Open Virtual Switch
PCF	Policy and Charging Function
PCIe	Peripheral Component Interconnect Express
PCRF	Policy and Charging Rules Function
PDU	Power Distribution Unit
PE	Provider Edge
PGW	PDN Gateway (PDN= Packet Data Network)
PLMN	Public Land Mobile Network
PSC	PGW Session Controller
PSU	Power Supply Unit
QEMU	Quick EMUlator
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network

RAT	Radio Access Technology
RDIMM	Registered Dual In-Line Memory Module
RMC	Rack Management Controller
RO	Resource Orchestrator
SA	Stand Alone
SATA	Serial Advanced Technology Attachment
SCP	Secure Copy Protocol
SCTP	Stream Control Transmission Protocol
SFTP	SSH File Transfer Protocol (SSH=Secure Shell)
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SMF	Session Management Function
SO	Service Orchestrator
SSC	SGW Session Controller
TDD	Time Divistion Duplex
TOSCA	Topology and Orchestration Specification for Cloud Applications
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UDM	Unified Data Management
UDR	Unified Data Repository
UP	User Plane
UPF	User Plane Function
VDC	Volts Direct Current
VIM	Virtualized Infrastructure Manager
VLAN	Virtual Local Area Network
vLC	virtual Line Card
VM	Virtual Machine
VN	Virtual Network
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
vNIC	virtual NIC
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
vRP	Virtual Route Processor
vRP	virtual Route Processor
vSFO	virtual Service Forwarder
VXLAN	Virtual Extensible Local Area Network

1 Introduction

1.1 Scope

This document describes the high-level design (HLD) of the Norway facility site. Section 2 describes the E2E design and detailed solution design, respectively of RAN, transport, 5G EPC, 5G Core, IMS, MANO and service orchestration, central cloud, edge cloud, satellite, security and distributed IoT data fabric. Section 0 presents the slices, services and applications implemented in the Norway facility site. Section 5 presents the dimensioning also taking into account aspects such as anti-affinity rules when deploying the VNFs. Description of the cross-facility site services and interconnection requirements and configurations are presented in Section 6 while Section 7 handles the APIs for orchestration and network management.

The 5G-VINNI facility sites will have a release cycle of six months where the first release (Release 0) was due in month 12 of the project. Release 0 has been used for internal validation of the 5G-VINNI facility and after testing and validation, Release 1 was launched in month 18 being the first release available for the verticals to trial their use cases. The focus of this version of the D2.1 annex of the Norway facility site is on Release 4.

1.2 5G VINNI Facility

The 5G-VINNI Facility with main and experimentation facility sites is illustrated in Figure 1.1, where the Norway facility site being the focus of this HLD is marked with the green arrow.

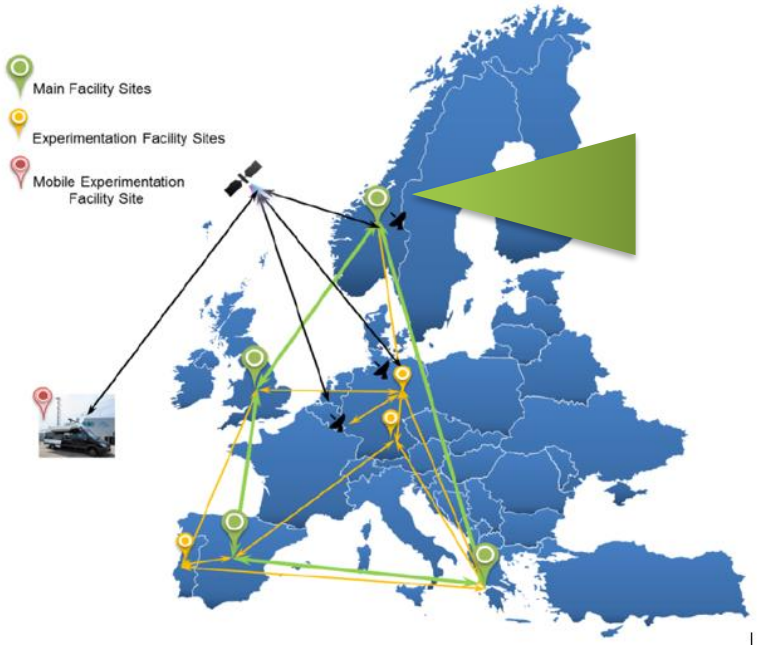


Figure 1.1 : 5G-VINNI Facility

1.3 Facility-site: Norway

Table 1.1 : Facility-Site details

Facility-site	
Type	Main Facility site
Locations	Oslo area
Provider	Telenor
5G-VINNI Release	*Release 4*

Note: “Facility-site” has the same meaning as “Site”. Within one site can be one or more “Locations”.

1.3.1 Location details

Table 1.2 : Location address

Address	
City, Street	*Snarøyveien 30,1331 Fornebu*
Building, Room number	*N/A*

1.3.2 Vendors information

Table 1.3 : Location vendors details

Domain	**Vendor**
5G RAN	*Ericsson, Huawei*
5G Core	*Ericsson*
NFVI	*Nokia*
E2E Service Orchestration	*Nokia*
Firewall	*PaloAlto*
IMS	*Metaswitch*
Testing functions	*Keysight*
Distributed Data Function	*Cisco*

2 Facility-site overview

5G VINNI Norway Facility-site network is built on two Data Centres. The main one is called **Central site** and the smaller one is called **Edge site**. These two sites are shared by all deployed slices. More **Edge sites** are expected and in the planning with ICT-19 projects going forward.

For NSA Slices selection DECOR functionality is implemented. MME-1 from Slice #1 is default MME and Figure 2.1 the type of slices are supported, what VNFs are deployed and how they are shared with slices at the time of writing this document. The slice configuration and specifically which VNFs the slices are composed of can be changed as needed based on the real use case needs.

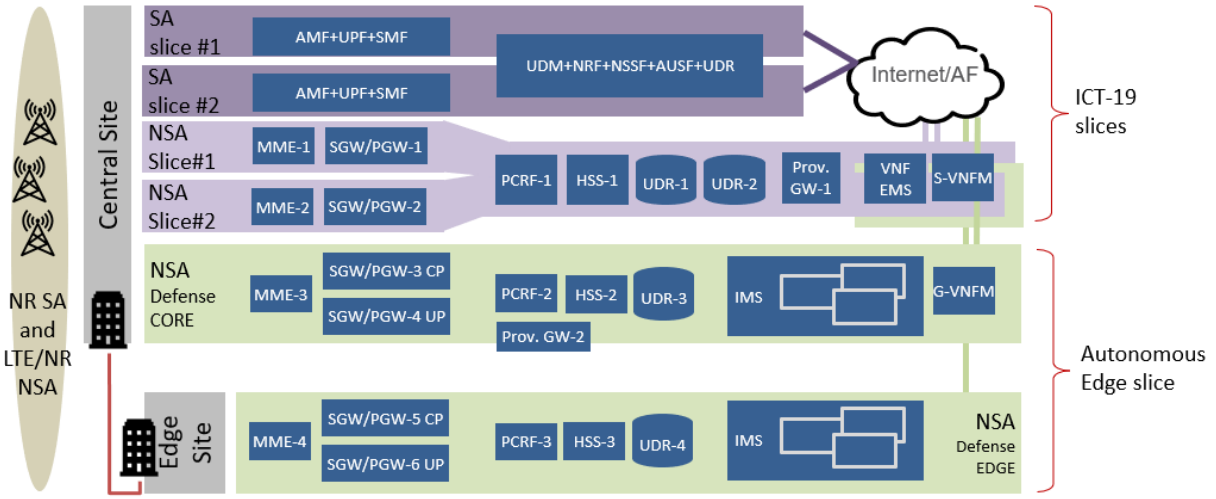


Figure 2.1 : Norway NSA and SA slicing

Figure 2.2 shows how NSA and SA Networks are mapped to the ETSI NFV architecture. Slices and VNFs deployment are fully automated using S-VNFM or G-VNFM and triggered from the Service Orchestrator or NFVO.

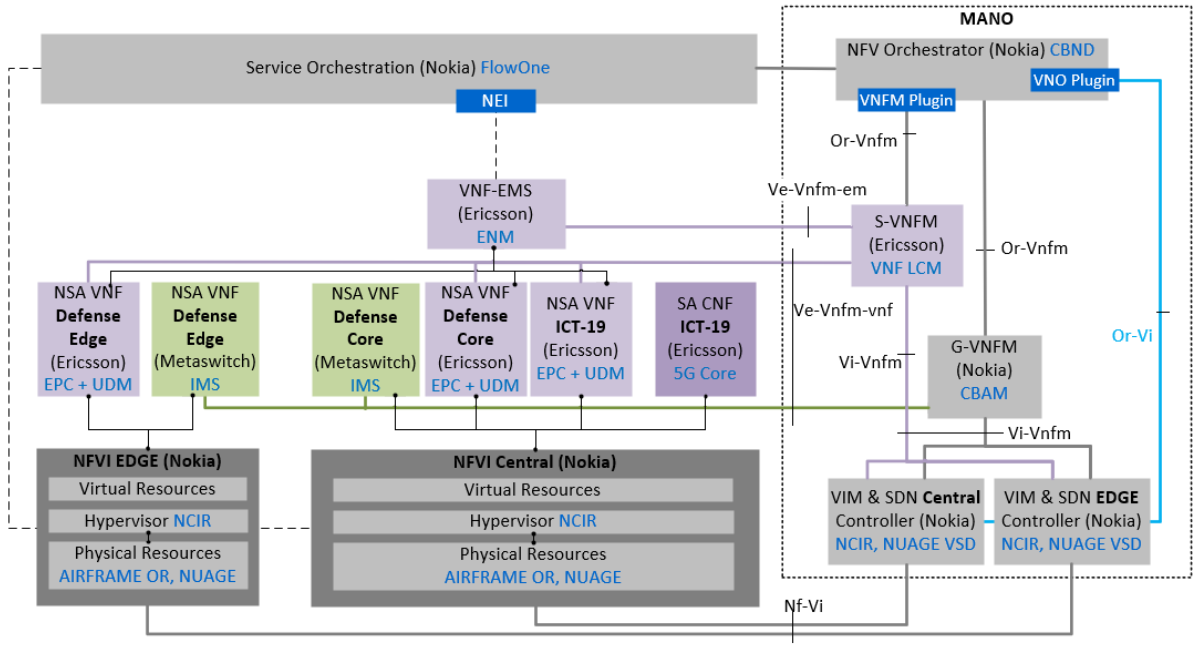


Figure 2.2 : NFV Architectural Framework for NSA and SA

3 Facility-site building blocks

3.1 Transport Network

The transport network for Norway facility site is based on the commercial transport network of Telenor Norway and is illustrated in Figure 3.1. Cell site routers (CSR) are used for connecting the RAN sites to the transport network. These CSRs exchange IP routes (OSPF/BGP) with the transport network, which then assigns the whole traffic into multiple dedicated VPNs that correspond to different slices.

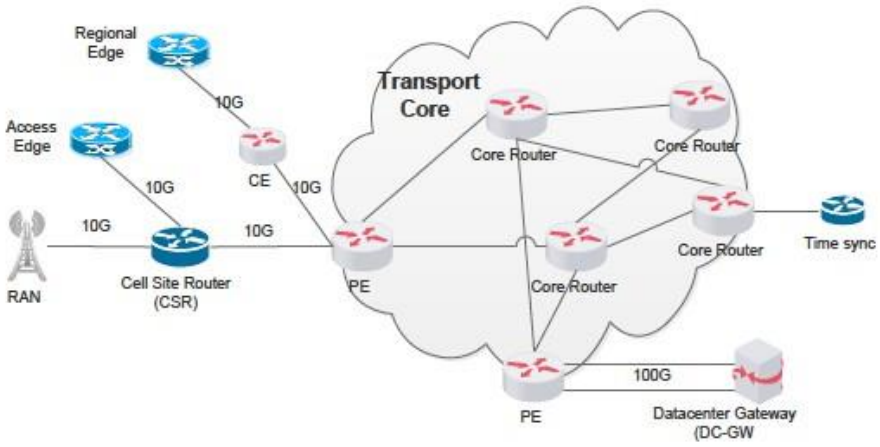


Figure 3.1 : Transport network for Norway Facility site

Cell site routers (CSR) are used for connecting the RAN sites to the transport network. These CSRs exchange IP routes (OSPF/BGP) with the transport network, which then assigns the whole traffic into multiple dedicated VPNs that correspond to different slices. Two different type of CSRs, Ericsson R6675 and Huawei ATN910-F, were commissioned initially for the 5G-VINNI site for Ericsson and Huawei RAN sites, respectively. But as the transport network for Norway facility is based on the commercial network of Telenor Norway only ATN910-F is used as that is the verified CSR. Unless otherwise specified, 10Gbps interfaces will be used in all CSRs in Norway facility.

The boarder leaf acting as the datacenter gateway in the NFV cloud is connected to the Provider Edge (PE) router. The PE router is used to connect the mobile core and NFV cloud to the transport network. The connections on the PE router are terminated on two different cards to secure redundancy within the PE.

Two boarder leaf switches will connect to the PE. Note that in the NFV Cloud one pair of switches will be used, where that one switch is assigned the role of boarder leaf/datacentre gateway, spine switch and leaf switch. This is possible since the deployment is limited to one rack of servers. In the case of expansion beyond that the spine and leaf would need to be separated. The interface between PE and the boarder leaf in the datacentre will use 100Gbps interfaces.

The management switch will connect to all the elements through iLOM, the OOB port on the Leaf/Spine switch (210 WBX 32QSFP28), and an uplink to the PE router.

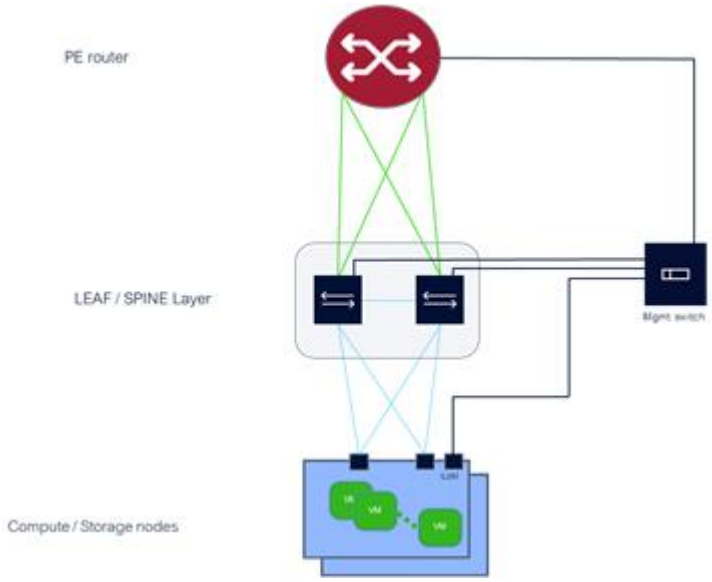


Figure 3.2 : Fronthaul and backhaul setup

The router to be used at edge sites depends on whether it is an edge at the customer premise, at the gNB or in a regional site serving multiple gNBs. In the case of edge at customer premise and RAN site the CSR router or another Customer Edge (CE) router will be used. In most cases a CE router and a VPN service (Nordic Connect) is used. In case of in a regional location serving multiple gNBs the PE will be used, then connected to a Customer Edge (CE) router. Connectivity to internet will be handled by the commercial transport network in Telenor Norway mobile operation (referred to as the BRUT network). Traffic will go from the datacenter to a dedicated VRF (Virtual Routing Function) interface in the PE designated for internet traffic.

The transport Core network including the PE is managed and monitored by Telenor Norway operations and so is the CSR and CE. DC-GW (Boarder-leaf/Spine switch) is managed by Nokia.

3.2 5G RAN

3.2.1 eNB

3.2.1.1 Interfaces

LTE interfaces are divided in internal interfaces and external interfaces as shown in Figure 3.3 and Figure 3.4, respectively. Internal interfaces are used for communication between nodes in the LTE network while the external interface is used for communication between a node in the LTE network and a node external to the LTE network.

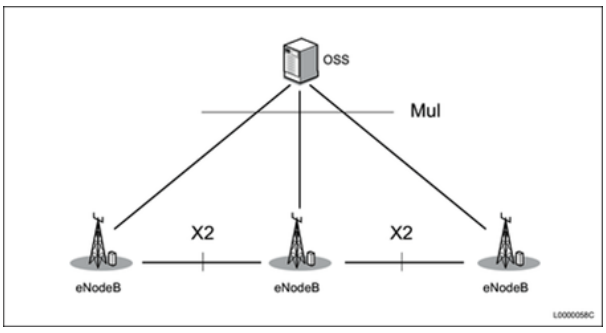


Figure 3.3 : eNBs - internal interfaces

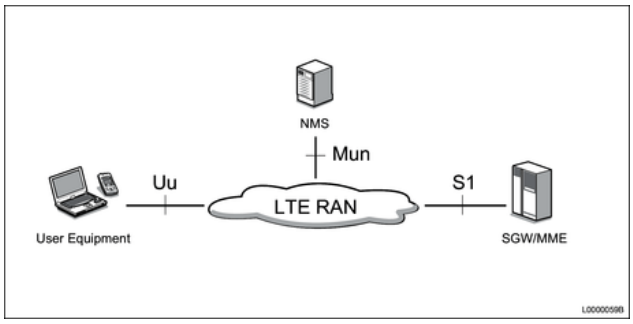


Figure 3.4 : eNBs - external interfaces

Table 3.1 : Description of LTE Interfaces

Interface	Description
Mul	Interface between the eNodeB and the OSS for network management. The Mul interface is also used to manage the node on site using client software on a PC.
Mun	Provides access to the OSS for external Network Management Systems.
S1	Interface between the eNodeB and Evolved Packet Core (EPC). The S1 interface is divided into the control plane and the user plane. The S1 control plane terminates in the MME core network node. The S1 user plane terminates in the SGW core network node. The S1 interface provides the capability for individual eNodeBs to connect to several MME and SGW nodes.
Uu	The Uu is the radio interface or the air interface and connects the eNodeB and the UE. The Uu interface carries payload data and control information for the radio connection in terms of mobility, security, and bearer management.
X2	Connects eNodeB pairs having neighbouring cells.

3.2.2 gNB

The Norway facility will leverage gNB from Ericsson and Huawei.

3.2.2.1 Concept

NG Radio Access Network

The NG-RAN in Norway is built for multiple bands, supporting Non-standalone (NSA) as well as Standalone (SA) deployments.

Components used in NG- RAN

The radio components used in 5G-VINNI are based on Antenna Integrated Radios for mid-band (3600 MHz) and high-band (24.5-27.25 GHz). The antenna integrated radio products are designed with 64T64R architecture for 3600 MHz frequency band both for Huawei and Ericsson while for the 26 GHz frequency band it is 512T512R for Ericsson while it is 384T384R (768 dipoles) for Huawei. Advanced functionality such massive MIMO (Multiple Input Multiple Output) and 256QAM modulation is supported. The antenna integrated radios are connected to the baseband unit which is designed for 19” rack installation and requires only 1U rack space. The interface towards the

advanced antenna integrated radios is based on eCPRI to minimize the number of required fibre links. The same baseband unit is also used for LTE when 5G is deployed in NSA setup.

The radios support 3GPP standardized 5G carrier bandwidths ranging from 20 MHz to 100 MHz for the mid-band frequencies and up to 400 MHz for the high-band frequencies. 3GPP standardized Time Division Duplex (TDD) patterns are supported.

For the non-standalone deployment in 5G-VINNI it has been decided to use 3GPP B1 (2100 MHz) as the LTE anchor band. The multi standard radio that supports 2100 MHz is designed with 4T4R architecture. It needs to be highlighted that LTE anchor carrier bandwidth will be aligned to the spectrum situation at the specific site location in Norway.

3.3 5G EPC

This section briefly describes 5G EPC VNFs, its internal structures and how they are integrated with the Nokia NFVI.

3.3.1 External interfaces for EPC VNFs

Ericsson Virtual Network Function (VNF) Virtual Machines (VMs) can run on the same or different Nokia compute node as Nokia SDN will use internal OVS switching. External network IP, all VNF interface IPs, Default Gateway IP and Service IP will be assigned dynamically and provided to the VNF by the NFVO during onboarding. Virtual IP (VIP) addresses are used. All these parameters provided by NFVO during onboarding will be specified individually in low level design (LLD).

In Figure 3.5, there is an example for the Mobility Management Entity (MME) VNF, where VNF VM1 (VM GBP-1) and VNF VM2 (VM GBP-2) communicates to each other on layer 2 networks. Static routing is expected for each VNF VM subnets.

In Figure 3.6 there is an example of Service IPs assigned to VNF MME. VIP1 and MME VIP2 belong to different subnet.

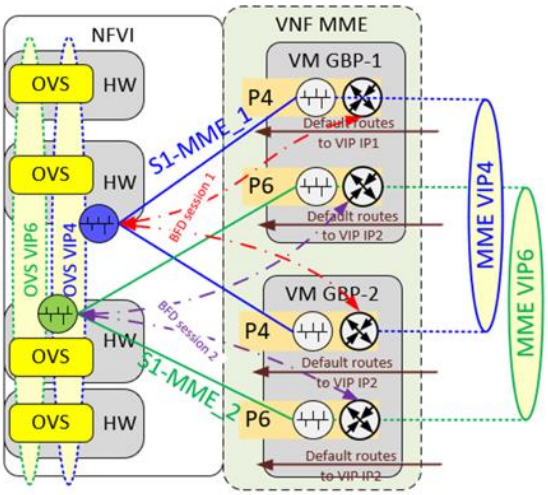


Figure 3.5 : MME, Example for SCTP Interfaces: S1-MME, S6a

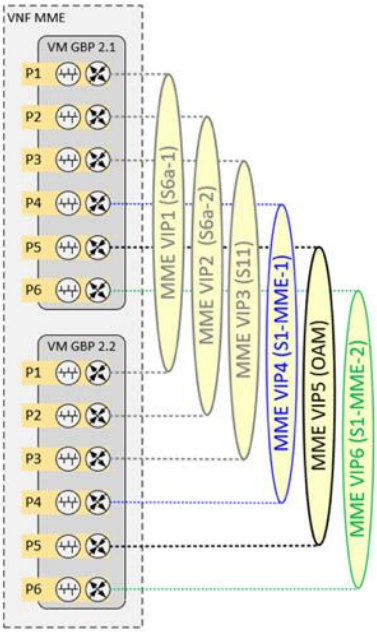


Figure 3.6 : VIP concept on MME VNF

3.3.2 MME - Mobility Management Entity

3.3.2.1 Concept

Mobility Management Entity (MME) is the main control node for LTE access network. The MME is responsible for handling signals between active UEs and the network within the EPC architecture. MME is also responsible for signalling between eNBs/gNBs and the core network. For continuous functionality, MME authenticates UEs by communicating with the HSS, and the mobility function allows the UE to access the network and keeps track of its location and state.

In 5G EPC the MME continues supporting legacy functionality based on 3GPP Rel-14 and older, adding 5G Option 3 content specified in 3GPP Rel-15. 3GPP Rel-15 introduces requirements for 5G operation as well as enhancements for LTE access.

3.3.2.2 Components

The software components of the virtual MME are distributed and executed on VMs as shown in Figure 3.7.

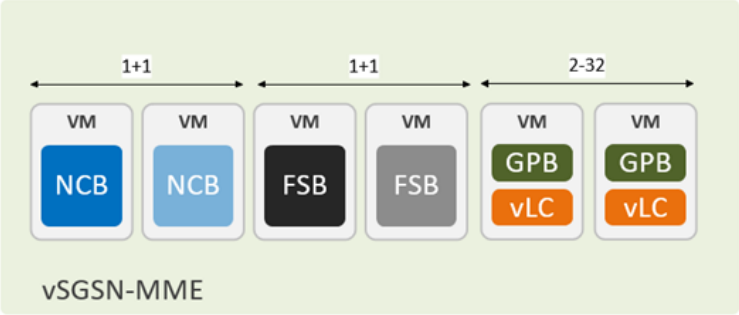


Figure 3.7 : High level architectural overview of vMME

The File Server Board (FSB) provides NFS storage and network boot services for all other VMs in the cluster. There is one primary FSB and one secondary FSB for redundancy.

The Node Controller Board (NCB) performs cluster supervision, software distribution, and provides O&M for the virtual MME. There is one active NCB and one passive NCB for redundancy.

The Combined General Processor Board (GPB) and virtual Line Card (vLC) performs MME application processing for LTE control plane and signalling. It also provides external connectivity with application aware single IP address load balancing (inbound) and forwarding (outbound), including support for session resilience

3.3.2.3 Deployment Type

The MME will be deployed as a Multi Host MME with integrated vLC. The vLC role is integrated in the GPB VMs. The main reason for this selection is that the workload will be evenly distributed across the compute hosts by avoiding packet intensive vLC VMs. This puts less demand on the compute host networking performance, especially the vSwitch.

3.3.2.4 Networking

A Virtual Network (VN) is a logically isolated L2/L3 network provided by the cloud infrastructure. It can be realized using different encapsulation or tunnelling technologies on top of a physical network as illustrated in Figure 3.8. The VN can be realized as an overlay network on top of an underlay network. For example, it is possible that an L2 overlay network spans multiple router hops in a routed L3 underlay network. How the VN is realized is transparent to the virtual MME as long as the characteristics required by the virtual MME are provided.

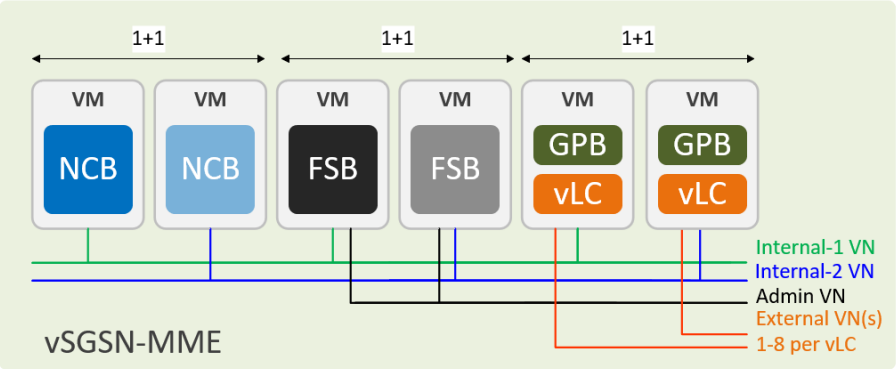


Figure 3.8 : Logical Virtual SGSN-MME Networking with Integrated vLC

Table 3.2 : MME Virtual Networks

VN Type	VN Name
Admin	Admin
Internal	Internal-1 and Internal-2
External	One or more External VNs (1-8 per vLC). Mandatory external traffic interfaces for this deployment are: **S11 interface:** The S11 interface is a GTP-based interface used for signalling between MME and the Serving Gateway. **S1-MME interface:** Connects the MME to eNodeB and UEs. The S1-MME interface is based on Stream Control Transmission Protocol (SCTP). S1 Application Protocol (S1-AP) messages are transferred between the MME and eNodeB, and NAS messages are transferred between the MME and UE. **S6a interface**: Connects the MME to the HSS. It enables transfer of subscription and authentication data for user access. The S6a interface is based on the Diameter protocol. **OAM interface**: The OAM interface provides the transfer of operation and maintenance traffic between the MME and the node management terminal.

Admin Interfaces

The Admin interface on the FSB connects to the Admin VN. The Admin interface is used for backup and restore of the virtual MME to an external storage server.

The Admin interface can also be used for temporary O&M access, using SSH, SCP, and SFTP when the normal O&M IP service through the vLC is not configured, or is lost. Typically, the temporary O&M access is used at initial configuration, and in some emergency situations. The Admin interface does not replace the normal O&M IP service through the vLC.

Internal Interfaces

The Internal-1 and Internal-2 VNs are used for the virtual MME VM-to-VM traffic. The Internal-1 VN is used for node internal traffic. The Internal-2 VN is used for node external traffic, sent between the vLCs and other VMs in the cluster.

External Interfaces

The External VNs are used for the virtual MME external traffic and is exchanged through the vLCs. The vLC vNICs connected to the External VNs are also referred to as vLC ports (see figure 2.6).

Network Separation

MME is configured with multiple IP Networks for network separation. Each MME IP Network is mapped to a separate vLC port, and therefore connected to a unique External VN. The application traffic is not VLAN tagged.

3.3.2.5 IP Connectivity and Routing

The virtual MME uses one or two IP service address per external logical interface. For example, S1-MME, S6a, O&M or NTP. The traffic on each logical interface is transparently load balanced across the cluster by the vLCs.

The virtual MME supports multiple IP Networks for (VPNs) network separation, and thus offers full flexibility to map IP services to IP Networks. Operators can also map IP networks to specific vLC ports.

Ericsson recommends using static routing in combination with BFD as routing protocol for external networks.

3.3.3 SGW and PGW - Serving Gateway and Packet Gateway

3.3.3.1 Concept

The Evolved Packet Gateway (EPG) acts as a gateway between mobile packet core networks and other packet data networks (such as the Internet, corporate intranets) and private data networks. In this role, the EPG is responsible for session management within the mobile network, as well as for encapsulation and de-encapsulation of bearer traffic sent to and from the Mobility Management Entity, MME.

The EPG includes support for 4G and 5G access in Evolved Packet Core network architecture and combines the logical nodes Packet Gateway (PGW) and Serving Gateway (SGW).

The EPG continues supporting legacy functionality based on 3GPP Rel-14 and older, adding 5G Option 3 content specified in 3GPP Rel-15. 3GPP Rel-15 introduces requirements for 5G operation (NR) as well as enhancements for LTE access.

3.3.3.2 Architecture

The virtual EPG application is built on Ericsson Virtual Router (EVR) using the Ericsson IP Operating System (IPOS). The software components of the virtual EPG are distributed and executed on VMs as indicated in Figure 3.9.

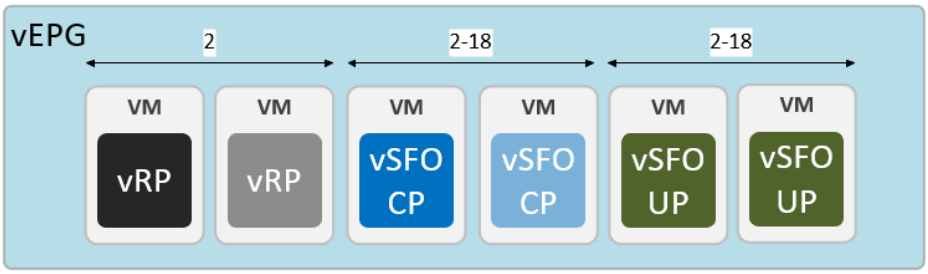


Figure 3.9 : Virtual EPG Logical Architecture

The VMs have the following roles:

Virtual Service-Forwarder (vSFO) provides combined application service, load balancing (LB) and data forwarding functions for the vEPG. vSFO VMs can be assigned to have the role as either Control Plane (CP) or User Plane (UP) for the vEPG.

User plane vSFO provides virtual EPG application user plane capabilities for LTE/NR. User plane vSFO also provide virtual EPG application aware load balancing (ingress) and forwarding (egress) traffic as well as Layer 2 and Layer 3 data forwarding.

Control plane vSFO provides virtual EPG application control plane capabilities for LTE/NR.

Virtual Route Processor (vRP) serves as a node manager for the virtual EPG application that performs cluster supervision, software distribution and provides O&M. There is one active vRP and one passive vRP for redundancy.

3.3.3.3 Networking

A Virtual Network (VN) is a logically isolated L2/L3 network provided by the cloud infrastructure. The VN can be realized as an overlay network using different encapsulation or tunnelling technologies, such as, VLAN (802.1Q), VXLAN, or GRE on top of a physical underlying network. It is possible that an L2 overlay network spans multiple router hops in a routed L3 underlying network. The VN is transparent to the virtual EPG, as long as the characteristics required by the virtual EPG are provided.

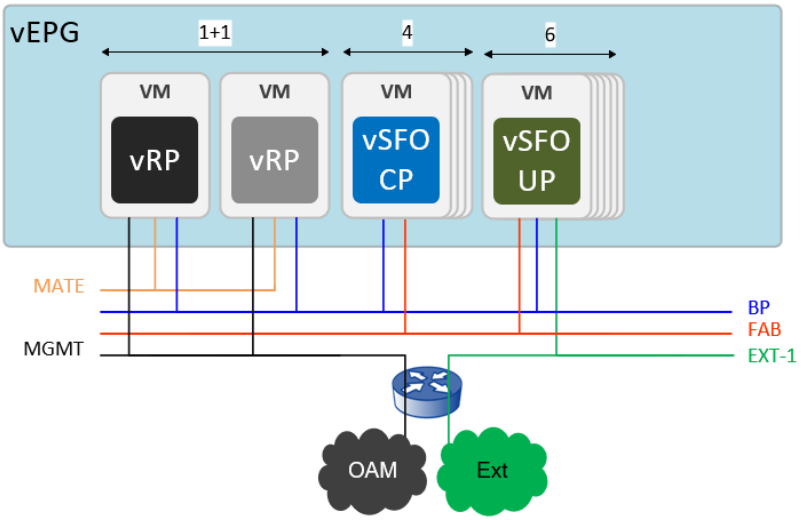


Figure 3.10 : Logical Virtual EPG Networking

Table 3.3 : EPG Virtual Networks

VN Type	VN Name
Admin	MGMT (Outband OAM)
Internal	MATE, BP, vFAB
External	EXT Mandatory external traffic interfaces for this deployment are: **Media**: Connects SGW to MME. This interface is used for control plane signalling, and to create, update, and delete EPS bearers. **Ran**: Connects SGW to eNBs or gNBs allowing for user data packet transportation. **Signalling:** Connects PGW to PCRF (Policy and Charging Rule Function). **OAM:** Operation and Maintenance of the EPG VNF. **Internet:** Provide IP connectivity Evolved Packet System (EPS) networks to external IP networks, such as the internet, corporate, or Internet Service Provider (ISP) service networks.

Admin Interface (MGMT)

The Admin interface on the vRP connects to the MGMT VN. The Admin interface is used for outband O&M access using SSH, SCP or SFTP when the normal OAM IP service through the vSFO is either not configured or lost. The outband OAM access is used at initial configuration, and also in some emergency situations. The Admin interface does not replace the normal OAM IP service through the vSFO VMs.

Internal Networks

MATE: Used for synchronization and monitoring traffic between active and hot standby vRP

BP: Used for internal signalling between all virtual EPG VMs

vFAB: Used for forwarding external control signalling and user data traffic between vSFOs

External Networks

All traffic VMs in vEPG are in a vSFO combined role where Virtual Forwarder (vFRWD) is combined as a load-balancer providing Virtual EPG application aware load balancing (ingress) and forwarding (egress). vSFO VMs is configured to have the role as either Control Plane (CP) or User Plane (UP). External control and user plane networks are configured on CP and UP vSFOs respectively utilizing virtio connections to the virtual switch (OVS). Performance boost techniques like Single Root IO Virtualization (SR-IOV) for i/O intensive workloads is supported if required in the future, but not deployed in this first phase.

3.3.3.4 IP Connectivity and Routing

The EPG supports routing of IP packets received from and sent to the networks on all internal and external interfaces. Static and dynamic routing protocols are supported, and optionally also supervised by BFD (Bidirectional Forwarding Detection).

For Vinni Static Routing Protocols will be used for all external networks. For each VRF default static routes will point to gateway address hosted by OVS.

3.3.4 PCRF - Policy and Charging Rules Function

3.3.4.1 Concept

PCRF is the Ericsson Multi-Access Policy Management Framework, which provides policy management for Mobile Broadband Networks, Fixed Broadband Networks, and Fixed-Mobile Convergence (FMC) Broadband Networks.

PCRF enables the applicability of policy control capabilities based on subscriber and service information. The main enabled policy types are related to service access control, Quality of Service (QoS) control and charging control, act as the PCRF in 3GPP standard.

3.3.4.2 Components

The virtual PCRF virtualization architecture consists of several VM taking different function roles:

- **Traffic Processors (TPs) VMs** provides the policy server implementation, quantity from 2 to 34. This VM are also referred as Payload (PL) VMs
- **System Controllers (SC) VMs** - 2 VM implementing the system controller function. These VMs provide the north-bound access to vPCRF and the cluster membership and control.
- **Virtual Router (VR)** - 4 VMs providing the Virtual Routing Service (based on Vyatta VR), 2 of the VR VM are responsible for Operation and Maintenance (OAM) tasks, and the other 2 for addressing the control plane traffic the Virtual PCRF manages.

  Note: VR's is kept for legacy reasons and is not used in the 5G VINNI solution

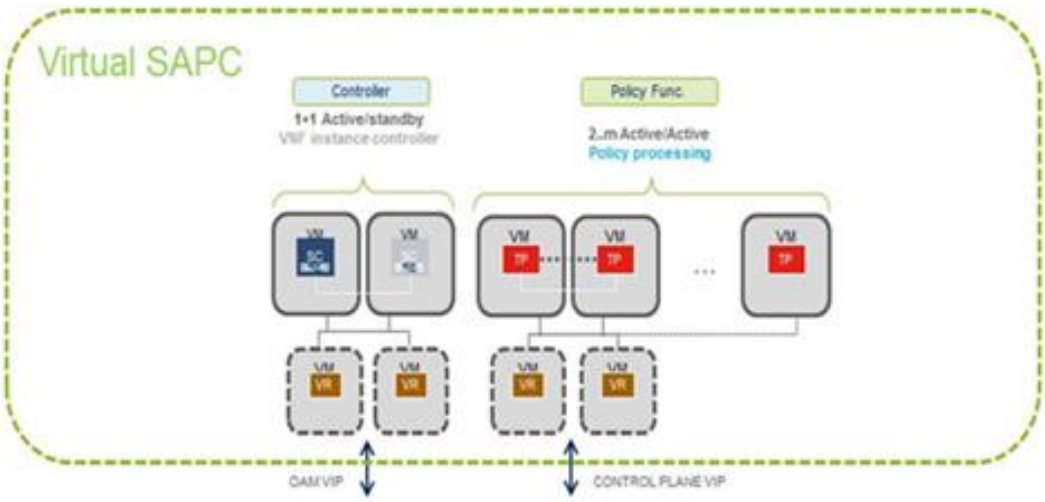


Figure 3.11 : Virtual PCRF (SAPC) Logical Architecture

PCRF application is a HW-agnostic, SW-only product that can be deployed on any HW fulfilling the minimum hardware requirements. It is possible to deploy the PCRF application cluster in several different HW configurations.

PCRF application cluster nodes and networks are virtualized, which allows the possibility of deploying the virtual cluster on a variable number of physical machines.

In 5G VINNI there will be four virtual machines each one of them with a different role which will be used for internal and external traffic routing.

- SC-1 and SC-2 are the system controllers (SC)
- PL-3 and PL-4 are the traffic payloads (PL)

SC-1 and SC-2 will be accessed through OAM_VIP.

PL-3 and PL-4 will be accessed through NW_VIP_SIG and NW_VIP_LDAP.

3.3.4.3 Networking

In this configuration, the System Controllers (SC) are directly connected to the OAM Gateway Routers and the Payloads (PL) are connected to the Traffic Gateway Routers, as shown in Figure 3.12.

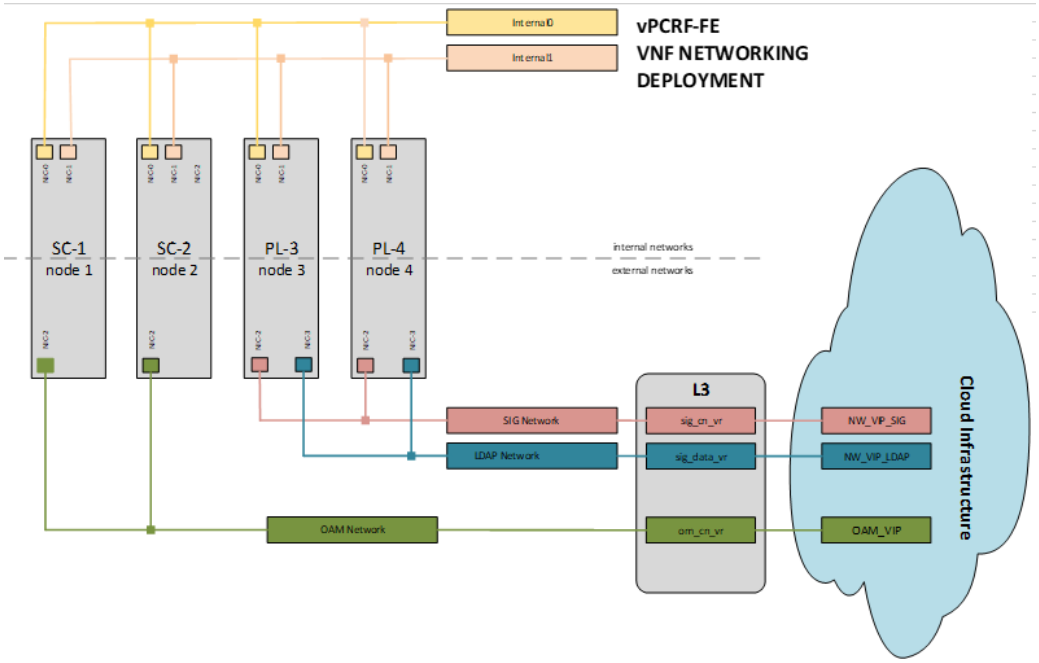


Figure 3.12 : PCRF (SAPC) Connected to the Gateway Routers of the External Network

The PCRF networks needed for this configuration are classified into the following categories, depending on their use and the region they belong to:

Internal: Internal networks inside the node are used to internally address the VMs in each PCRF node. Therefore, addresses within these networks are not routable outside the PCRF.

External: External networks are used to transport incoming and outgoing traffic between the PCRF SCs and PLs and the Gateway Routers, the latter serving as VIP Gateway Routers, so, these networks can also be referred to as VIP networks. Through these networks, the Virtual IP (VIP) addresses that neighbours can use to communicate with the PCRF node are accessible. These neighbours include, among others, PCEFs, External Databases, or Provisioning Systems. The addresses of the External networks must not overlap with other networks within the site.

Internal Networks

The Internal network provides internal VM cluster connectivity, and therefore exists in each PCRF node. This network is used for the communication between the members of the cluster, including traffic distribution, installation, booting and internal services, such as NTP and NFS.

Also, a Layer 2 Internal Network also exists for TIPC communication among the members of the cluster.

Virtual IP (VIP) Networks

The VIP addresses of the PCRF hide the internal architecture of the cluster by presenting only a limited set of IP addresses to the External network. Also, they provide scalability and redundancy for IP-based services by transparently distributing the IP traffic among the members of the PCRF node.

The VIP networks are used to provide access to the VIP addresses of the PCRF from the External network.

Table 3.4 collects the most relevant information regarding PCRF VIP networks.

Table 3.4 : VIP Networks Summary

Network Common Name	Purpose	Allocated VIPs
OAM VIP Networks	Provides access to the public IP addresses of the PCRF application for OAM and Provisioning purposes. There is always one mandatory OAM VIP Network to connect both OAM VIP Gateway Routers with the PCRF System Controllers. Also, there can be a second network dedicated to provisioning traffic.	OAM and Provisioning VIPs
Traffic VIP Networks	Provide access to the public Virtual IP addresses of the PCRF application for traffic handling. The Traffic VIP Networks connect both Traffic VIP Gateway Routers with the PCRF PLs providing the VIP addresses. The number of Traffic VIP Networks depends on the Traffic Network Separation Solution implemented.	Traffic VIPs

Virtual IP (VIP) Gateway Routers

VIP Gateway Routers are the integrating point of the PCRF cluster into the External network, and together with the VIP addresses of the PCRF, distribute and balance traffic.

External Networks

The External networks are used to interoperate with the neighbour's nodes in the customer networking. Addresses are always allocated from the IP range of the customer networking.

Through the External networks, the PCRF VIP addresses are reachable. When the PCRF is directly connected to the Gateway Routers of the External network, the External networks and the VIP networks are the same.

Table 3.5 collects the most relevant information regarding PCRF external networks.

Table 3.5 : External Networks Summary

Network Name	Purpose	Allocated VIPs
OAM Networks	OAM network. Provides a public IP address to access PCRF application for OAM and optionally, another public IP address for Provisioning purposes. The VIP for OAM and the VIP for provisioning, if exist, are external addresses reachable through this network. Provisioning network. Optional. It can be configured to separate provisioning traffic. In such cases, provisioning VIP is reachable through this network.	One OAM VIP per PCRF node in the site. One optional Provisioning VIP per PCRF node in the site. For Geographical Redundancy Active-Standby scenarios, one Provisioning VIP per GeoRed pair.

Network Name	Purpose	Allocated VIPs
Traffic Networks	Traffic network. Provides public Virtual IP addresses to access the PCRF application for traffic handling. For deployments with no traffic separation, all the VIP Addresses for traffic handling, Replication, and External Database are reachable through this network. For deployments with traffic separation, all the VIP Addresses for traffic handling, Replication, and External Database are reachable through different networks.	One or several Traffic VIPs per PCRF node in the site.

3.3.5 HSS - Home Subscriber Server and Subscriber Database

The Home Subscriber Server (HSS) Front End (FE) (HSS-FE) type of configuration makes it possible to deploy the HSS as a Frontend system, interconnected with a centralized database. This implies that subscriber data no longer reside in the HSS but in an External Database. This type of configuration applies to every module in HSS.

CUDB system is the data repository where related subscriber data is stored.

The HSS-FE needs to read subscriber data from CUDB to perform the HSS procedures. HSS-FE can be configured to store IMS/LTE subscriber data temporarily and reuse them along a network procedure.

3.3.5.1 Overview of User Data Consolidation (UDC)

User Data Consolidation (UDC) is the Ericsson Subscriber Data Management solution. UDC provides consolidation of user data for all network functions, like user authentication, service authorization, mobility management, policy control, and fraud protection on a single SDM system. It enables the convergence of the user profile related to former functions.

The UDC components in the scope of this project are described below:

Consolidated User Database (CUDB) is a geographically distributed and telecom-grade database used in UDC for user data storage in centralization scenarios as shown in Figure 3.13. CUDB provides local single logical points of traffic and provisioning access at network level. CUDB stores user information using an LDAP Data Information Tree (DIT) as the data model used by applications. CUDB provides an LDAP v3-compliant point of access to all LDAP clients connecting to it.

CUDB is a system made up of a set of CUDB nodes. There are two different types of CUDB nodes, with and without a PL VM replica. CUDB nodes with a PL VM replica provide access to the whole user-base, regardless of how data is distributed across CUDB nodes.

Ericsson Dynamic Activation (EDA) is the functional component in UDC that makes it possible to terminate the provisioning protocol, control the validation of the provisioning requests, write the data into the data store, and handle massive operations.

Home Subscriber Server (HSS) is the component in UDC that supports subscription management, user mobility management, session establishment procedures, authentication, authorization, user traffic protection, and generation of authentication vectors.

HSS-FE supports the following accesses in the context of the 3GPP specifications: Long Term Evolution (LTE) (E-UTRAN and NB-IoT), GSM/WCDMA Packet Switch (GPRS) (via S4-SGSN), and New Radio (NR) access with the 5G 3GPP non-standalone architecture. It provides mechanisms for the subscription, authentication, and mobility management related to the EPS.

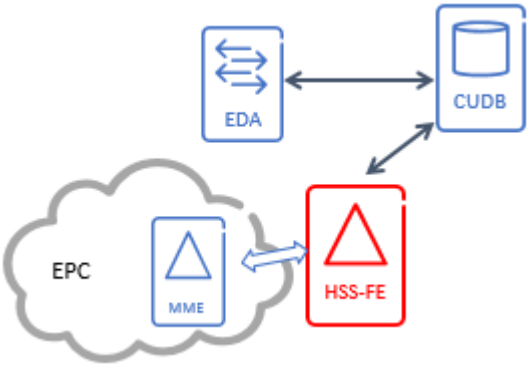


Figure 3.13 : Overview of UDC nodes (not including MME)

3.3.5.2 VUDC VNF Architecture

Figure 3.14 shows the VNFs with the number of VMs that will be deployed in each slice for vUDC. Note that vEDA will only be deployed in one of the slices, but will be integrated towards both slices.

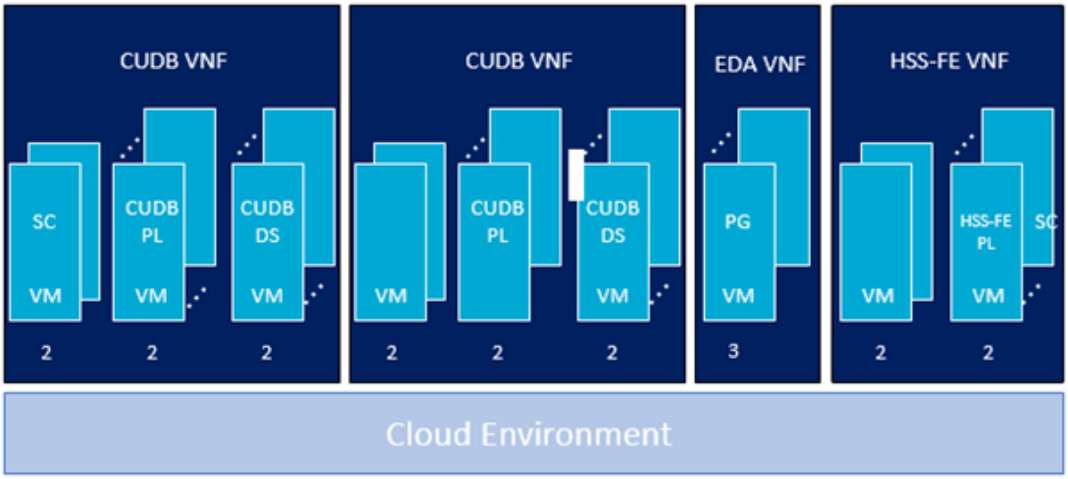


Figure 3.14 : Virtual CUDB Logical Architecture

3.3.5.3 Interfaces

Table 3.6 : UDC Interfaces

Interface	UDC Component	Protocol	Description
S6a	HSS-FE – MME	Diameter	Used for generation and provision of user authentication, integrity and ciphering data and to update user location information.
PROV1	EDA – CAS	Cai3g (over SOAP)	Used for provisioning purposes.
Ud	CUDB – HSS-FE CUDB – EDA	LDAP	Used for retrieval, storing and modification of user data stored in CUDB.

3.3.5.4 Home Subscriber Server Front End (HSS-FE)

3.3.5.4.1 Concept

The Ericsson HSS-FE is a real-time Network Element (NE) residing in the core network and containing the subscription-related information to support authentication, authorization, and mobility management procedures in the IMS and EPC domain.

The HSS-FE adopts the concept of modularity, making it possible to handle user subscriptions in any combination of the previous domains. It is deployed as a Virtual Network Function (VNF).

The HSS-FE provides user management functions for EPS users as specified in 3GPP.

3.3.5.4.2 Components

Following brief description of HSS-FE module:

EPC Subscription Manager (ESM) implements the support of the LTE Evolved UMTS Terrestrial Radio Access (E-UTRAN) accesses and other Non-3GPP accesses in the context of 3GPP EPS specifications. ESM provides support for the subscription management, authentication, authorization, and mobility management for EPC.

The introduction of subscription-based 5G (NR) authorization and extended bit rates for subscribed Aggregate Maximum Bit Rate (AMBR) in the ESM enables 5G evolution in EPC.

The following functions are included for enabling 5G EPC support in HSS-FE:

- **Subscription Based 5G (NR) authorization**

  An EPS subscriber can be enabled with 5G NR by setting the subscription type to eMBB.

  For 5G-enabled EPS subscribers, operators can further allow or disallow the 5G NR access by provisioning the ARD[1]. The NR as Secondary RAT Not Allowed bit in the ARD is used to notify the MME about the access restriction of the NR as secondary RAT. The capability of NR as Secondary RAT support is negotiated between the MME and the HSS using the NR as Secondary RAT bit in the supported feature list included in the ULR[2]/ULA[3] and IDR[4]/IDA[5] command pairs over S6a.

  If the MME does not support this feature, the HSS does not send (in ULA) or update (in IDR) the 5G NR ARD, that is, the NR as Secondary RAT Not Allowed bit is always set to a value of zero in the subscription data downloaded by the HSS. If it does, the 5G NR ARD is set according to the subscription type and the provisioned ARD.

- **Extended bit rates for subscribed AMBR**

  For 5G-enabled EPS subscribers the AMBR can be used to support 4G bps to allow full bandwidth utilization. The HSS signals to the MME on the allowed UE-AMBR and APN-AMBR, using extended S6a messages.

  The original Max-Requested-Bandwidth-UL and Max-Requested-Bandwidth-DL AVPs encode the bandwidth value in bits per second, having an upper limit of 4294967295 bits per second.

[1] Access Restriction Data

[2] Update-Location-Request

[3] Update-Location-Answer

[4] Insert-Subscriber-Data-Request

[5] Insert-Subscriber-Data-Answer

The Extended-Max-Requested-BW-UL and Extended-Max-Requested-BW-DL AVPs encode the bandwidth value in kilobits per second, having an upper limit of 4294967295 kilobits per second.

Authentication Vector Generator (AVG) - The AVG module hosts the user-related authentication data needed to generate the authentication vectors used for the following types of authentication:

- EPS-AKA[6]: The AVs[7] are requested by the ESM module when the user accesses a USIM UICC.
- EAP-AKA (non-trusted, non-3GPP networks) and EAP-AKA' (trusted non-3GPP networks) in EPS: The AVs are requested by the ESM module when the user accesses a USIM UICC
- GBA-AKA: The AVs are requested by the SDA module when the user accesses either USIM or ISIM applications in the UICC.

3.3.5.4.3 HSS-FE VNF Internal Architecture

The HSS-FE VNF (Figure 3.15) is composed of multiple Virtual Machines (VMs), where each VM takes one of the following roles:

- System Controller (SC)
  - Two SCs work in an active-standby fashion.
  - They are used to control and manage the HSS-FE VNF.
  - They receive and handle incoming O&M traffic.
  - They provide the HSS-FE VNF with a common file system with high availability.
- Pay Load (PL)
  - They handle the incoming network traffic in a load-sharing fashion.
  - Their number is chosen to provide the desired traffic handling capacity (n) and redundancy at node level (k)

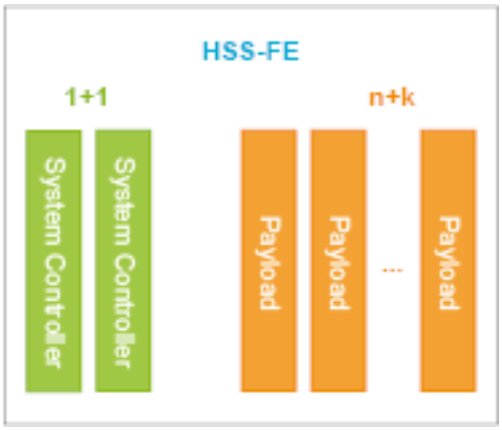


Figure 3.15 : SC and PL VMs Comprising the HSS-FE VNF

In this 5G-VINNI project, the vHSS-FE will be deployed with the minimum configuration, each vHSS-FE VNF consisting of 2 x SC VMs and 2 x PL VMs (2+2).

3.3.5.4.4 Deployment

The deployment of the HSS-FE in layered architecture is illustrated in Figure 3.16.

[6] AKA; Authentication and Key Agreement protocol

[7] Authentication Vector

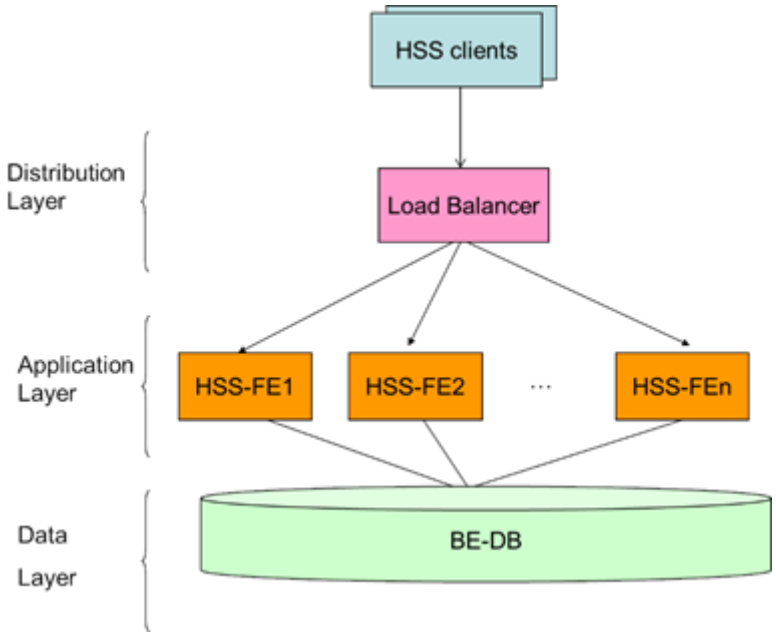


Figure 3.16 : Example of HSS-FE Configuration

The protocol used for accessing the external database is LDAPv3. Consequently, the external database needs to be defined as a directory server implementing a given object class data model tree.

As many FEs as needed can be used to provide the desired traffic handling capacity and redundancy at network level.

3.3.5.4.5 Provisioning

The operator provisioning system is provided with two components:

- A validation component to check the consistency of provisioned subscription profile data (for example, semantic and syntax checking) before storage in the BE-DB.
- A notification component supporting the logic of the notification mechanism for immediate detection of changes in provisioned data, affecting ongoing session information in the control layer.

The validation and notification components are external software. They are required for ordering the validation or notification mechanisms. They are used by the triggering entity (the provisioning system) to request the validation or immediate execution of specific provisioning orders along with the modification of subscription profile data.

3.3.5.5 Centralized User Database (CUDB)

3.3.5.5.1 Concept

CUDB is the component in UDC used for user data storage in centralization scenarios.

CUDB is a telecom-grade database, implying the following properties:

- Single logical database
- Real-time database with low access latency
- High storage capacity
- High throughput
- Geographically redundant: Double 1+1 user data (geographical) replication
- Exposed using Lightweight Directory Access Protocol (LDAP) (3GPP Ud interface)

- Notification support. CUDB supports outbound notifications, so whenever data is modified in a user profile, the CUDB can send Simple Object Access Protocol (SOAP) based notifications to the corresponding application FE
- Application counters framework allows applications to create custom sets of counters about application data stored in CUDB

CUDB provides local single logical point of access at network level.

CUDB is a system, made up of a set of CUDB nodes. Each of the CUDB nodes provides an LDAPv3 compliant Single Point of Access (SPoA) to all LDAP clients.

Each CUDB node provides access to the whole subscriber base, regardless of its distribution across CUDB nodes. it hides the CUDB internal data distribution, storage and redundancy to Application FEs and EDA.

3.3.5.5.2 Components

Each CUDB comprises of

- **Processing Layer:** LDAP Front End: Servers that make protocol conversions and can locate any subscriber data info across the distributed CUDB by accessing the Partition Layer.
- **O&M Systems:** Additional systems deployed to meet O&M related tasks such as Backup System, management web servers, import and export clients and monitoring tools.
- **Partitioning Layer Unit:** A set of Data Clusters storing the location of every subscriber in the Data Storage Units. These clusters are geographically replicated in all CUDB nodes forming the PL Group.
- **Data Storage Units:** A set of independent Data Clusters (one or more) storing different partitions of the entire subscriber data set. Each one of these clusters is geographically replicated in other remote CUDB nodes, forming a DS Unit Group.

3.3.6 Provisioning GW

3.3.6.1 Concept

The Provisioning GW (EDA) is the functional component in UDC, which makes it possible to terminate the provisioning protocol, control the validation of the provisioning requests, write the data into the BE database, and to handle massive operations.

The EDA provides UDC with a single point of provisioning. Once it receives a provisioning request from the customer information and administration system, it orchestrates the provisioning and the subsequent validation logic, triggers the network notifications, and distributes the provisioning load.

3.3.6.2 Components

The main functions are the following:

Data Model Management

EDA provides a higher abstraction provisioning interface and works as a mediator. It also enables the User Data Consolidation by managing the life cycle of the user data hosted by the CUDB. The business logic ensures that user data is provisioned correctly. The Customer Administration System (CAS) sees a simple information model, while it is protected from changes in the database implementation. EDA/PG handles the translation of information model to data model. The following aspects are covered:

- Mapping of the Customer Administration System (CAS) order to the LDAP objects in the data model for a user.
- Checking and adding default values to attributes that are required (mandatory) in CUDB.

- Handling of identities and aliases under root identity entries, generate identities, and validate their relations for a given user.

Single Point of Provisioning

EDA receives the incoming requests from the administration system and executes the correct logic depending on the request.

Validation of Provisioned Data

The data is not written to CUDB unless it is validated, for example, by checking the service dependencies. The validation is application-specific and depends on the type of data provisioned; it can be either hosted on EDA, or delegated, that is, distributed to the application.

The following validation mechanisms are use:

- Syntax validation

  Assurance of syntax correctness of provisioning requests (for example, that mandatory parameters are present).

- Semantic validation

  Data range validation including service restrictions.

- Induced data analysis

  Some provisioning requests have implications on other user data. For example, activating one service can temporarily deactivate other services.

Notification of Data Updates

After the successful completion of an activation request, the application FE can have the need to be notified that the data has been added, modified or deleted. Triggering of network notifications depends on the type of data provisioned.

Massive Provisioning

Massive provisioning is a solution function, enabling the capability for managing user data for large number of users that fulfils certain criteria of a single order. It also enables the request of common subscriber data. This type of data is not connected to a particular user, such as General Packet Radio Services (GPRS) or Customized Applications for Mobile Networks Enhanced Logic (CAMEL) profiles.

Access Control

EDA allows the definition of different administration domains, and further configuration of each domain with a number of access rules, to support secure and safe provisioning in a multi-region context. In this way, it is possible to grant provisioning rights to administrators on a per-region or per-tenant basis. This is to limit the ability of an administrator to initiate provisioning operations to a subset of users in another administration domain.

3.3.6.3 Networks

The network infrastructure for Dynamic Activation in a virtual and cloud environment resides on three networks: Internal, Operation & Maintenance (O&M) and Provisioning traffic.

To establish communication between the Virtual Machine (VM) and the IP backbone, either two or three virtual networks must be defined (depending on if separate traffic network is used) and connected to the host.

The OpenStack administrator must create the following provider networks before vEDA deployment:

- External Provisioning Network

- External OAM Network

Cluster internal networks include the following:

- Provisioning network address range
- Management (O&M) network address range
- Internal network address range

All cluster internal network address ranges use Private IP Addresses and can be configured when deploying infrastructure.

3.3.6.3.1 External Physical Connectivity

With traffic separation: Two separate networks (OAM and Provisioning Traffic) are used for external traffic as illustrated in Figure 3.17.

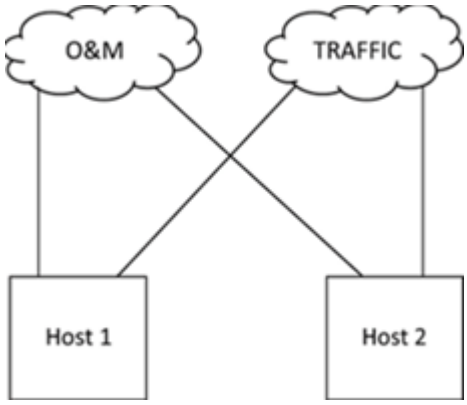


Figure 3.17 : Dynamic Activation Connectivity Overview with Traffic Separation

3.3.6.3.2 IP Allocation for Cloud Deployments

The principle for node IP addressing in a cloud deployment is the same as in a virtualized deployment but addresses are allocated dynamically using DHCP.

3.3.6.3.3 IP Allocation for OpenStack Deployment

In OpenStack vEDA deployment, the "floating IP" concept is used. The floating IP consist of a pool of IP addresses, that are public routed IPs that you typically get from an ISP. Floating IPs are assigned to the instances, thus making them reachable from the outside world.

During vEDA deployment, node-1 and node-2 gets floating Management (O&M) and floating Provisioning (if traffic separation is used) IP addresses. Also, VIP address, Management (O&M), and Provisioning (if traffic separation is used) gets a floating IP connected to the vEDA cluster.

Cluster internal networks include Provisioning network address range, Management (O&M) network address range, and internal network address range. They are configured when deploying the infrastructure. All cluster internal network address ranges use Private IP Addresses and can be configured when deploying infrastructure.

DHCP is used for assigning IP address during vEDA deployment.

As a minimum, one NTP and one DNS must be available and configured when deploying vEDA. NTP IP address and DNS IP address must not be part of internal provisioning network address range or internal management network address range.

The deployment will be done in OpenStack in the setup uwint OpenStack IPv4 with traffic separation.

3.3.6.4 Load Balancing

The load balancing functionality is divided between the Keepalived and HAProxy solutions. Virtual IP is handled by the Keepalived solution, and load balancing is handled by the HAProxy solution.

3.3.6.5 Provisioning Workflows

3.3.6.5.1 Provisioning EPS Services

A simplified and general flow for the provisioning of EPS Services is shown in Figure 3.18.

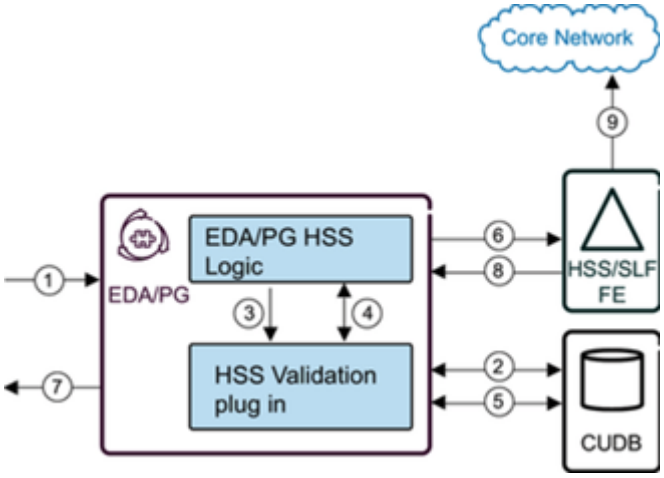


Figure 3.18 : General HSS Provisioning Flow

The provisioning flow for EPS is as follows:

1) A provisioning request is received, and its syntax is validated.
2) The EDA fetches the user data from CUDB.
3) The EDA merges the received data in the provisioning order with the data fetched from the CUDB, and sends it to the HSS validator plug-in.
4) The HSS validator plug-in validates the user data and sends the result to EDA. This data is called mutation data.

Note: Step 3 and Step 4 are performed for create and set provisioning orders.

5) The EDA compiles the provisioning order data, the CUDB data, and the possible mutation data resulting from the validation performed by the HSS validator plug-in. The add, delete, and modify operations are performed on the CUDB for the mentioned data.
6) A notification of changed data is sent to the HSS Front End, if required.
7) A response to the provisioning order is sent back to the originating system.
8) A notification response is received from the HSS Front End if a notification has been sent. Since the communication is asynchronous, the response can come before the CAI3G response in Step 7 or not.
9) HSS Front End notifies the Core Network on the provisioning updates.

Note: HSS subscription data contains references to profile data that is stored in HSS Front End. The existence of the referred profile is not checked by EDA at the time of provisioning since the HSS Front End configuration is not known to EDA. Also, deletion of a profile that is referred to by a subscription is allowed by HSS Front End. If subscription with non-existing profile is found by HSS Front End during relevant traffic operation, HSS Front End will raise an alarm and use a predefined default profile for that subscriber. For detailed description of this functionality refer to HSS Automatic Detection of Profile Inconsistencies.

10) Through the CAI3G provisioning interface, create, set, delete, and get provisioning orders can be performed for the following HSS functions:
    - Authentication Vector Generation (AVG)
    - EPS Subscription Manager Module (ESM)

3.3.7 VNF EMS - Element Management System

Ericsson Network Manager (ENM) is the Element Manager managing Ericsson VNF's.

ENM provides centralized operation and maintenance of radio and core.

It provides unified performance and configuration management, software, hardware and fault management, together with security, self-monitoring and system administration for the ENM.

The vENM (virtual ENM) used in 5G-VINNI is a virtualized ENM.

3.3.7.1 vENM Software Architecture

ENM on Cloud is deployed using a concept of application stacks/ VM types. Each application stack/VM type is composed of a set of VMs which comprise a given application. The installation, upgrade and lifecycle management of the applications is handled using VNF-LCM which is the co-deployed Ericsson S-VNFM.

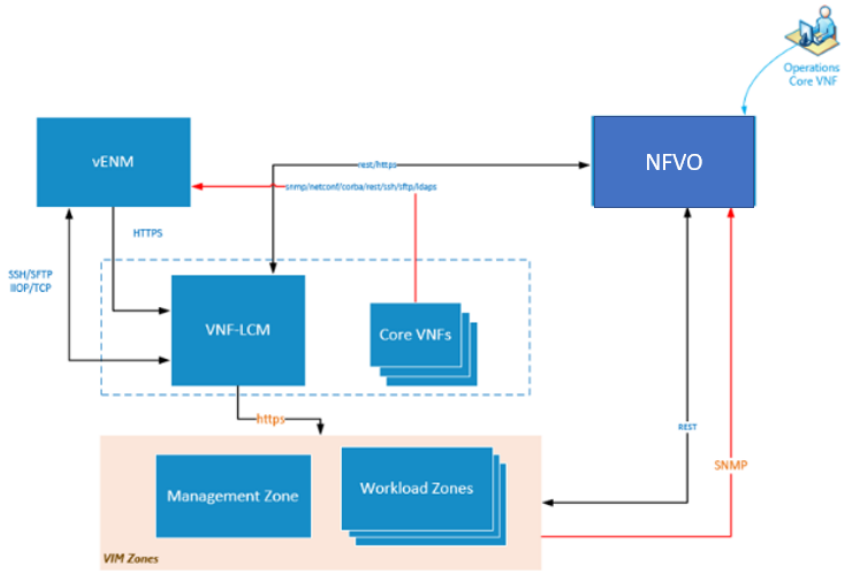


Figure 3.19 : Virtual ENM Architecture Overview

3.3.7.2 ENM - Core Network Base Package

Within the Core Network Package there are common functionality components, which are technology independent and allow operators to perform routine tasks for basic network management. This includes following functions:

- Topology Management
- Fault Management
- Performance Management
- Configuration Management
- Software and Hardware Management
- Security Management
- System Administration
- Network Health Monitor

- Node Health Check
- Release Independence

3.3.7.3 Virtual ENM application architecture

The ENM software architecture is a modular service-oriented architecture (SOA) with strong focus on separation of business logic and mediation by means of layering.

ENM is model-driven, meaning that the contribution of models can be used to influence ENM functionality, easily extendable through SDK.

vENM is built on cloud Infrastructure. vENM deployment can be automated with High Availability.

3.3.7.4 Virtual Machines Roles

Figure 3.20 presents the service grouping of virtual ENM deployment.

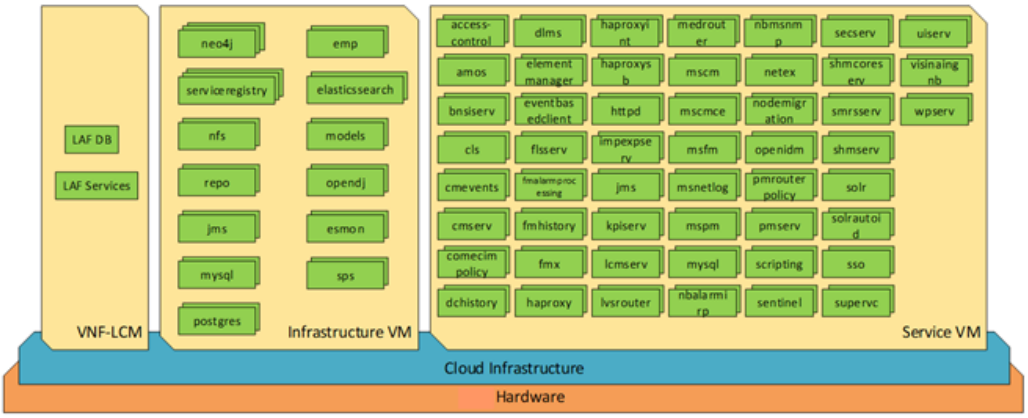


Figure 3.20 : Service VM overview on vENM

3.3.7.5 General Applications

ENM is comprised of a suite of different management applications supporting the various elements associated with FCAPS management. ENM also contains more advanced management applications, focusing on Automation. Applications are controlled by human interfaces (GUI and CLI) or machine interfaces, this varies from application to application. **High Availability and Fault Tolerance** - This ensures that failures in software processes, whether controlled or not, are sustained and not of consequence to operations.

Horizontal Scaling - This is the ability to scale-up or scale down the capability of the ENM system, by choosing different deployment variants (the software components that are needed and the number of software components that are needed).

3.3.7.6 Network Design

3.3.7.6.1 VLAN Layout

Comparing to physical ENM deployment, vENM only needs two VLANs. All ENM VMs are connected to the internal VLAN. Only VMs that require direct external access are connected to the public VLAN. The following VLANs are required:

- **ENM Internal VLAN**

  Each VM within ENM will need an address on the internal VLAN. The internal VLAN is used for network communication between different service VMs. The internal VLAN does not need external routing so private IP addresses can be used.

- **ENM External VLAN**

  There are some service VMs that need public external IP addresses to communicate with NE nodes, ECM, northbound OSS systems and end user. Public IP addresses shall be used. For services which need external VLAN addresses, please check details in [6.2].

3.3.7.6.2 Physical Connectivity

Physical connectivity towards Leafs from the computes of vENM is using the same resilience techniques within the fabric. The compute will be configured with Linux Bonded (passive LAG) interfaces for data and storage whilst the Leafs will have Active/Active MC-LAGs.

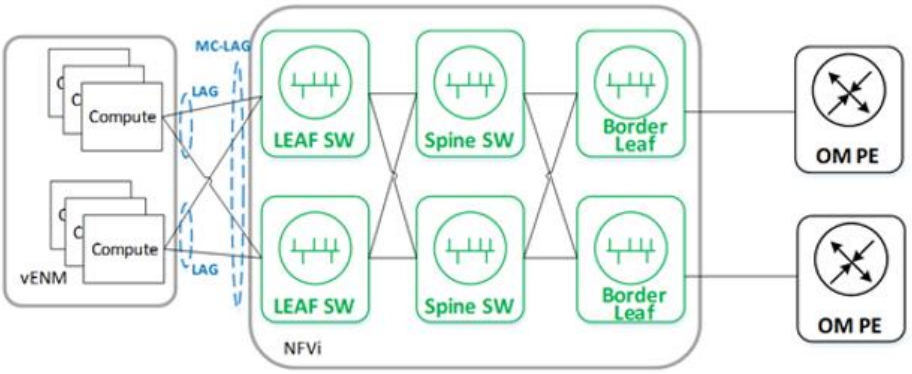


Figure 3.21 : vENM Physical connectivity in Vinni NFVI network

3.3.7.6.3 Logical Connectivity

Lvs routers are located on 2 VM instances of vENM and act as external interface of vENM. All the vENM traffic will pass through Lvs routers to external network.

vENM will use vENM_external vlan to connect a pair of vRouter located in NFVI layer. And the vRouter will use an existing L3 link to connect the OM PE.

vENM will use the VRRP in an Active/Passive configuration on the vRouter in NFVI for OMtraffic.

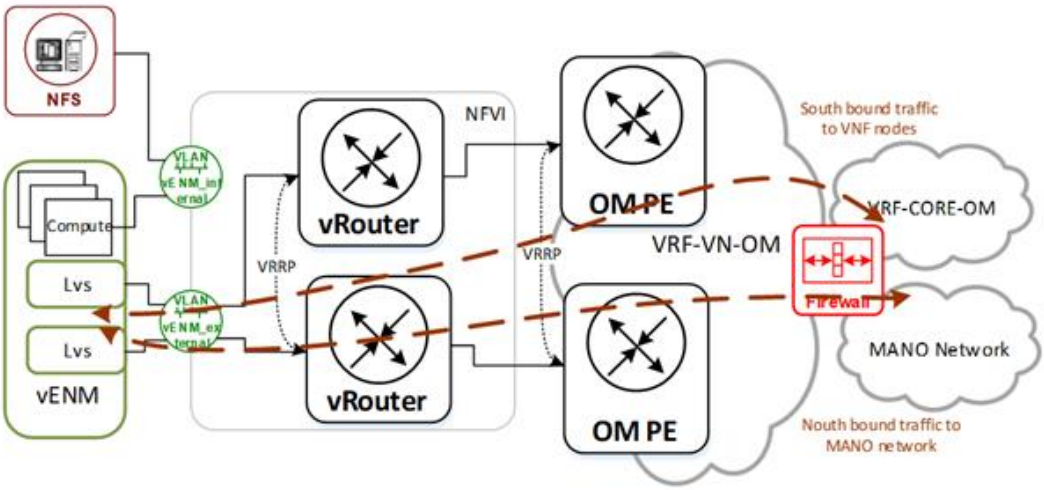


Figure 3.22 : vENM Logical connectivity

3.4 5G Core

This section briefly describes 5G SA core (5GC) Containerized Network Functions (CNFs) and how they are integrated with the Nokia NFVI.

5GC Ericsson products are delivered and executed as a set of containers and designed to run on a Kubernetes container orchestration platform (CaaS).

A Container-as-a-Service (CaaS) layer will be deployed as a set of VMs on top of Nokia cloud infrastructure (NCIR) and will facilitate two SA network slices with a combination of independent NFs per slice (AMF, SMF, UPF) and shared NFs (UDM, UDR, AUSF, NRF, NSSF).

An overview of the deployed 5GC solution can be seen in Figure 3.23.

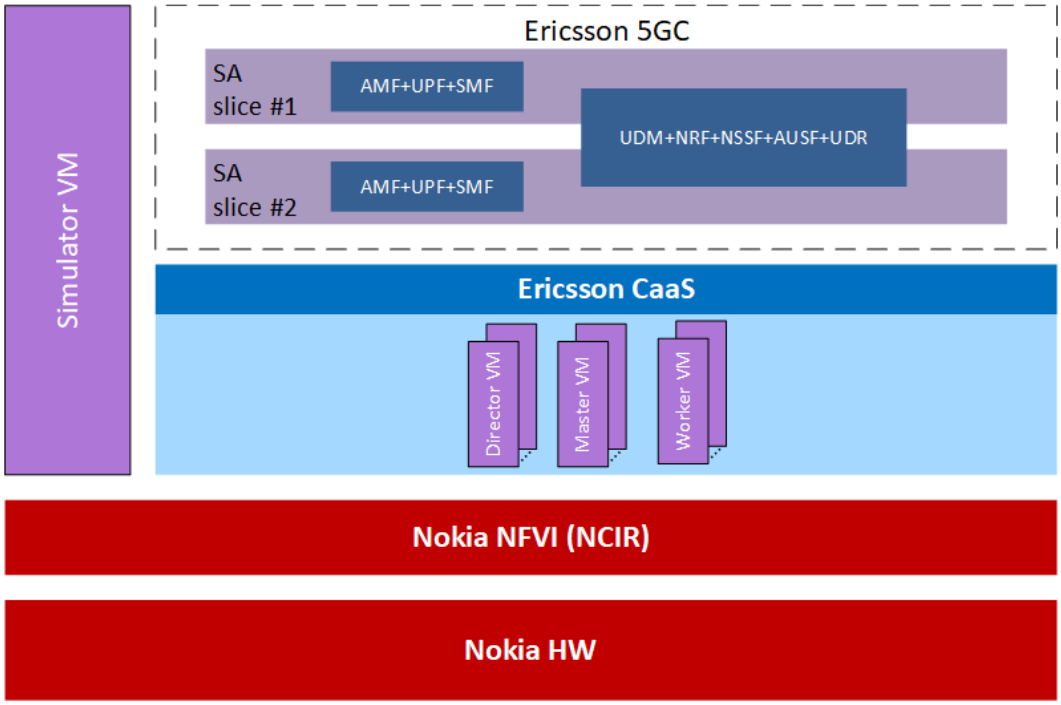


Figure 3.23 : Ericsson 5GC deployment overview for 5G-VINNI.

Note that these two 5GC (SA) slices are depicted in the context of overall facility architecture in Section 2 and especially Figure 2.1.

3.4.1 Container-as-a-Service (CaaS)

3.4.1.1 Concepts

Ericsson CaaS platform provides container orchestration and management based on Kubernetes and other open source components, adding components for ingress, networking, storage, and monitoring among other capabilities. It serves as a generic execution environment for container-based workloads including cloud-native telecom network functions.

In 5G-VINNI CaaS layer is deployed as an application on NCIR with centralized (Cinder) storage, using the image-based deployment option and acting as a CaaS layer for 5GC CNFs.

3.4.1.2 Components

Each CaaS VM-based cluster can be composed of at least one each of Director, Master and Worker VMs.

In 5G-VINNI two CaaS clusters will be deployed (from now on referred to as CaaS-1 and CaaS-2) with each cluster composed of:

- 1 Director VM
- 1 Master VM
- Worker VMs

Details of hardware resource consumption are detailed in Section 5.4.10.

3.4.1.3 Networking

There are several types of basic networks used by Ericsson CaaS clusters:

- **Internal network** – used to interconnect the CaaS cluster VMs, L2 only (tenant network)
- **OAM network** – used to access the Director VM for CaaS cluster management purposes (provider network)
- **Traffic network** – used to carry application (CNF) packets (provider network)
- **DC network** – used to carry application (CNF) packets (provider network)

Note: DC network is only needed in the CaaS-1 cluster

In addition, the CNFs will use additional IP addresses that are used to address the various applications. These can be considered virtual IPs, and requests to/from these addresses are always carried over CaaS external Traffic and OAM networks.

CaaS-1 cluster will be part of the Exposed zone, and CaaS-2 cluster will be part of Non-Exposed zone.

An overview of SA core external connectivity can be seen in Figure 3.24.

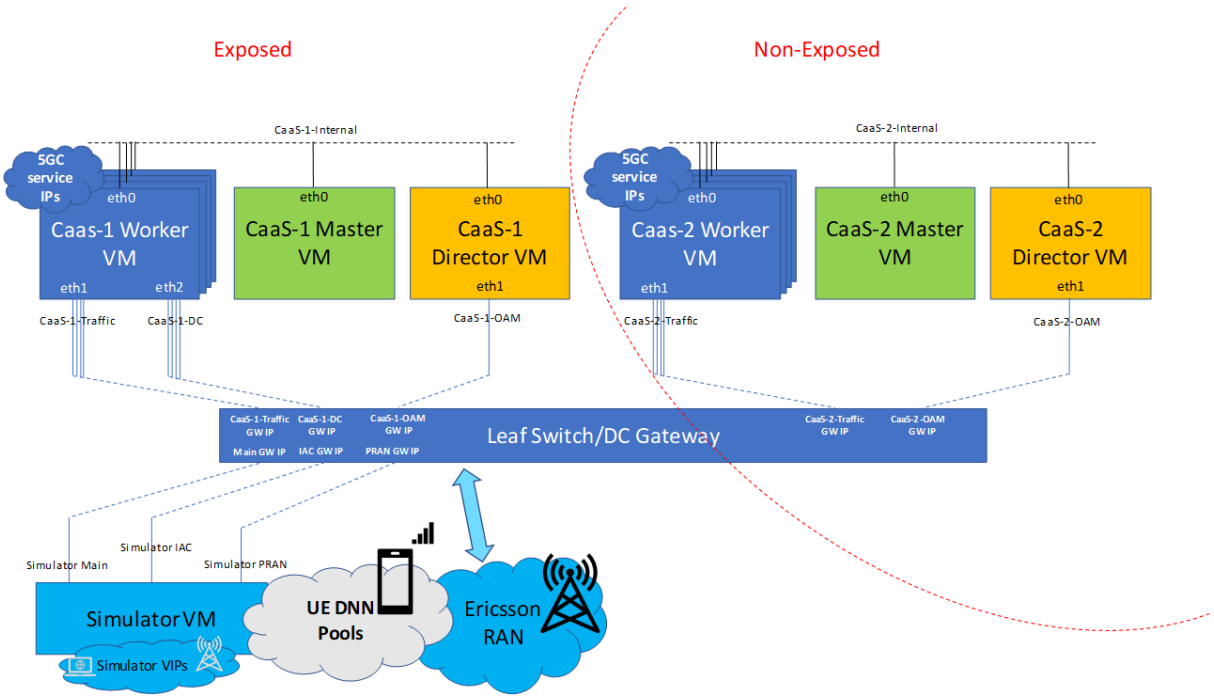


Figure 3.24 : 5GC core external networking interfaces

3.4.1.4 IP Connectivity and Routing

Depending on the type of network and CNF, several main routing approaches are employed:

- CaaS-2 OAM network makes use of static routing
- BFD + static routes with ECMP are used by CNFs in the CaaS-2 cluster, via the Traffic network interface

- Either BFD + static routes with ECMP or BGP is used by the CNFs in the CaaS-1 cluster, via Traffic or DC network interfaces – both depending on specific application

3.4.2 Ericsson 5G SA CNFs

Ericsson's 5G Core solution is based on cloud native principles, with software architecture based on microservice technology and Containerized Network Functions (CNFs).

A fundamental principle of a CNA is to decompose software into smaller more manageable pieces (independent functional software modules). This is usually done through utilizing a microservice architecture. Some of these modules are generic and re-used across several Cloud Native applications while other modules are application specific. A **Microservice** is a software module that is designed, developed and maintained as a separate component.

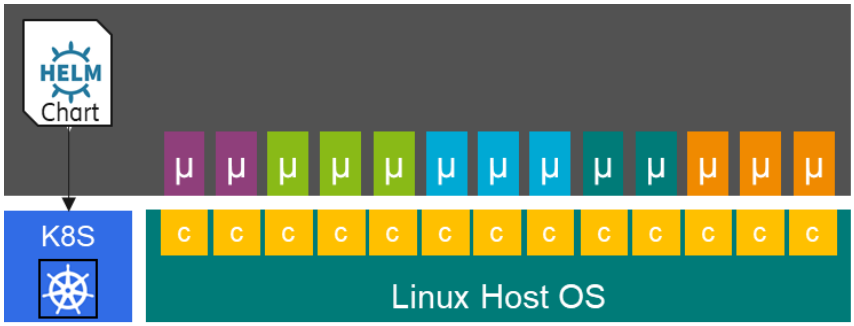


Figure 3.25 : Micro-Service Architecture

3.4.2.1 Components

In the scope of 5G-VINNI Norway facility 5G SA core solution, the following 3GPP network functions are deployed:

- **Access and Mobility Management Function (AMF)**
- **Session Management Function (SMF)**
- **User Plane Function (UPF)**
- **Unified Data Management (UDM)**
- **Unified Data Repository (UDR)**
- **Authentication Server Function (AUSF)**
- **Network Repository Function (NRF)**
- **Network Slice Selection Function (NSSF)**

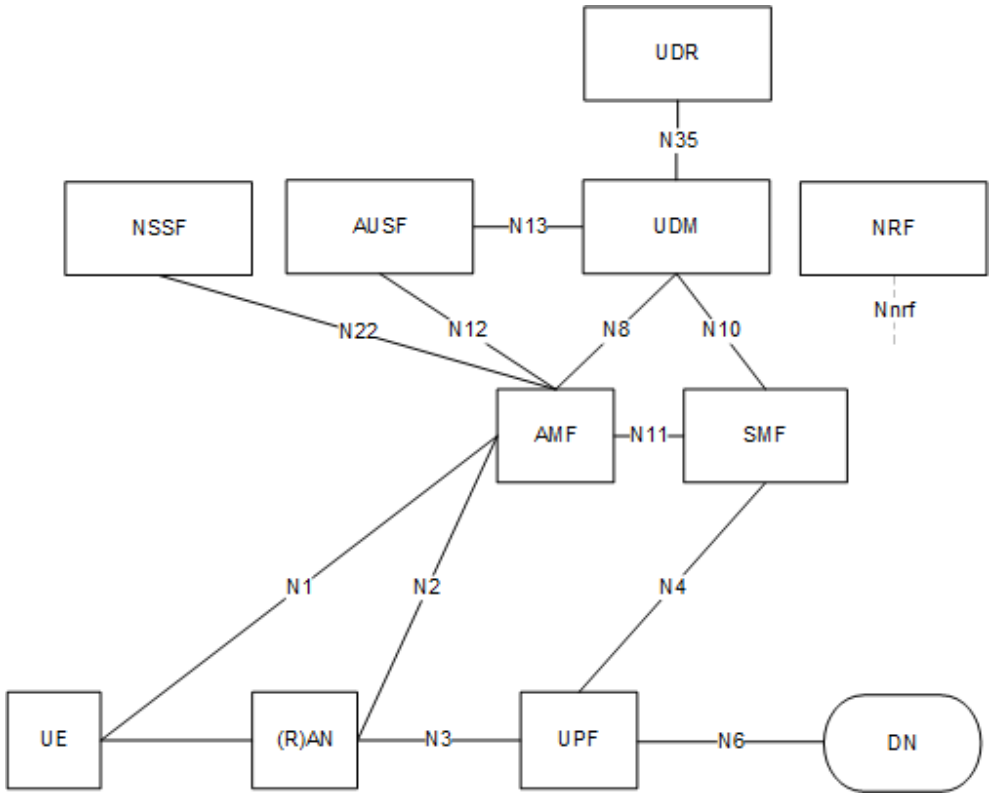


Figure 3.26 : Reference-point representation of the 5GC solution deployed in 5G-VINNI Norway facility

Note that NRF Nnrf interface is left unconnected in this diagram for simplicity, whereas in reality it is used by most 5GC NFs for NF discovery purposes.

More information on the above 3GPP functions can be found in 3GPP TS 23.501 chapter 6.2, and information on 5G core architectural guidelines in 5G-VINNI can be found in D1.1 chapters 3.1 and 4.3.2, D1.4 chapter 4.3.1.

3.4.3 Simulator

An Ericsson simulation tool will also be deployed, in this case used to simulate 5G UEs, 5G radio and data network, and used to run basic use-cases. It will be deployed as a single VM on top of NCIR to allow basic 5GC functionality testing and validation after system deployment.

3.4.3.1 Networking and routing

As illustrated in Figure 3.2, there are three basic networks used by the simulator VM:

- **Main network** – used for OAM and signalling (e.g. N2)
- **PRAN network** – used for access network user-plane (e.g. N3)
- **IAC network** – used for data-network user-plane (e.g. N6)

Static routing is used on all interfaces.

3.5 IMS (IP Multimedia Subsystem)

IMS is introduced to support Voice services for customers in 5G-VINNI. The primary customer at this point in time is the Military/Defense, which is a partner in the 5G-VINNI ESB. The IMS solution is delivered by Metaswitch. The IMS implementation in 5G-VINNI today is target to support the Defense use case of having autonomous edges, i.e. if the link to the Edge site goes down the Edge

should be able to provide the required mobile services for the users in the area connected to that Edge site.

Requirements for the IMS implementation;

- Military use case has Core and Edge sites – a few Core sites, and 10s of Edge sites
- Subscribers can attach to the network in any Edge site
- Subscribers need to be able to call anyone in any Edge site
- Need the ability to still be able to make calls when Core site has failed – between subscribers registered in Edge
- Supplementary services not required when Core failed, only basic 2-way calls.

EPC will use the CUPS model – or 5GC equivalent

- In normal state only user plane components are active in the Edge, with control plane in Core.
- On failure, load balancer will detect loss of contact to Core and re-route to control plane components in Edge.

EPC will notify UE of APN failure when contact with Core is lost.

- Following procedures in TS23.007 – sections 20.3.6 and 27.1
- UE will re-establish IMS APN on failure

3.5.1 Network Overview

There are two modes of operation proposed for the IMS implementation; the Active Edge and the Inactive Edge. In the Active Edge mode the voice service delivered to the customers is in normal operation served from the IMS functions that are running running in the Edge site(s). In the Inactive Edge the voice service delivered to the customers is in normal operation served by the IMS functions running in the Central site, but if the link goes down to the Edge it will be the IMS functions running in the Edge site that will serve the customers. There are pros and cons with both solutions. In the following we describe the implementation architecture for both solutions.

3.5.1.1 Active Edge

3.5.1.1.1 EPC/IMS

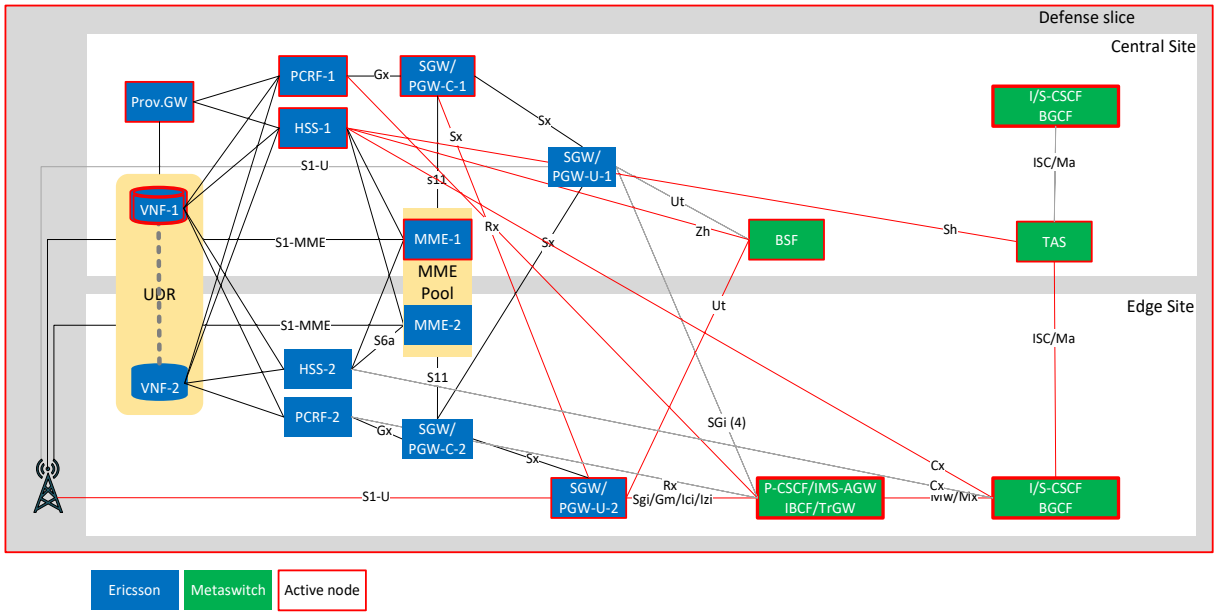


Figure 3.27 : IMS Active Edge architecture.

3.5.1.1.2 IMS

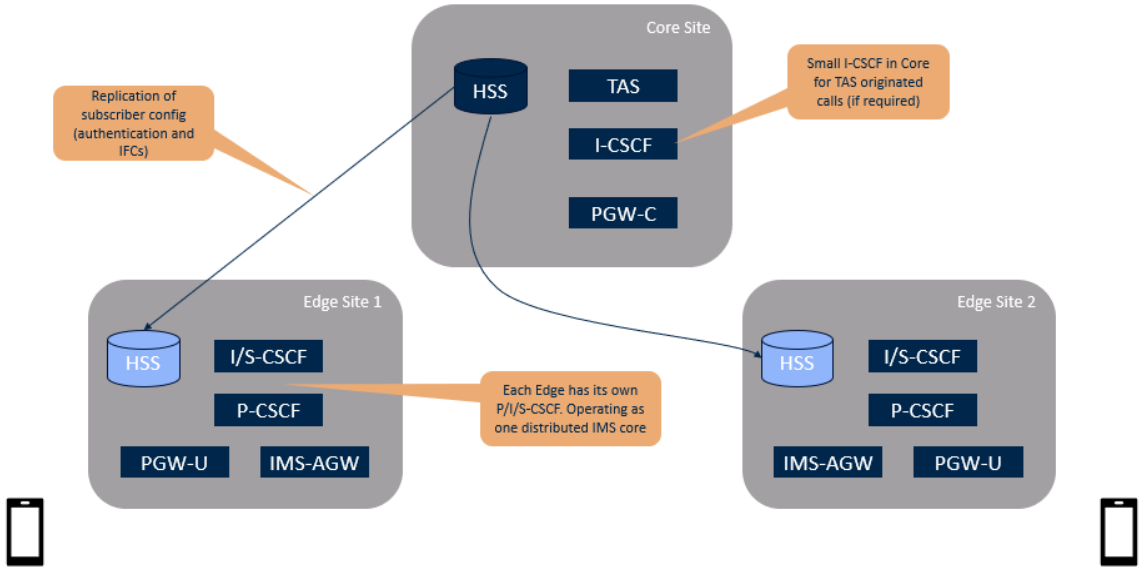


Figure 3.28 : IMS configuration in Active Edge mode.

3.5.1.1.3 Registration

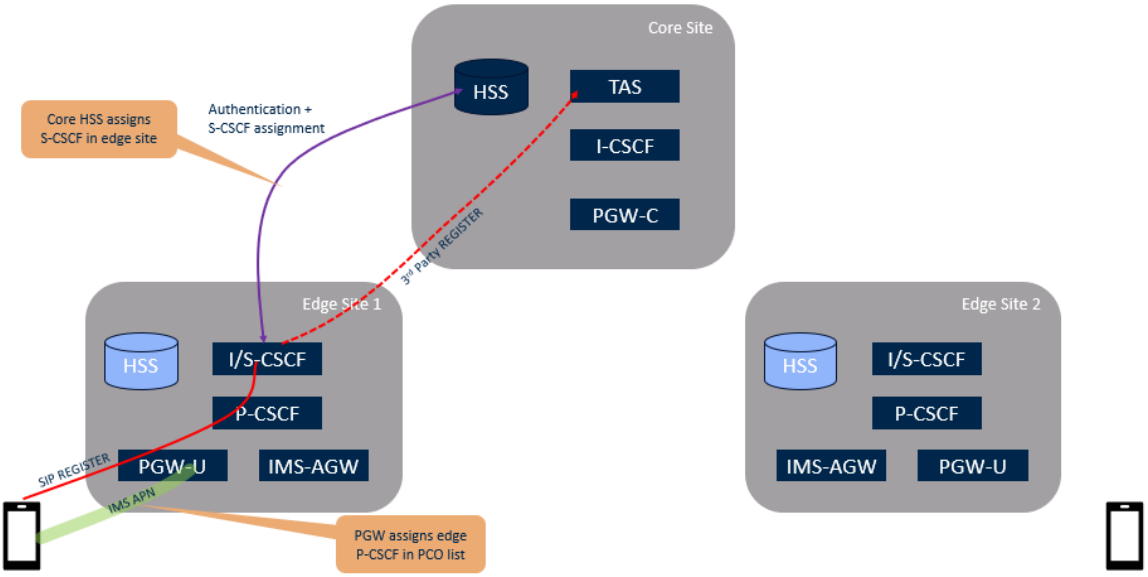


Figure 3.29 : IMS Registration in Active Edge mode.

3.5.1.1.4 Call Flow

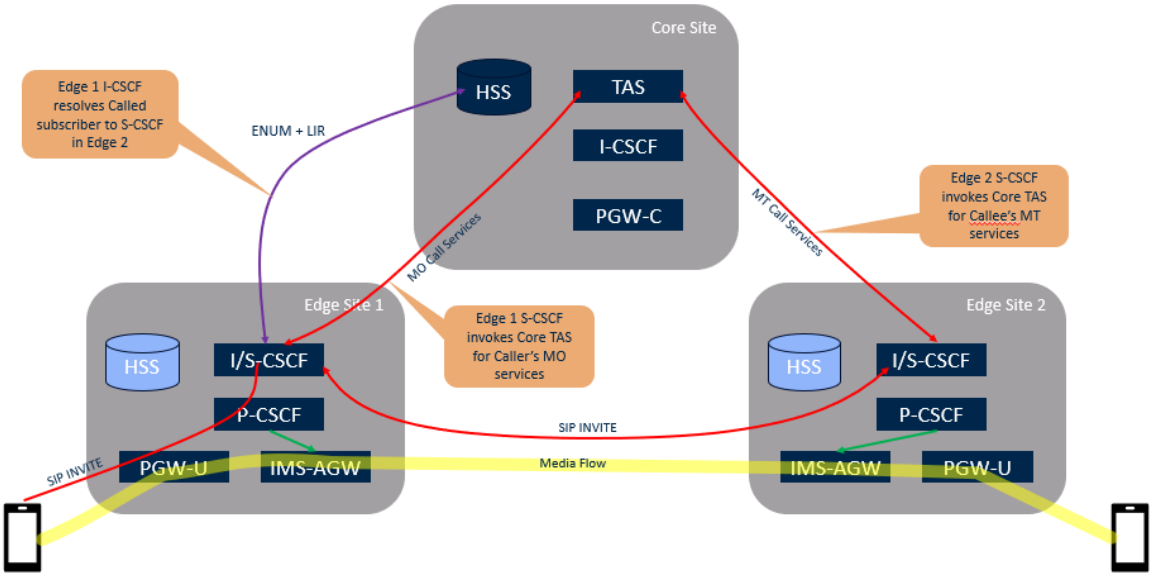


Figure 3.30 : IMS Call Flow in Active Edge mode.

3.5.1.1.5 Core Connectivity Failure

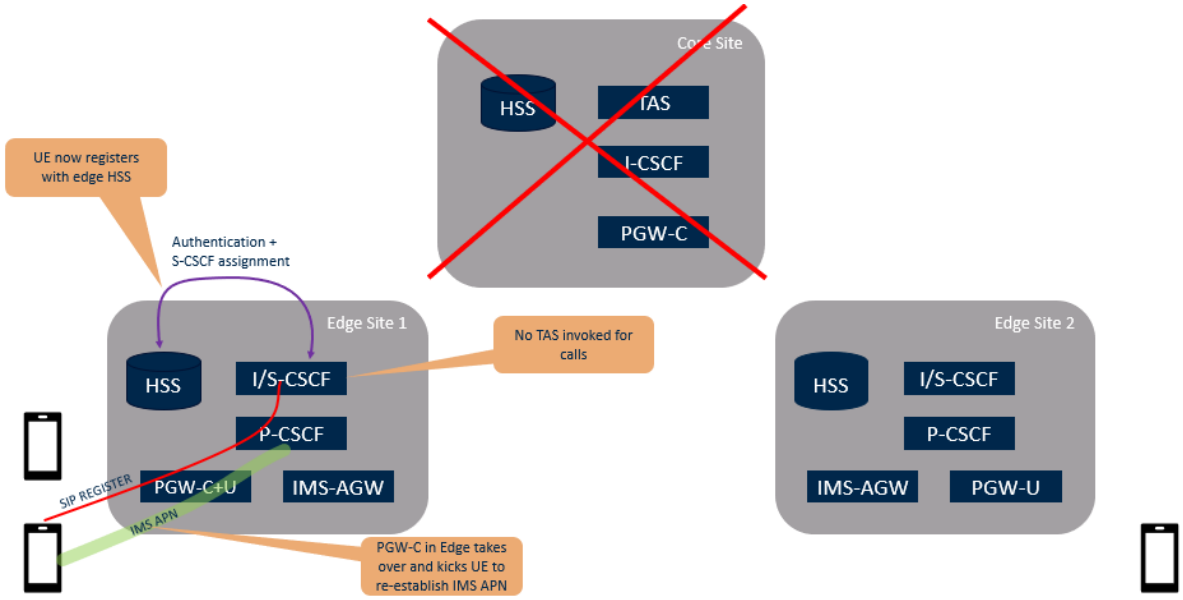


Figure 3.31 : IMS operation upon Core Connectivity failure in Active Edge mode.

3.5.1.2 Inactive Edge

3.5.1.2.1 EPC/IMS

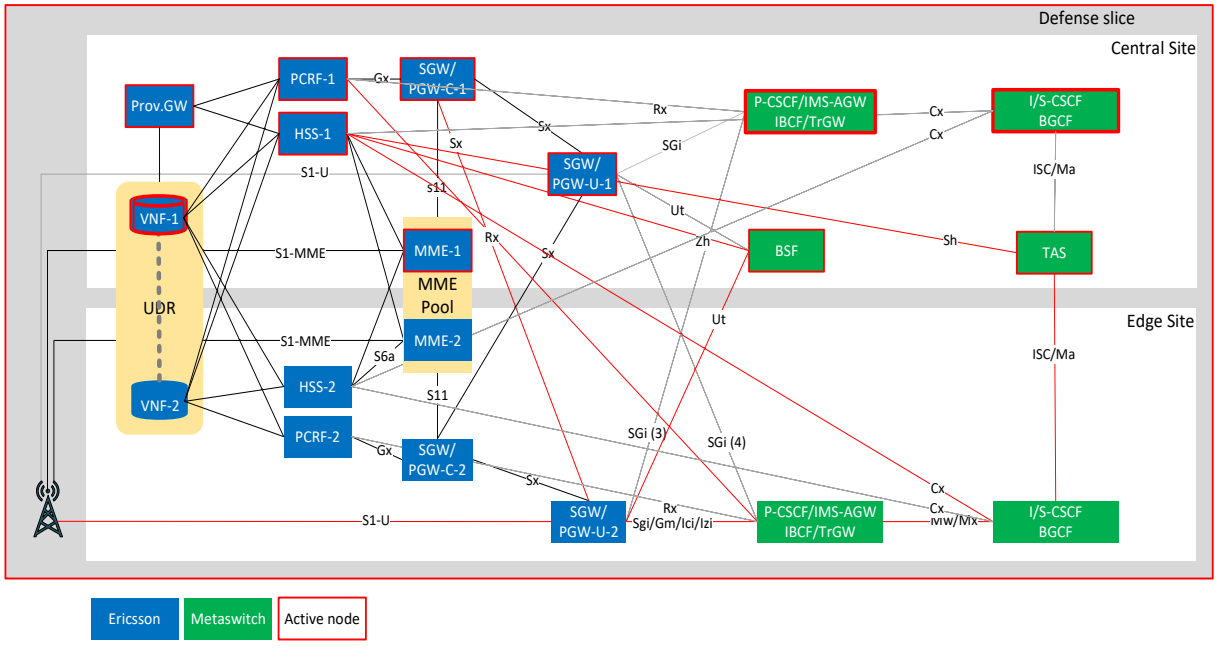


Figure 3.32 : IMS Inactive Edge architecture.

3.5.1.2.2 EPC/IMS Edge Failover

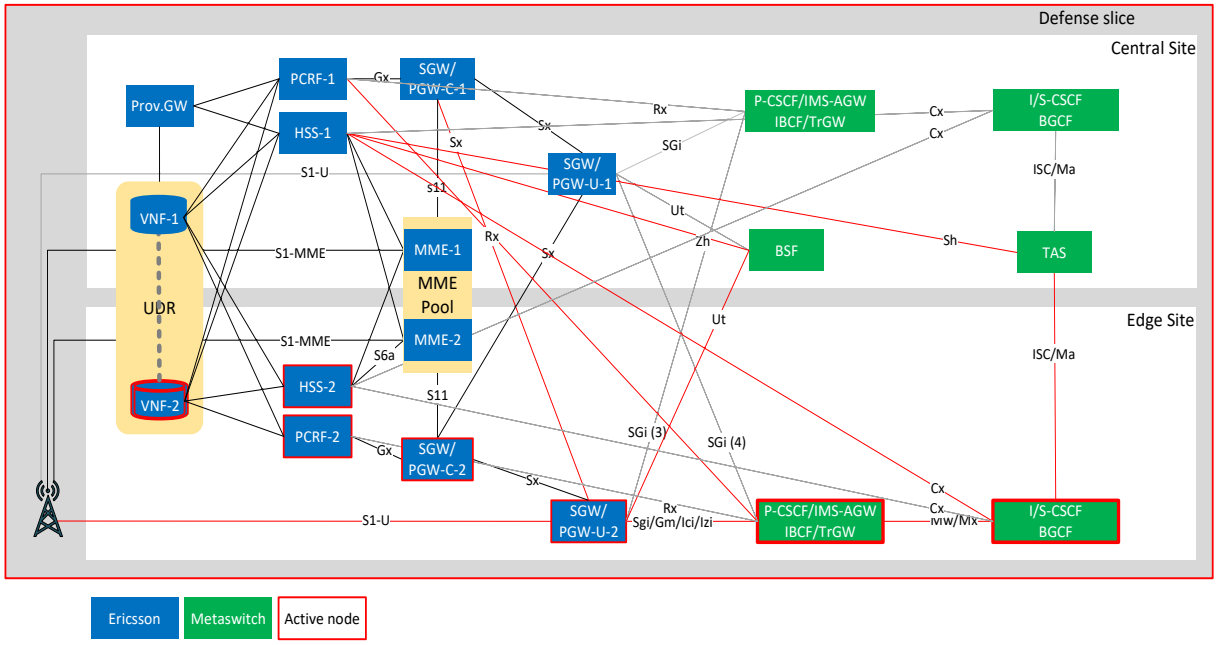


Figure 3.33 : IMS setup in Inactive Edge architecture in failover scenario.

3.5.1.2.3 IMS

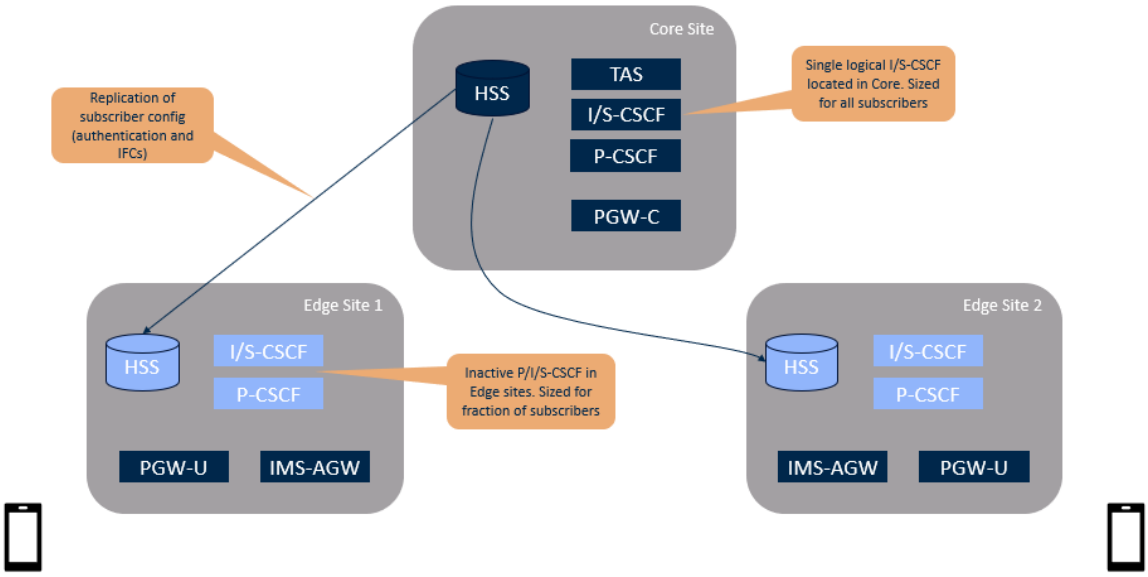


Figure 3.34 : IMS configuration in Inactive Edge mode.

3.5.1.2.4 Registration

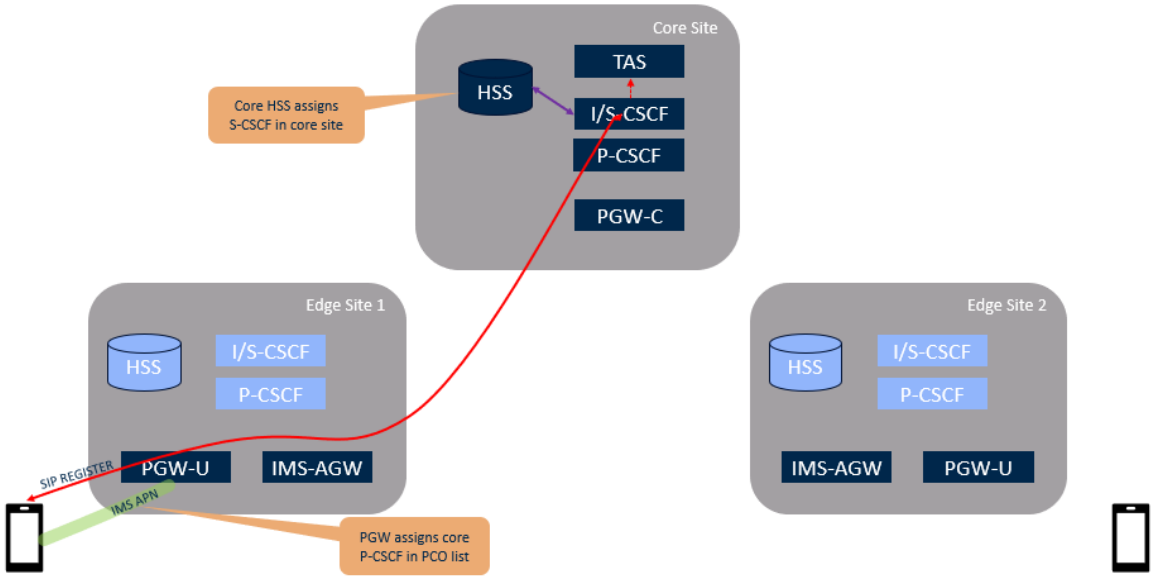


Figure 3.35 : IMS Registration in Inactive Edge mode.

3.5.1.2.5 Call Flow

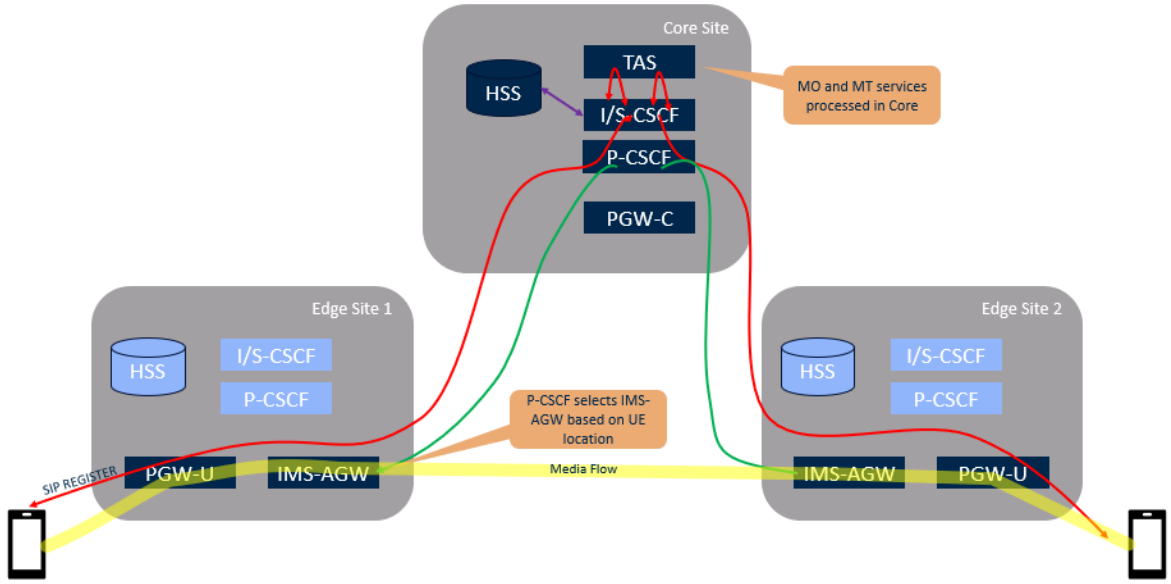


Figure 3.36 : IMS Call Flow in Inctive Edge mode

3.5.1.2.6 Core Connectivity Failure

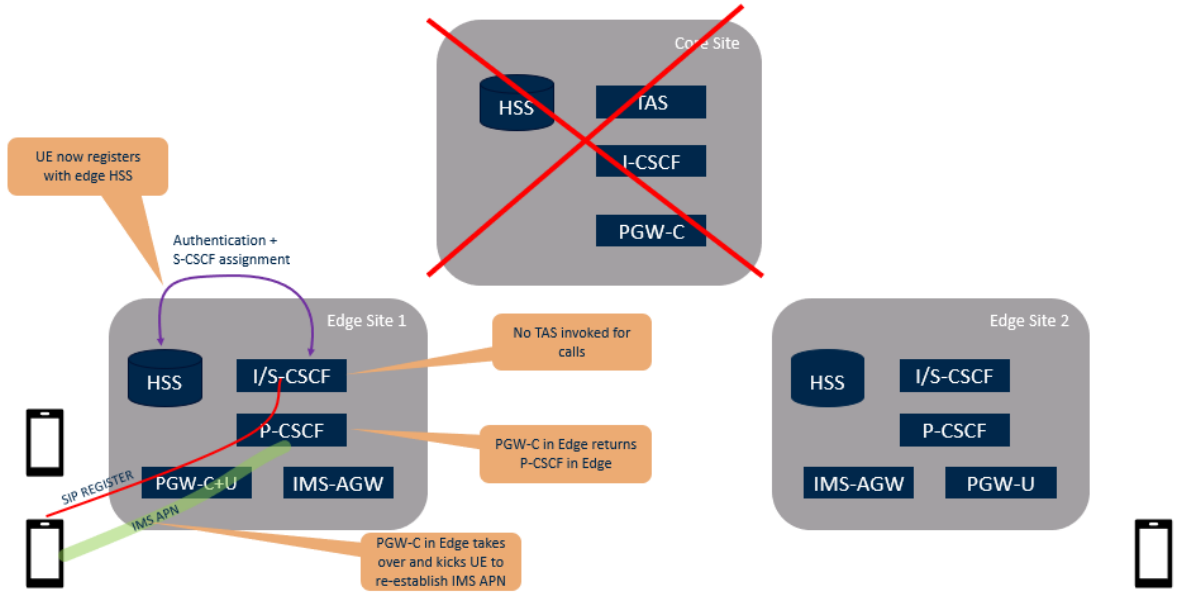


Figure 3.37 : IMS operation upon Core Connectivity failure in Inactive Edge mode.

3.5.2 IMS Components

3.5.2.1 Software Versions

The solution comprises the following component versions:

Table 3.7 : IMS Components software version

AMS:	V9.5.20-2
CFS:	V9.5.20-4
Clearwater Core:	V11.4.01-2-1
DCM:	V3.4.0-3
EAS:	V9.5.20-2
MAG:	V2.9.0-2
MDM:	V2.14.0
MMT:	V2.9.0-2
MRS:	V9.5.20-2
MVD:	V9.5.20-4
MVS:	V9.5.20-4
Perimeta:	V4.6.40-68
Radisys MRF:	V12.1.0.5-1.0
SAS:	V11.20.1
ShCM:	V2.9.0-2
SIMon:	V9.2.0

3.5.2.1.1 Accession Messaging Service (AMS)

The Accession Messaging Service (AMS) is used in an Accession Communicator deployment to provide Instant Messaging, Presence, file transfer, and SMS messaging on Accession Communicator. AMS also provides authentication of the Accession Communicator clients each time they log on to a network.

The Accession Messaging Service enables you to provide the following features on Accession Communicator. The feature set differs, depending on whether you have Business or Consumer users. You can choose whether or not to offer SMS messaging.

Features for Business users:

- Instant Messaging
  - From AMS V9.4.20 and Accession V2.27, chat messages are synchronized across all a subscriber's Accession devices, allowing subscribers with up to four Accession devices to see their full chat history with their contacts on all devices, and not just on the device they used to respond to the chat message. This includes any existing Accession clients that are currently offline - once the client reconnects, it will receive any outstanding chat messages.
- Presence
  - You can also choose to configure your deployment to show Presence information for non-Accession lines.
- File transfer
- SMS messaging

Features for Consumer users:

- File transfer

- SMS messaging

3.5.2.1.2 Call Feature Server (CFS)

3.5.2.1.2.1 Function

The Call Feature Server (CFS) is an IMS TAS which provides a wide range of Class 5, PBX, and Business call services.

3.5.2.1.2.2 Architecture

Each CFS is a high availability pair of servers, with one server active and one server a hot standby.

CFS configuration is either shared, per-element or movable. Shared configuration is replicated across all CFSs in the cluster and relates to areas that affect the whole cluster, such as Routing, Number Validation and global subscriber configuration. Per-element configuration is anything that is node specific, for example IP addresses, and is mostly what is configured through the craft menu. A movable block is a PBX, individual subscriber or business group and the associated configuration, for example directory number and enabled call services. A movable block is homed on a specific CFS but can be reinstantiated on another CFS if the original CFS fails.

There will be 1 CFS pair in the Core site.

3.5.2.1.3 Clearwater Core

Clearwater Core provides the IMS core components, specifically the S-CSCF, I-CSCF and the BGCF.

Clearwater consists of three different node types which together implement the I-CSCF, S-CSCF and BGCF functions

- SPN - SIP Processing Node. This node handles all the SIP processing of the Clearwater Core. It is a processing-only node, it has no local storage. It uses the SCN to store SIP transaction state. A SIP session may be started on one SPN and finished on another, as the session state is held remotely. This makes it easy to handle failures and makes it easy to scale up based on BHCA and SIP processing requirements.
- DGN - Diameter Gateway Node. This node handles all the Diameter processing of the Clearwater Core. This handles the external Diameter links to external Diameter nodes such as HSS. It is a processing-only node, it has no local storage.
- SCN - Storage Cluster Node. This node provides a distributed storage system for the Clearwater Core based upon a Cassandra database. Any configuration or state data needed by the SPN or DGN nodes is stored in the SCN. The SCN nodes scale based on the number of subscribers configured on the system, whereas the SPN nodes scale based on the number of SIP transactions. This allows for easy independent scaling.

3.5.2.1.4 Distributed Capacity Manager (DCM)

Metaswitch Distributed Capacity Manager manages the ongoing licensing and validation of the Metaswitch components in the network. The licenses are network wide and are not attached to any specific server. DCM clients are able to access Internet to connect to the Metaswtich central licensing server hosted on Amazon Web Services.

DCM is deployed as a fault-tolerant cluster of two servers in each site. This is sufficient to handle all the nodes in the deployment.

In a geographically redundant deployment, licensing clients still validate their licenses against the primary DCM (the DCM instance with the lowest Token ID), even if this is in a separate geographical site. If the primary DCM fails, the licensing client will elect a new primary DCM from among the DCM instances it can contact.

DCM is geographically redundant, and license limits are enforced across the whole deployment.

3.5.2.1.5 MetaSphere Enhanced Application Server (EAS)

3.5.2.1.5.1 Function

MetaSphere EAS is the Enhanced Applications Server (EAS) that is used to deliver value added applications to the CFS (TAS). The EAS Application Suite overlays new revenue-generating services on top of core telephone provision. MetaSphere EAS provides a mature and widely-deployed enhanced services solution including applications like Voicemail, CommPortal Web, Incoming Call Manager, Easy Call Manager, Easy/Premium Attendant and Call jump.

3.5.2.1.5.2 Subscriber Management (MetaView Web)

MetaView Web (MVW) provides three dedicated web-based user interfaces:

- MetaView Subscriber Management for staff responsible for advanced provisioning and administrative tasks.
- MetaView Provisioning for provisioning staff.
- MetaView CSR for customer service representatives.

MVW runs on the MetaView Server and provides fast network-wide access to the key functions needed to support subscribers served by MetaSphere CFS or EAS systems.

Figure 3.38 illustrates the typical MVW screen used to administer subscribers.

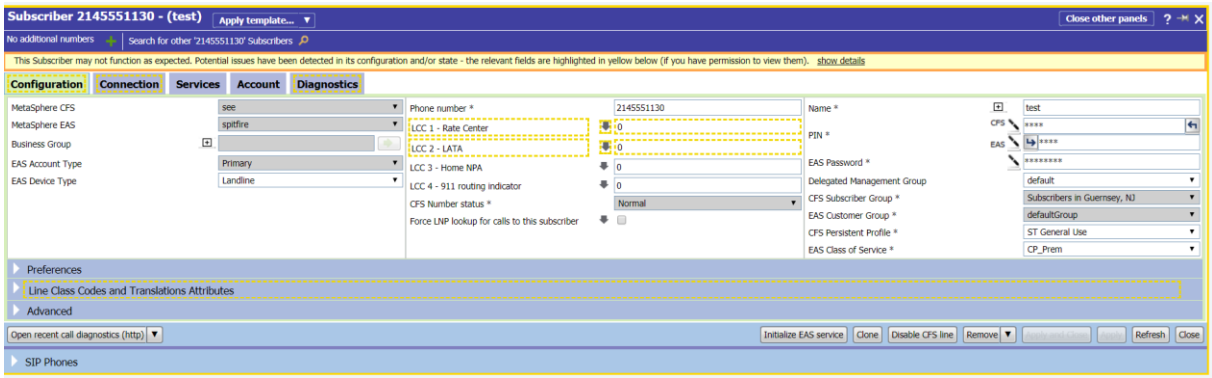


Figure 3.38 : IMS subscriber administration

Figure 3.39 illustrates an example of line features and configuration.

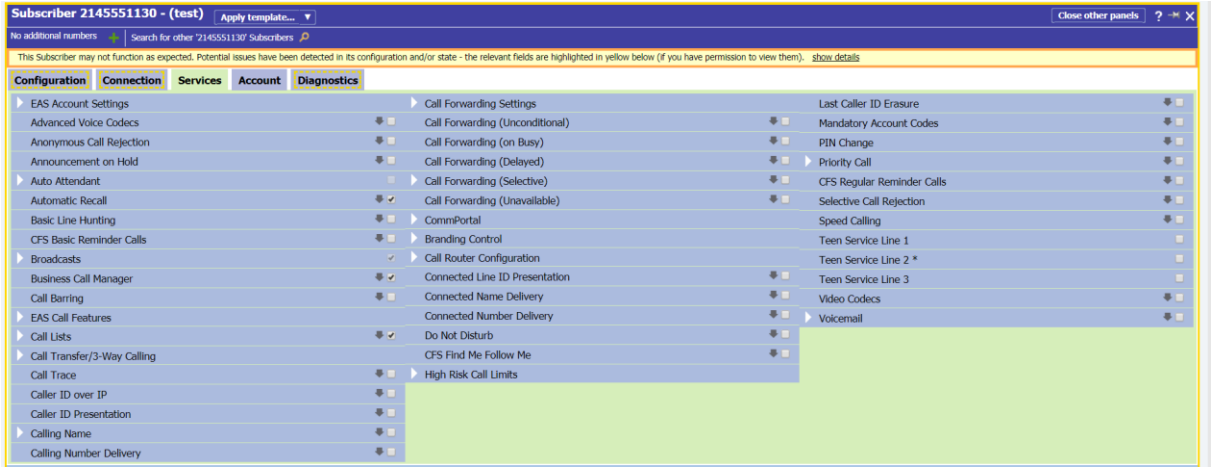


Figure 3.39 : IMS line features and configuration.

3.5.2.1.6 Rhino Management Authentication Gateway (MAG)

This Authentication Gateway provides an authenticated way for subscribers to make updates to their configuration. It consists of the following subcomponents:

- Ut Authentication Proxy (NAF)
- Bootstrapping Server Function (BSF)

3.5.2.1.7 Metaswitch Deployment Manager (MDM)

Metaswitch Deployment Manager (MDM) is the central component of Metaswitch's orchestration solution, allowing for automatic management and orchestration of selected Metaswitch products when deployed as Virtualized Network Functions (VNFs).

MDM exposes a flexible, RESTful External Orchestration API which, when used in conjunction with an orchestrator of your choice, allows full automation of key lifecycle events such as creation, scale out and scale in, and healing. It also allows you to automatically configure deployment-wide settings such as DNS and NTP server addresses and timezone. The External Orchestration API is an HTTPS interface. It uses mutual TLS for both encryption, client authentication and server authentication.

Additionally, MDM allows you to view a summary of the orchestration state of your deployment, enabling you to easily identify whether instances of Metaswitch products are in the desired state.

You must deploy MDM as a pool of virtual machines (VMs) that run alongside the Metaswitch products that it helps to orchestrate.

3.5.2.1.8 Rhino Multimedia Telephony (MMT)

The MMTel provides the various application functions required in a VoLTE network, connecting into the I/S-CSCF across the Ma and ISC interfaces. It is an IR.92 / IR.94 compliant MMTel-AS which provides a standardized set of call services, along with an XCAP server to provide a Ut interface.

3.5.2.1.9 Media Resource Server (MRS)

3.5.2.1.9.1 Function

The Media Resource Server (MRS) provides announcement, tone and mix point resources to the CFS TAS.

3.5.2.1.9.2 Architecture

MRS is a SIP resource server and CFS can communicate directly with it. MRSs function as an N+K pool available to CFS across the cluster.

There will be 2 MRSs in the Core site.

3.5.2.1.10 MetaView Director (MVD)

3.5.2.1.10.1 Function

MetaView Director (MVD) maintains a record of which CFS each subscriber line is homed on. When requested, it provides this information to the RPAS or to MetaView Web so that SIP requests and subscriber provisioning requests are routed correctly.

3.5.2.1.10.2 Architecture

Each MVD is a high availability pair of active / hot-standby servers, with one server active and one server a hot standby.

There will be 1 MVD pair in the Core site.

3.5.2.1.11 Perimeta

Perimeta provides the P-CSCF, IBCF, IMS-ALG, E-CSCF, IMS-AGW and TrGW components. It includes a variety of features such as:

In the signalling plane:

- session policy control
- security and DDOS protection
- SIP encryption,
- session forwarding
- routing and load balancing
- lawful intercept (data)
- topology and infrastructure hiding
- billing

In the media plane:

- transcoding
- firewalling
- filtering
- bandwidth control and steering
- lawful intercept (content)

In addition, Perimeta has been specifically engineered to provide powerful tools for manipulating the contents of SIP messages (inbound and outbound) while ensuring that there is limited degradation in performance. These powerful tools can solve difficult interoperability challenges that are not already covered by Perimeta's built-in interoperability features.

- SIP Message Manipulation Framework (MMF) - enables service providers to add, remove, or edit various parts of SIP messages, and use flexible customized conditions to control when these actions are applied.
- Lua SDP Editing - Enables service providers to edit the SDP in SIP messages using the Lua scripting language.

3.5.2.1.11.1 Internal Architecture

The Perimeta product comprises separate software modules for signalling session control and media session control, and these can be deployed on different instances or machines to provide a distributed SBC function.

- The Signaling Session Controller (SSC) provides the P-CSCF, I-BCF, IMS-ALG, and E-CSCF functions.
- The Media Session Controller (MSC) provides the IMS-AGW and TrGW functions.
- The Integrated Session Controller (ISC) provides the SSC and MSC components in a combined instance.

3.5.2.1.11.2 Perimeta Instances

Each Perimeta instance in the Telenor's network provides:

- VoLTE and Access interface. This provides access to IR.92/IR.51 clients arriving in the core network from the VoLTE access network.

3.5.2.1.12 Radisys Media Resource Function (MRF)

The Radisys MRF is deployed to provide media resource for conferencing and announcements, as directed by Rhino VoLTE TAS. The MRF also provides video support for IR.94 conferencing and transcoding capabilities.

Note: transcoding on MRF is not for general purpose (i.e. regular call) transcoding, rather only for conferencing.

3.5.2.1.13 Rhino Sh Cache Microservice (ShCM)

The Sh Cache Microservice is a network element that provides a caching layer in front of a Home Subscriber Server (HSS) for certain queries over Sh.

- Centralise the cache location, so that it is accessible to any number of users
- Provide Sh access to a wide range of clients, that may not support Diameter but can support HTTP
- Simplify configuration for the client (no diameter peer/routing tables to configure)
- Efficient and effective caching of Sh data without the need for sharding subscribers
- Provide a container/VM image for easy integration into virtualized environments.
- Centralise connectivity to the HSS so the HSS has a controlled number of Sh peers.

3.5.3 Operations, Administration and Management (OAM)

3.5.3.1 MetaView Server (MVS)

The MetaView Network Management System, more commonly known as MetaView Server (MVS) provides centralized management of the Metaswitch network elements with the following clients and APIs:

- MetaView Explorer GUI (for trunk configuration)
- MetaView Web GUI (for subscriber configuration)
- SOAP/XML, JSON/REST, CORBA, SNMP and SQL APIs provided for configuration and statistics integration with Telenor back-office systems

The MVS includes audit trails for configuration made through it.

Telenor will have 1 MVS pair in the Core site. The MVS is deployed as a high-availability pair, per-site, to provide added resiliency.

3.5.3.1.1 MetaView Explorer (MVE)

MetaView Explorer (MVE) is a GUI client used to manage the deployment. Telenor will use the following features of MVE:

- the ability to set, view and modify configuration for CFS (excluding subscriber specific config, for which MVW should be used)
- A list of alarms currently raised on Metaswitch network elements
- Interactive, context-sensitive help that scrolls to explain the exact item the user is currently working on
- a wide range of statistics, including historical data, from the network elements it monitors and a GUI to view this statistical data, which can also be accessed by external systems using standard SQL queries.

3.5.3.1.2 MetaView Web (MVW)

MetaView Web (MVW) is the subscriber management GUI, allowing multiple network elements to be configured at once using a simple, logical web form.

Telenor will be provisioning subscribers using APIs from Telenor's OSS. However, Telenor operations staff may still find MetaView Web useful for ad-hoc scenarios which are not possible from the OSS.

Full details on using MVW are given in MetaView Web Guide, available in the manuals section of Communities - https://communities.metaswitch.com/manuals/latestindex/5685.

MVW can be configured to use https (instead of http).

3.5.3.2 Service Assurance Server (SAS)

The Service Assurance Server provides two key functions in the network:

- It acts as the primary diagnostics platform. Metaswitch components report events in real-time, including signaling and application logic, and the SAS network element collates the data and presents it in a web-searchable GUI. SAS automatically combines all the output from every relevant element to show the end-to-end behavior of the service. SAS is "always on", so there is no need to reproduce problems with additional diagnostics or (expensive) network probes.
- Key data may also be output from SAS to upstream analytics engines that Telenor may already have or will obtain in the future.

SAS preserves diagnostics and KPIs logged to it, typically for up to one week, so they are always available, even if a server or process is not available due to a problem or maintenance.

3.5.3.3 ServiceIQ Monitoring (SIMon)

ServiceIQ Monitoring (SIMon) manages logs, metrics, and alerts raised by Metaswitch products and provides operator GUIs and programmatic APIs.

- Logs are records of events. For example, connecting to a service.
- Metrics are measurements over time. For example, the total number of calls connecting in a given period.
- Alerts are notifications of problems. For example, the total number of calls failing to connect exceeding a threshold.

ServiceIQ Monitoring incorporates best-of-breed open source components, such as Prometheus for generating metrics and Grafana for viewing dashboards. You can replace these components with other third-party components if required - speak to your support representative for details.

ServiceIQ Monitoring provides:

- Configurable dashboards for monitoring your Metaswitch service and platform. The dashboards show black-box metrics representing overall solution performance (for example number of transactions per second, average and 95th percentile latency, errors per 100k requests).
- Configurable graphs of system metrics. These can show individual or aggregated metrics (that is, metrics from individual nodes or summed over the service as a whole) over different time periods.
- Open source GUIs for viewing logs and alerts.
- Tools for exporting logs and metrics for offline analysis by Metaswitch support.

APIs for integrating with third-party OAM solutions.

3.6 Central Cloud - NFVI and VIM

The Nokia Data Center Solution is based on the ETSI reference model and aims at a modular and layered architecture with clear roles for each component. Figure 3.40 shows the functionalities provided by the Data Center Solution.

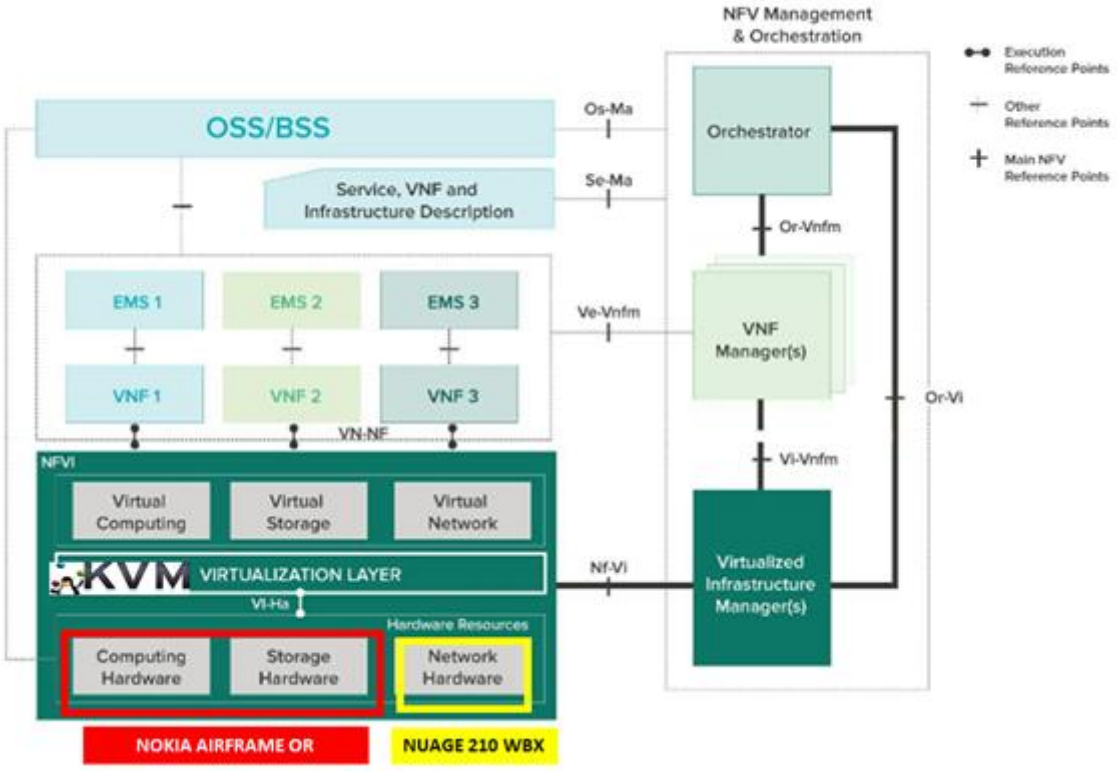


Figure 3.40 : Data Center Solution

NOKIA's hardware infrastructure in the Norway facility site is based on OCP (Open Compute Project) rack and servers. Nokia OCP-based servers are designed to meet the requirements in CSPs (Communication Service Providers), IT and enterprise datacenters. OCP is now incorporated into hardware components of the Nokia AirFrame Open-Rack (OR) Data Center Solution, including servers, switches, storage, and racks.

OCP-based infrastructure is expected to have a profound impact on cloud and datacenter environments by reducing energy and operations cost while still incorporating the latest CPU technology.

Building Blocks

Nokia Airframe Open Rack 18 uses the following hardware building blocks:

- Rack: provides mounting positions for server, switch, storage and power feed products
- Power shelf: Feeds power from the site power feed to Open Rack building blocks
- Cubby: 2 Open Rack Units (OU) three-bay shelf for server sledges
- Server sled: 2 OU dual socket Skylake based server (three server node per cubby)

Figure 3.41 : Nokia Airframe Open Rack 18 building blocks

Equipment Rack

The rack space typically consumed by two rack-mount servers with 1U each can now be used to host three OCP server nodes (2 OUs). This leads to 50% more efficient floor space utilization for the datacentre.

Open Rack equipment is assembled in 42 OU / 21" rack frame that is based on Open Rack v2 specification. The rack frame is divided for two independent power zones. Each power zone is equipped with power shelf that feeds compute, storage and other devices inside the power zone. Power distribution between power shelf and equipment is implemented with one 12,5VDC bus bar assembly that is part of the rack structure. A single chassis can be between 1x OU and 8x OU in height inside one power zone.

The 42OU / 21" rack frame with 1067 mm depth for the equipment, cables and peripherals. Rack height is 2258 mm and width 600 mm. Weight for the empty rack is 185kg. This rack supports seismic kit that improves rack seismic characteristics for NEBS (Network Equipment & Building System) Zone 4 compliancy with 850kg IT load.

There are 4 OU reserved for the switches and cable management in the middle of the rack and two 2 OU 19" adapters are included in rack frame structure. Rack layout supports up to 32 OU positions for the equipment in addition to the switches and AC power shelves.

AC power shelf reserves 3 OUs in the rack. Additional 0,5 OU support mechanic is located in the middle of rack between switch adapters. Figure 3.42 shows the rack layout with AC power shelves.

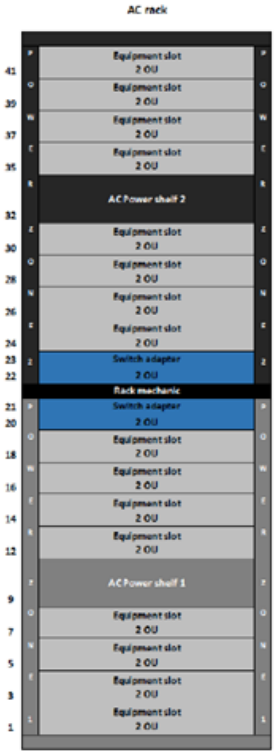


Figure 3.42 : Indicative AC powered rack

Power shelf and Power Distribution Unit (PDU)

The Power Shelf provides power feed to the Server nodes and Switches equipped in the rack. AC Power Shelf load capacity is 12,5kW with 5+1 redundant 2,5 kW PSUs.

The AC power shelf has redundant three phase inputs with two input voltage options. Power shelves support six hot-swappable Power Supply Units (PSUs) and one Rack Management Controller (RMC).

Power shelf is a worldwide model and has no input cord nor plug. The interface for the power feed is located on separate Power Distribution Unit (PDU). There are two different PDU models available to select the input connection based on regional requirements. Power shelf dimensions are 3 OU x 483 x 630 (mm) and weight is about 14kg without PSUs.

Figure 3.43 : Power shelf unit

As shown above, each shelf power can have up to 6 PSUs, each with 2,5 kW power supply. PSU has dual input for the 200 - 240 VAC and 12,5V, 200A as output. All the PSU outputs are connected to one bus bar. PSUs work with 5+1 redundancy and power shelf level output is 12,5 V / 1000 A through one bus bar that makes 12,5 kW output power.

PDU is used with rack frame and power shelf. PDU can be located on the left-right and top-bottom of the rack depending on the site cabling. Power shelf supports dual three phase inputs and two independent PDUs are used with one rack. Two PDUs could power up two power shelves in redundant manner.

PDU has six C13 type AC outlets for AC powered devices. Two leaf switches and the maintenance switch will be connected there.

Open Rack server node

AirFrame OR server node design is based on OCP specification. This server is used to form a compute node and also a storage Controller node.

AirFrame OR server node is tool-less equipment which ensures fast maintenance. Simplified construction of the OCP server mechanics leads to server change time around 1 minute and is limited to simple pull-out of old server and plug-in of new serer. There is no need for cabling and screw off from the back and front.

The server is a dual-socket 2 OU and 1/3 shelf server barebone. Server barebone is used with three bay shelf that receives power feed through one bus bar.

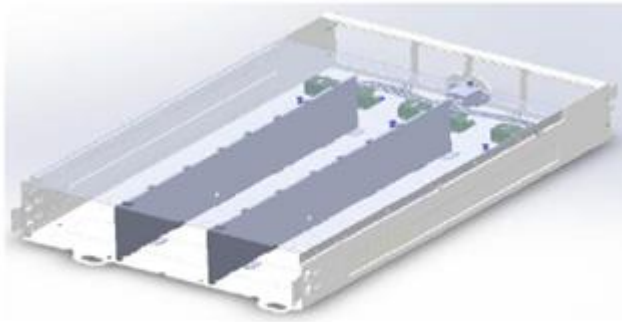


Figure 3.44 : Three bay shelf

The Three bay shelf is based on power distribution design that is compatible with Open Rack V1 and V2. This shelf design provides three bays and occupies 2 Open U (96mm). Each three bays receive power feed through one rack bus bar that provides 12,5VDC and 40A for each equipment bay.

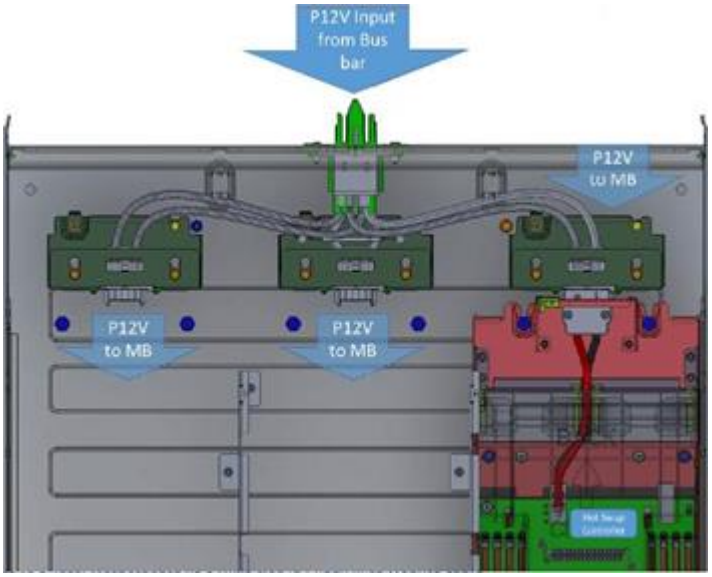


Figure 3.45 : Bus bar and servers power feed

The OR server supports Intel Xeon Skylake processor(s) and up to 12x DDR4 RDIMM modules max. 2666MHz. OCP mezzanine slot supports dual port NICs up to 100Gb Ethernet. Mezzanine slot has PCIe x16 connection towards Socket 0. There are also two PCIe card slots for flexible expansion use, both with PCIe x16 connections. Lower expansion slot is connected to Socket 0 and upper slot to Socket 1. Barebone has two 2,5” bays for SATA or NVMe devices from U.2 interface and two M.2

slots with SATA and NVMe interfaces. One 1000Base-T connection is available for Baseboard Management Controller (BMC) use.

3.6.1 Hypervisor

The host OS for all nodes within a Nokia Cloud Infrastructure Real-time (NCIR) cluster deployment (NOKIA's openstack-based cloud infrastructure) is CentOS 7.4 Linux.

NCIR implements KVM alongside QEMU hypervisors in order to run virtual machines at near-native speed. The libvirt library is used as the management API for both hypervisors.

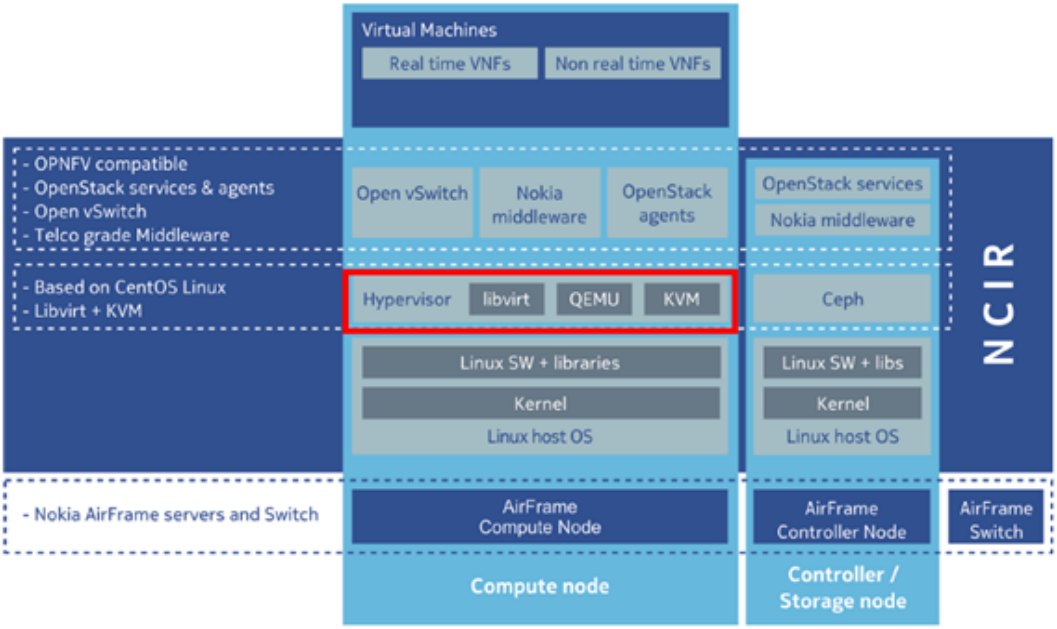


Figure 3.46 : NCIR's hypervisor

Hypervisors take on the task of virtualizing computing resources and applications.

KVM (Kernel Virtual Machine) is a Linux virtualization technology module that allows a user space program access to the hardware virtualization features of various processors. It is used to:

- Set up the guest Virtual Machine address space. The host must also supply a firmware image that the guest can use to bootstrap into its main OS.
- Feed the guest simulated I/O

QEMU (Quick Emulator) is a hosted virtual machine monitor. It emulates CPUs through dynamic binary translation and provides a set of device models, enabling it to run a variety of unmodified guest operating systems. QEMU achieves near-native performance by executing the guest code directly on the host CPU.

The resources within an NCIR stack are managed by the standard agents within the OpenStack framework. NCIR supplements standard OpenStack solutions with additional components in order to secure Carrier Grade Telco cloud performance.

Accelerated Virtual Routing and Switching (AVRS) runs inside the hypervisor and removes performance bottlenecks by offloading virtual switching from the networking stack. The CPU resources necessary for packet processing are drastically reduced, so that fewer cores are required to process network traffic at higher rates.

AVRS is based on the Data Plane Development Kit (DPDK) technology from 6WIND fully integrated with Nuage VRS and the Linux environment, so that existing Linux applications do not need to be modified to benefit from packet processing acceleration. For the Linux application there is no

difference between VRS and AVRS from the end user usage perspective. AVRS supports standard VMs using virtio drivers. AVRS also supports vhost with hugepages for zero-copy packet forwarding.

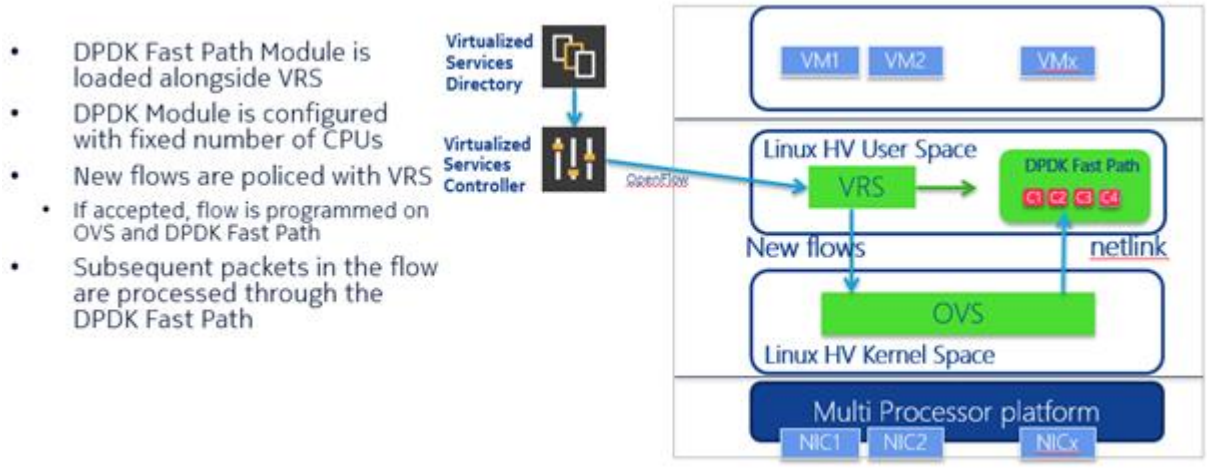


Figure 3.47 : Nuage AVRS DPDK solution

AVRS will be deployed automatically with the Virtual Infrastructure Manager (VIM) NCIR in all compute nodes.

3.6.2 Computing

The OR servers will be used as compute nodes, controller nodes and storage nodes. Based on dimensioning requirements there will be 21 servers, which means seven 3-bay shelves.

The OR servers will be used as follows:

- 6 servers as compute nodes only
- 3 servers as compute and controller nodes
- 3 servers for Nuage components (bare-metal), not part of NCIR
- 9 servers as compute and storage nodes

The hardware configuration for a), b) and c) groups listed below is the same. The detailed configuration is listed in Table 3.8.

Table 3.8 : Compute server configuration

Compute and Controller nodes	Configuration
Server/Processor	Airframe OR 18 Server: 2x Intel Xeon 6138, 20-Core 2.0 GHz (Dual socket)
Memory	384GB (DDR4), 2666MHz
Network	Totally 4 ports x 25Gb: 1 x Airframe OCP Mezzanine NIC (2x 25Gbit) 1x Airframe PCIe NIC (2x25 Gbit) + BMC port used for IPMI (1000Base-T RJ45)
Storage	1 x 480GB Airframe Disk SSD 2.5 Inch 1x 480GB Airframe M.2 2280 SATA

NCIR18 will require vCPU resources and this depends on the server role. As mentioned above, in this deployment we expect each server to act as in one of the below roles:

a) Compute and Controller
b) Compute and Storage
c) Compute only

A server could also act as a storage server only, but this is not applicable in the Norway facility site.

Host CPU isolation partitions physical CPUs between host system tasks (including OpenStack services) and virtual machines, which protects critical system tasks from potential malfunctions.

Dedicated CPU resources are allocated to host system services (OVS, Ceph, interrupt handling, SW agents, etc.). Host resources are excluded from pool available for virtual workloads.

NCIR support host CPU isolation. This is configurable and it sets the number of CPUs to isolate what will be used only by the hypervisor processes. The number must be a multiplication of the CPU hyper threading configuration which is usually 2.

When a high load performance is required, it's recommended to isolate the CPU resources used by the hypervisor, from the CPU resources used by the VMs.

An example of a compute node CPU allocation is illustrated in Figure 3.48.

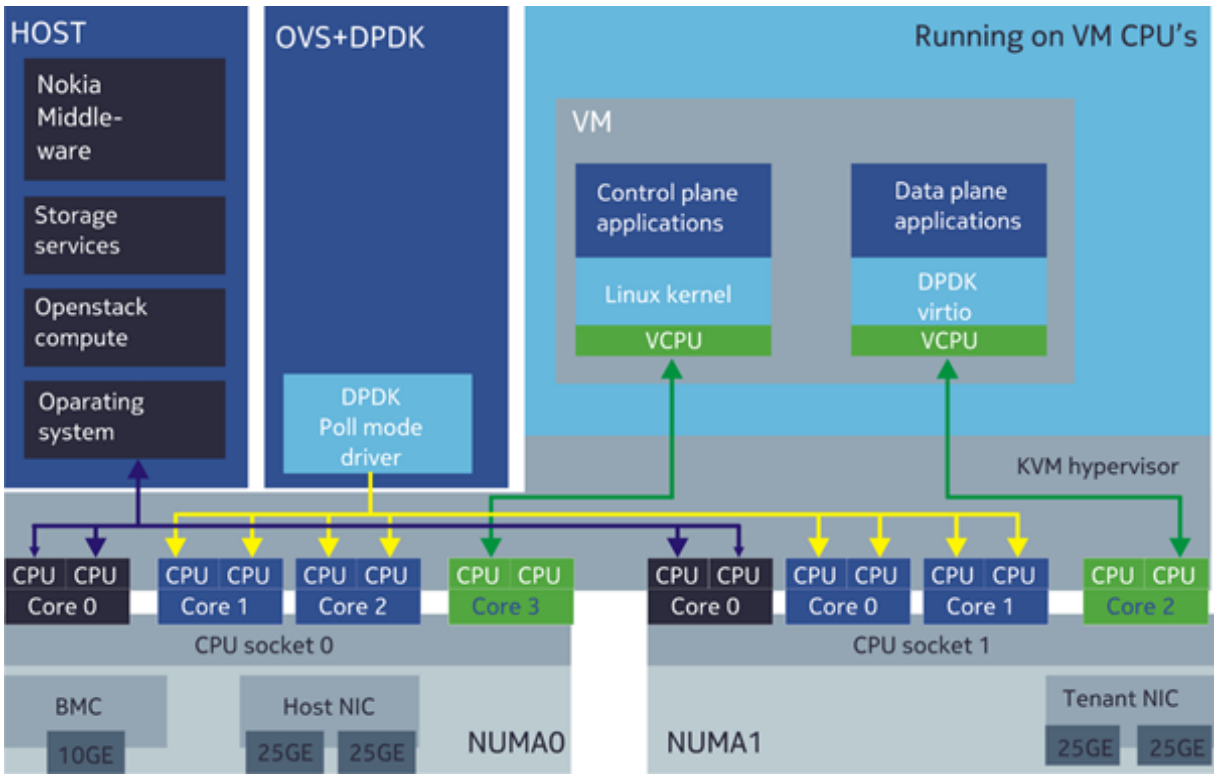


Figure 3.48 : Compute node CPU allocation

NCIR allows configurable allocations of CPUs in three distinct allocation pools:

- Middleware CPUs for host processes (OS and Nokia middleware)
- OVS-DPDK CPUs for Poll mode threads (OVS-DPDK will be AVRS in this case)
- VM CPUs

In nodes that have compute services, platform CPUs and OVS-DPDK CPUs are configured. The rest are allocated to the VM CPUs.

An example of the core allocation is the following:

- Middleware CPUs: 2 cores (4 threads)
- OVS-DPDK: 2 cores (4 threads) as minimum requirement. The OVS-DPDK should be configured to have at least one core from each of the NUMA nodes. CPU allocation is configurable and it is possible to be reduced in case VMs needs more core and the amount of traffic does not require so.

When the combined storage on compute node profile is used, physical resource separation is needed to guarantee the unobstructed functionality on high load situations.

For OS and Ceph configurations with two OSD disks, the platform requires 2 additional cores (4 threads if HyperThreading is enabled) and additional memory.

	Controller + Compute	Storage + Compute	Compute
	OR18	OR18	OR18
Middleware	16	2	2
Storage (OSD)	0	4	0
OVS+DPDK (min 4 vcpu)	4	4	4
Host vCPU total	20	10	6
VNF vCPU total	60	70	74
vCPU total (HT enabled)	80	80	80
Number of sockets	2	2	2
Physical cores per socket	20	20	20

Figure 3.49 : Compute node's CPU isolation

There will be 32GB memory per server for NCIR, while the rest is available for VNF use.

3.6.3 Network

For 5G-VINNI there will be three networking devices, two leaf switches and one management switch.

Management switch

Ethernet switch is a high performance and low latency layer 2/3/4 Ethernet switch with 48x 10GBase-T ports and 6x QSFP port in a 1U form factor. It provides connections between external networks and server nodes.

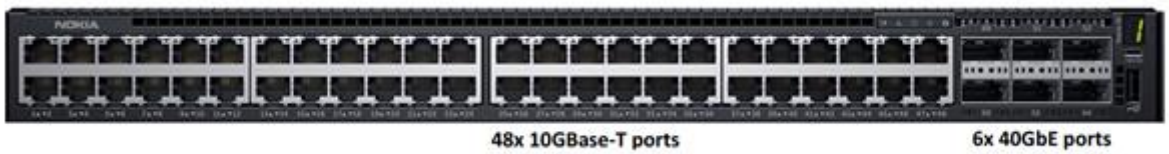


Figure 3.50 : Management switch

Power feed units are hot-swappable and power feed is 1+1 redundant. Both AC and DC power feed options are available. Fan units are hot-swappable and fan array is N+1 redundant.

Figure 3.51 : Management switch power feed

Each server and leaf switch will connect to the management switch (1Gb) and then to OOB uplink device that is provided by Telenor.

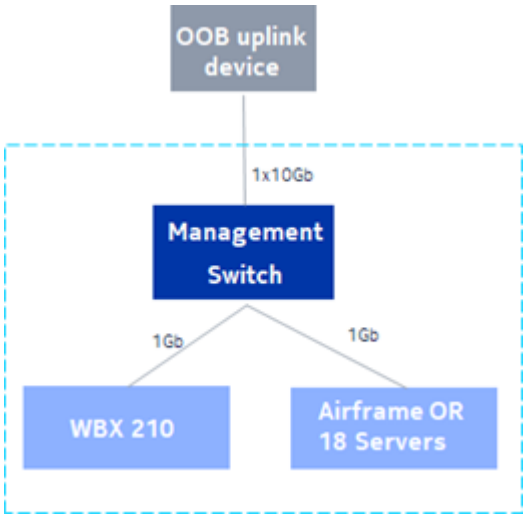


Figure 3.52 : Management switch connectivity

Leaf switches

In 5G-VINNI the 210 WBX will take the role as Leaf and Spine switch in the IP Fabric architecture as well as the datacentre gateway.

The 210 WBX running Nuage Networks software is a 1 RU datacenter gateway supporting software-defined networking (SDN).

The Nuage leaf switch is a L2/3/4 Ethernet switch with 32 QSFP28 ports in a 1U form factor. It provides connections between external networks and server nodes. Each QSFP28 port can be independently configured as 100GbE, 2 x 50GbE, 1 x 40GbE, 4 x 25GbE or 4 x 10GbE. This would allow for higher server speeds then the n times 25G as planned now. In the Norway facility site, each QSFP port will have a splitter to 4x25Gb towards compute server's ports.

Figure 3.53 : Nuage WBX 210 switch

Power supply units (PSUs) are hot-swappable and power feed is 1+1 redundant. Fan units are hot-swappable and fan array is n+1 redundant.

Physical ports:

- 32x 100GbE QSFP+ ports
- Supports various port breakout (100GbE, 2 x 50GbE, 1 x 40GbE, 4 x 25GbE or 4 x 10GbE)
- 4x 10GbE per Port towards servers, 2x 100GbE uplink towards Provider Edge router

High availability

- Redundant hot-swappable power supply 1+1

- Hot-swappable fan tray N+1

Features

- MLAG
- OSPF, BGP4, ECMP
- VXLAN
- VTEP for L2 and L3

Each compute node is equipped with two NICs, each supporting 2 x 25Gbps ports. Compute node is connected to both leaf switches in the rack. The traffic separation is shown in Figure 3.54.

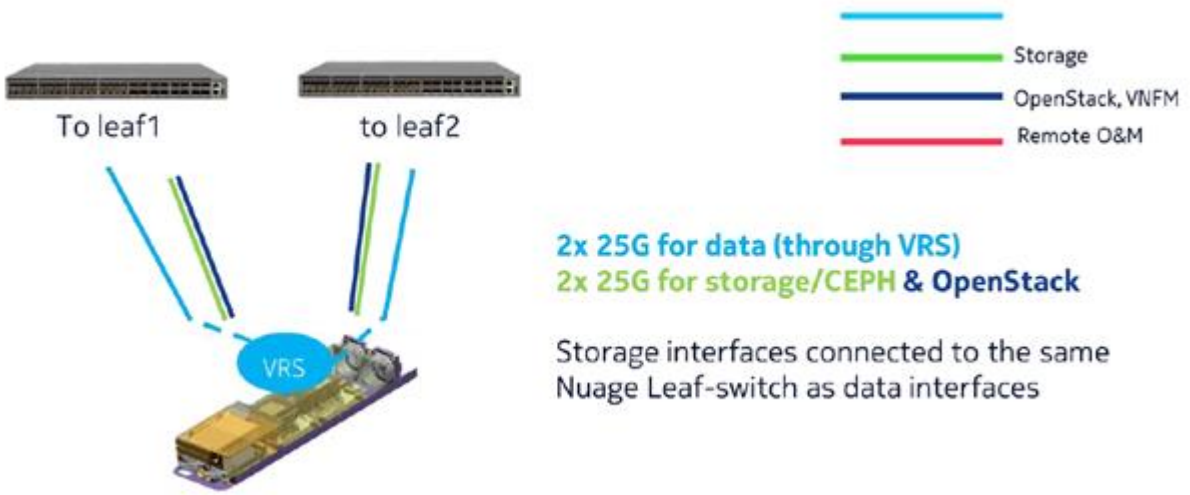


Figure 3.54 : Connectivity from compute servers to the leaf switches

There are no separate WBX switches in this deployment (one rack solution), so 100Gb speed ports will be used to interconnect the Leaf-switches towards the PE router. In this setup the single pair of switches takes the role of aggregator-router, leaf and spine switches. There is no requirement for resilience on PE router, so both leaf switches will be connected to one router using two different cards to secure the redundancy. The PE router is provided by Telenor. The connectivity between datacentre and the PE router is illustrated in Figure 3.55, but note that the redundant connectivity between switches and PE will not be configured initially.

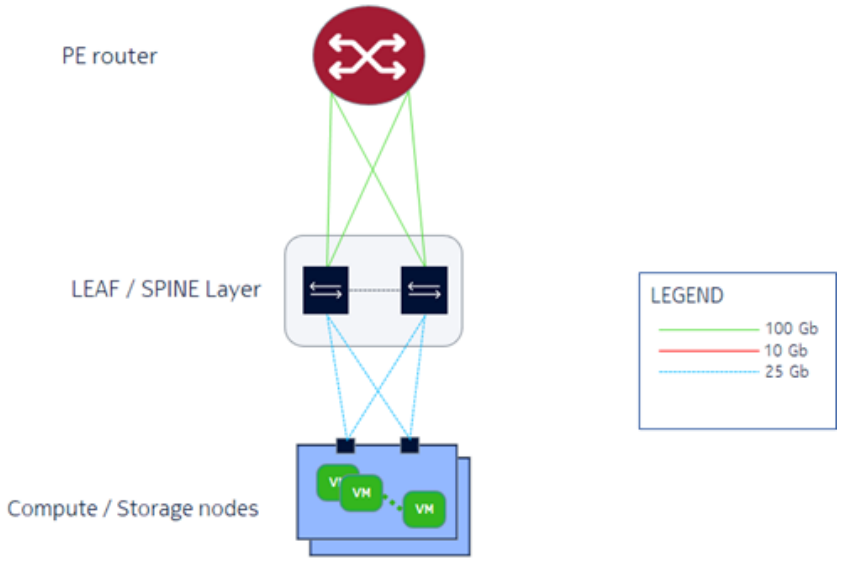


Figure 3.55 : Leaf switch to PE router connectivity

3.6.4 Storage

3.6.4.1 Storage Architecture

When VMs are deployed on a physical server, they consume space in the server's disks. When the capacity needs increases and the physical server run out of storage space there might still be available storage space in another server.

CEPH solves this problem by aggregating storage space from all the hard drives. CEPH creates a large pool of storage, then secures and redistributes it according to the VM requirements.

CEPH is software defined storage designed to provide excellent performance, reliability and scalability.

CEPH version will be 12.2.2:

- Object Storage Daemon (OSD) disk are hosting single OSD
- No dedicated Journal disk
- Blue Store backend
- Ceph-ansible – 2.3.0rc5

There are three main Ceph components in the storage architecture.

- The Ceph client is the entity accessing or requiring storage in the system
- The OSD is a software component in charge of the local storage unit on the server. One OSD is defined per storage unit (disk) and this means that if you have 2 storage units you have 2 OSD instances.

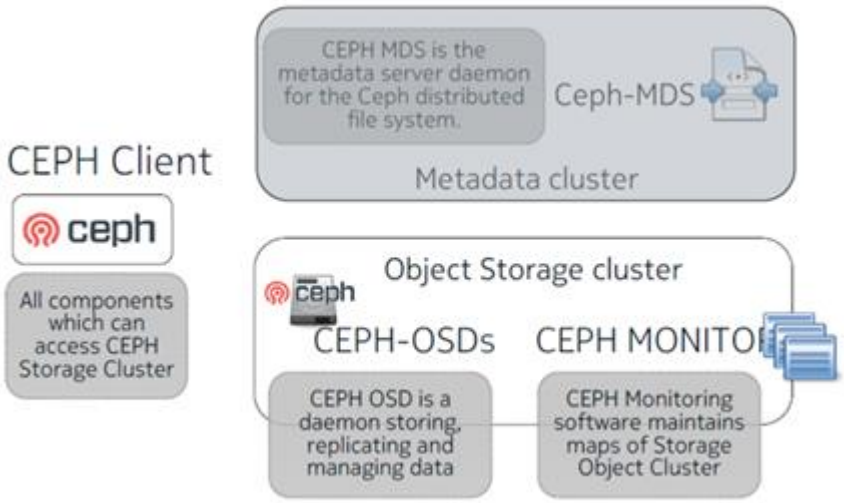


Figure 3.56 : CEPH storage architecture

The monitor components are in charge of the monitoring the system's health and they also manage and maintain the map of storage units.

In the Norway facility site, Ceph is used as a storage service for VM. In other words, Ceph stores mainly volume for VMs which is still managed by cinder service.

The Ceph Monitor components are located in Controller nodes only. They provide the map view of the storage resource. In total we have 3 CEPH monitors that reside in the servers as the Openstack controllers.

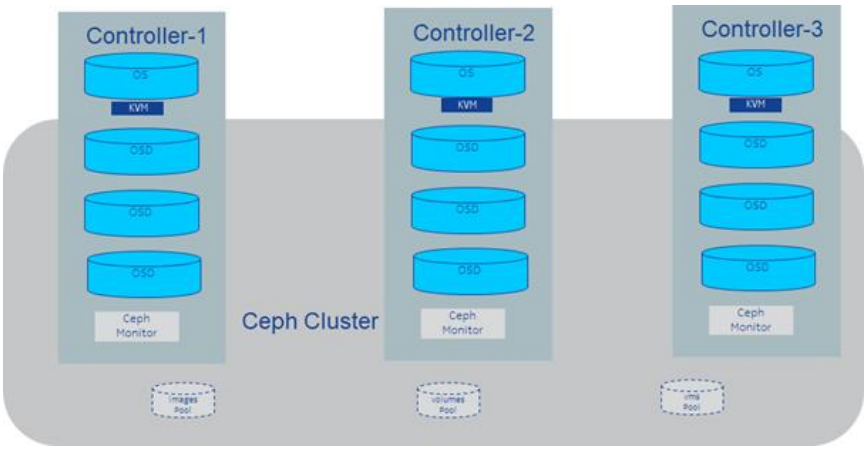


Figure 3.57 : CEPH monitor's deployment in Controllers.

The Ceph OSDs are located in compute or storage nodes only and set up the shared storage resources.

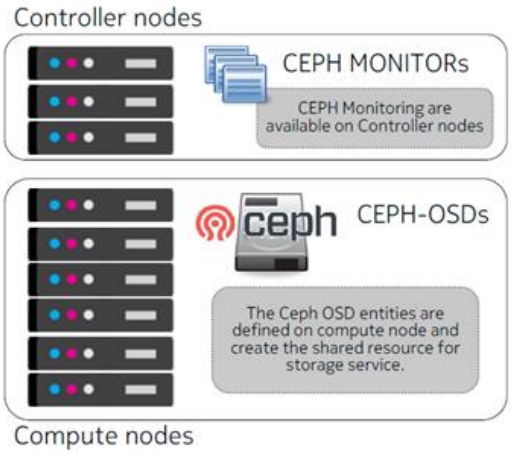


Figure 3.58 : CEPH's storage nodes and OSD

Cinder attached volume is mounted through CEPH-RBD. The same applies for VM root disk (ephemeral) which is also mounted through CEPH-RBD.

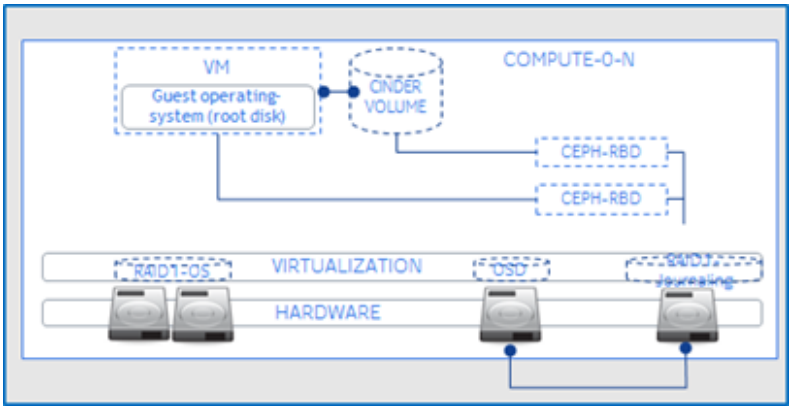


Figure 3.59 : CEPH's clients

The CEPH clients are Cinder and Nova, for which the following settings will apply:

- Cinder Back End volumes will be attached through Ceph RADOS Block Device (Ceph-RBD).
- The VM root disk (ephemeral) will be mounted through Ceph-RBD.
- Images will use the local disk in the controllers.

3.6.4.2 Storage Implementation

Ceph was designed to run on commodity hardware, which makes building and maintaining petabyte-scale data clusters economically feasible. When planning out the cluster hardware a number of considerations must be balanced, including failure domains and potential performance issues. Hardware planning should include distributing Ceph daemons and other processes that use Ceph across many hosts.

Compute nodes can contribute their disks in the CEPH storage cluster for the hyper-converged implementation or there is an option to dedicate several servers to act as storage nodes.

The Ceph deployment in the Norway facility site is a hybrid hyper-converged solution for compute and storage servers. A number of servers will be used as Compute nodes (VM deployment) and as Storage nodes. In this case the VM root disk and attached volumes will be stored on the storage node. Storage nodes will use Ceph as a distributed storage solution.

The same type of Airframe OR 18 servers will be used for storage (and compute as well). In total we have 9 storage servers with Data OSD disks in each one. Their hardware configuration is below.

Table 3.9 : Storage server configuration

Compute and Storage nodes	Configuration
Server/Processor	Airframe OR 18 Server: 2x Intel Xeon 6138, 20-Core 2.0 GHz (Dual socket)
Memory	384GB (DDR4), 2666MHz
Network	Totally 4 ports x 25Gb: 1 x Airframe OCP Mezzanine NIC (2x 25Gbit) 1x AirframeC PIe NIC (2x25 Gbit) + BMC port used for IPMI (1000Base-T RJ45)
Storage	2 x 3.84TB Airframe Disk SSD 2.5 Inch (OSD Data) 1x 480GB Airframe M.2 2280 SATA (Boot OS)

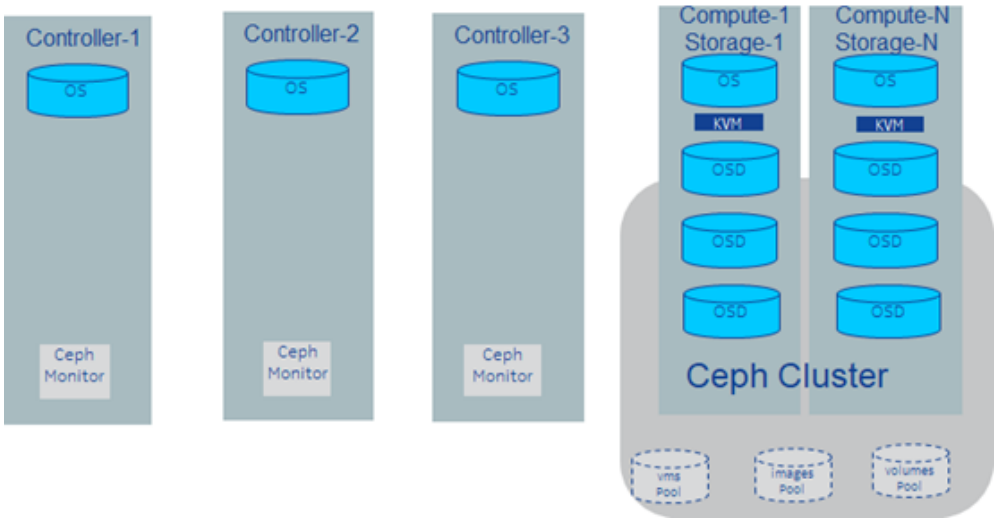


Figure 3.60 : CEPH cluster

The net storage requirements are 24 TB, which means the gross storage should be higher considering the data replication ratio.

CEPH using its CRUSH algorithm distributes objects and their replicas to OSDs. The number of replicas can be set, but it's recommended to have at the least the same number of storage servers.

Table 3.10 : Ceph replication factor

Settings	Description
CEPH Replication factor: 2	Each CEPH cluster should have a minimum of 2 Storage Servers (in this site we have 9 servers). This is due to the CEPH replication factor of 2. Data will always be stored in 2 different servers for high availability.

For the Norway facility site deployment, the allocation is:

- 9 servers to act as storage nodes (OSDs will reside there)
- 3 monitors that reside in the same servers with the controllers
- 18 disks for OSD data (2 disks in each server)

Table 3.11 : Ceph disk configuration

Disk category	Description
OS/Boot disk	1 x SSD disk will be used for Host OS in each storage servers
OSD	Two 3.84TB SSD disks will be used as OSD in each storage server. It will be totally 2 Disks x 9 Servers x 3.84TB raw data.

3.6.5 EMS

NADCM (Nokia AirframeData Center Manager) may be deployed optionally as a VM (it could be in Nuage baremetal servers). There is no plan yet for NADCM deployment in 5G VINNI.

3.6.6 VIM

Nokia Cloud Infrastructure Real-time (NCIR) is a Network Functions Virtualization cloud solution offering unique scalability and performance for most demanding telco workloads in 5G era.

It is an OPNFV verified telco-grade solution covering the requirements of high bandwidth and low latency applications at edge datacenters. NCIR leverages core Nokia NCIR virtualization and carrier-grade technologies, Intel's DPDK high-performance packet processing, real-time optimized open architecture, and Openstack software suite to implement a unique carrier-grade, high-availability architecture on which high performance production systems can be deployed. Figure 3.61 shows its high-level architecture.

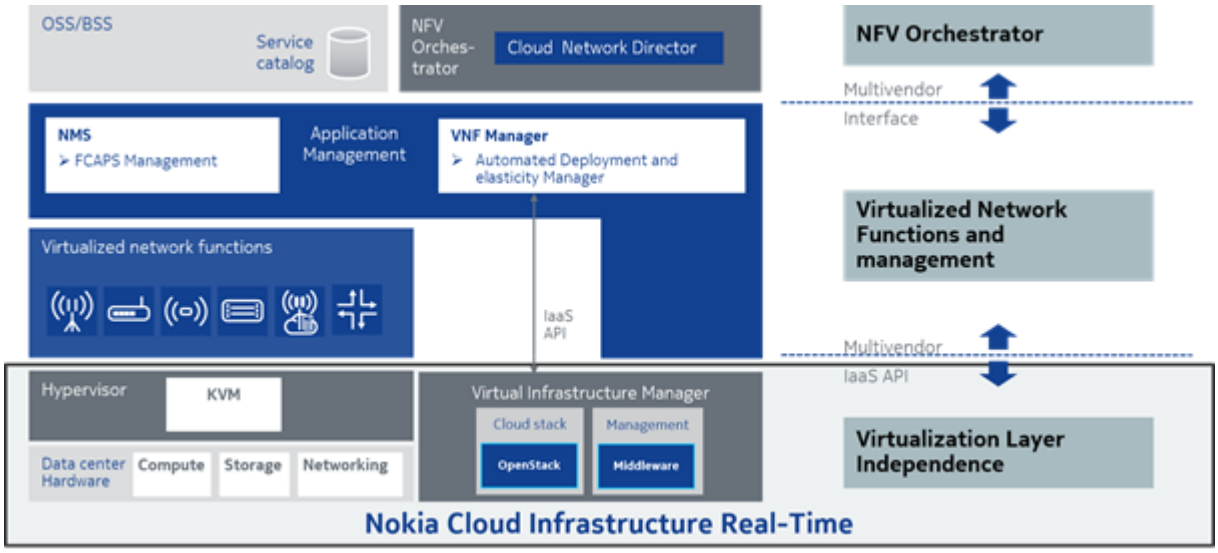


Figure 3.61 : Nokia Cloud Infrastructure Real-time (NCIR)

NCIR comprises a Cloud Host environment, mainly focused on building a Network Function Virtualization Infrastructure (NFVI) and Virtualized Infrastructure Manager (VIM) by integrating with Nokia Middleware features, with components from upstream projects, such as OpenStack, Ceph Storage, KVM, Open vSwitch, Ansible and Linux, deployed into Nokia AirFrame Data Center Solution (NDCS) hardware.

The current NCIR release uses Linux CentOS 7.5 and incorporates elements from OpenStack Queens, additional open source software components and Nokia Host Middleware services tailored to the needs of a fully automated installation for different hardware and Virtual Network Function (VNF) configurations.

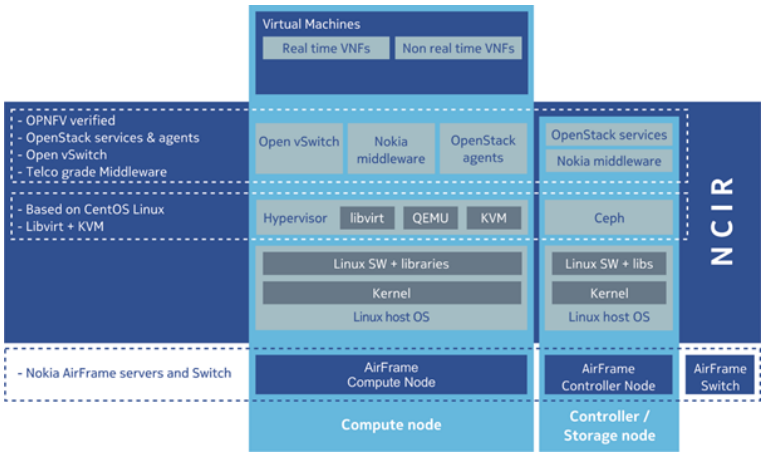


Figure 3.62 : NCIR architecture

NCIR implements KVM alongside QEMU hypervisors in order to run virtual machines at near-native speed. The libvirt library is used as the management API for both hypervisors.

The resources within an NCIR stack are managed by the standard agents within the OpenStack framework. NCIR supplements standard OpenStack solutions with additional components in order to secure Carrier Grade Telco cloud performance.

OpenStack is an open-source platform for cloud-based applications. It is an integration of several components providing services for deploying applications in the cloud.

OpenStack is used in NCIR in accordance with the Nokia strategy to use open and standard-based solutions.

Currently NCIR uses OpenStack Queens, August 2018 baseline, and integrates the components/services listed in Table 3.12.

Table 3.12 : Openstack components and version for Release 0

OpenStack components¶	
aodh	6.0.1
cinder	12.0.3
glance	16.0.1
horizon	13.0.1
ironic	10.1.4
keystone	13.0.1
neutron	12.0.3
nova	17.0.5

NCIR integrates the following OpenStack services: Nova, Neutron, Keystone, Glance, Cinder, Horizon, Aodh, and Heat.

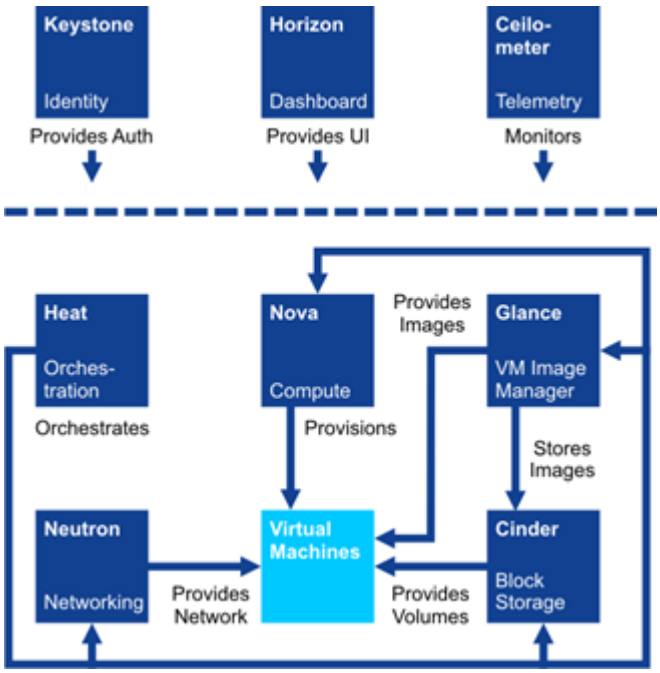


Figure 3.63 : Openstack services in NCIR

3.6.6.1 Controller nodes

They run the NCIR services needed to manage the cloud infrastructure. Services are run in carrier grade mode, with controller nodes acting as a high-availability cluster.

Controller nodes manage hosts over the internal management network. They also provide administration interfaces to clients over the OAM network.

In the absence of dedicated storage nodes, the controller nodes also provide storage services. In Norway facility site case, there are three controllers which are co-located with the compute nodes.

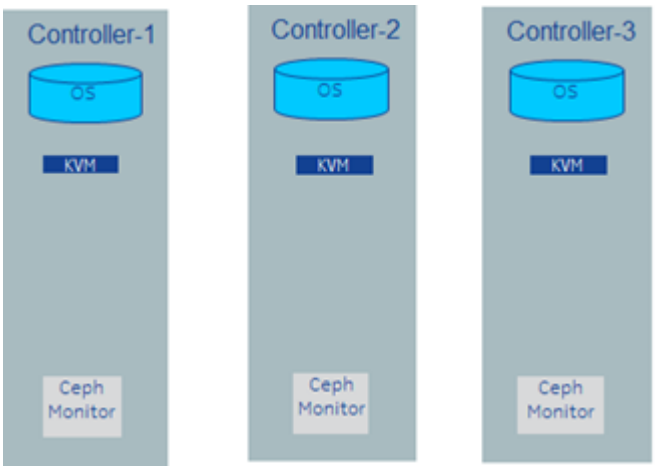


Figure 3.64 : NCIR controllers in HA mode

3.6.6.2 High Availability

NCIR provides features to support highly available hosting of virtual machines.

For 5G-VINNI Norway facility site, NCIR will be deployed with 3 controllers for high availability.

The NCIR High Availability (HA) solution is a Telco-grade solution filling the upstream gap. It is integrated with OPNFV Doctor project. Its modularity makes OpenStack upgrades transparent and seamless, and it is a scalable solution to any number of nodes.

HA provides fault detection and recovery in milliseconds for:

- Service level monitoring
- Data link status monitoring
- Node level monitoring
- Disk monitoring
- Virtual machines handling in case of compute node failure (auto evacuation)
- State aggregation
- Split brain detection.

NCIR includes the following extensions to OpenStack, that support high availability:

Fast detection of compute node failures

Implementation through an efficient and scalable heartbeat protocol between controller and compute nodes by using corosync and pacemaker.

Fast recovery of virtual machines instances upon detection of a compute node failure

NCIR automatically reschedules VMs instances to available compute nodes in the cluster when the original VM's hosting compute node fails.

Fast detection of virtual machine failures

NCIR high availability agents automatically detect the failure in KVM/QEMU instances. The failure is automatically handled by the NCIR VIM.

Automatic recovery of failed VM instances

NCIR automatically detects the VMs in Error state. The VMs in this state are automatically restarted.

Live migration support with DPDK-accelerated networking

Live migration support of virtual machines using high-performance networking options.

Graceful shutdown (and other operations) of virtual machines

Nova extensions turn the shutdown operation of virtual machines into an ACPI shutdown. Guest applications can execute operations such as closing files, updating persistent databases, or cleanly disconnecting from subscribed services, by registering shutdown scripts using standard ACPI mechanisms.

Link Aggregation (LAG) support

Support for LAG, also known as Aggregate Ethernet, on controller and compute nodes for link protection. Link Aggregation Control Protocol (LACP) is used for bundling several physical interfaces into one logical aggregated Ethernet interface.

Protected HA Middleware

NCIR Service Manager protects all critical processes. In case of failure, individual processes can be independently restarted.

For hardware recovery, NCIR supports single-fault scenarios. If a single node fails, NCIR detects the fault and immediately initiates recovery, including VM evacuation if the fault is on a compute host.

3.6.6.3 Simultaneous Multi-threading

Hyper-Threading is Intel's proprietary simultaneous multithreading (SMT) implementation used to improve parallelization on their CPUs.

Depending on the workload being executed the end user or cloud admin may wish to have control over how the guest uses hardware threads. To maximise cache efficiency, the guest may wish to be pinned to thread siblings. Conversely the guest may wish to avoid thread siblings. This level of control is of particular importance to Network Function Virtualization (NFV) deployments

Except host specifications, flavors can be distinguished using or not using (to run in isolated mode) hyper threading.

As in the NCIR installation all computes will be installed with hyperthreading enabled in the BIOS settings, attention is needed for the VMs that require to work in isolated mode (with the requirement 'hyperthreading disabled'). A special 'Extra Spec' item needs to be added to the flavor: **hw:cpu_thread_policy=isolate**. This will make sure the hyperthreaded sibling of the pCPU will not be used by any other VM deployment and as such will have the same effect as if the hyperthreading would have been disabled in the BIOS.

3.6.6.4 SR-IOV

Single Root IO Virtualization (SR-IOV) provides hardware abstraction of a PCI device for the use of multiple consumers. This capability, used by KVM and OpenStack, allows exposing Virtual Functions (VFs), which are slices of the physical function, directly to virtual workloads. In NCIR, SR-IOV is used for providing direct access to networking hardware.

Workloads assigned SR-IOV VFs can use the hardware resources directly (using appropriate drivers), without interacting with the hypervisor layer, therefore providing a performance boost for workloads that are I/O intensive.

The maximum number of VFs per port depends on the network adapter. Mellanox NIC can support up to 128 VFs. Once the VFs have been created, one or more VFs can be assigned to a VM. Upon successful assignment, the VM is ready to use.

5G Core VNFs will use only OVS-DPDK, thus compute nodes will not be needed.

Network adapters and OS can support SR-IOV, so if there is any requirement in the future for compute nodes it will be possible

3.6.6.5 Performance Optimization

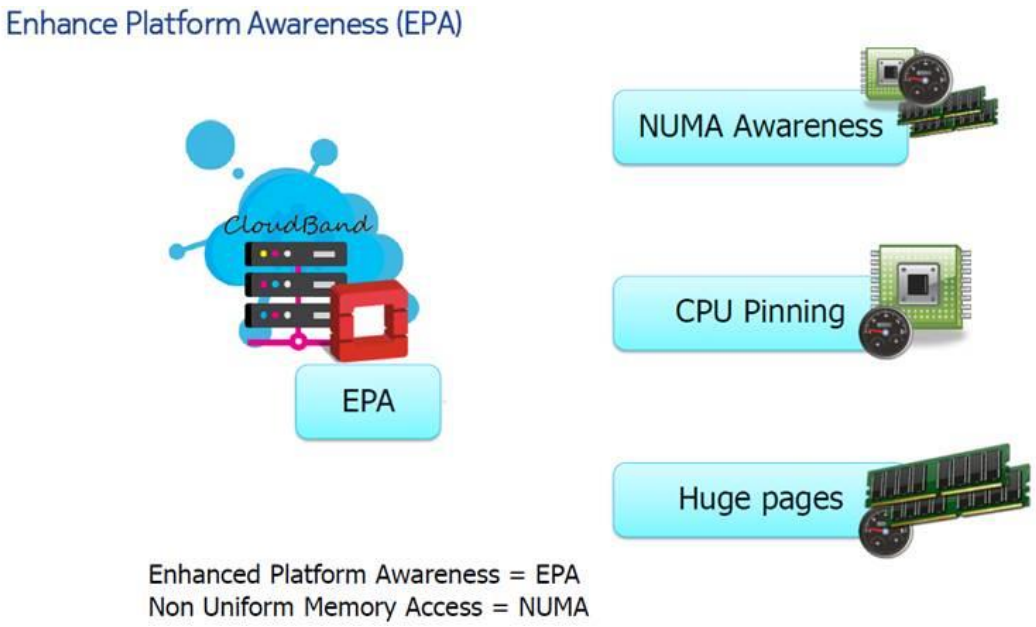


Figure 3.65 : Enhance Platform Awareness

NCIR comes with EPA (Enhanced Platform awareness). Enhanced Platform awareness will enable virtualized applications to have direct access to a physical resource. For example, this allows VMs to be strictly assigned to CPU and memory for high performance. In other words, in telco cloud, a real-time application can request exclusive physical resource assignment instead of resource sharing with other applications.

3.6.6.5.1 Huge Pages

Most current CPU architectures support bigger pages (so the CPU/OS have less entries to look-up), those are named Huge pages (in Linux).

Huge page optimizes the memory paging or table. It is defined during the installation of the server.

In a regular OS installation, RAM paging defines allocation units with a specific size, for example of 4KB (Kilo Bytes). The hypervisor assigns a set of Units to a Guest VM. To allocate 1GB to a VM, the system has to assign 262,144 units or chunks of 4KB. Every time the VM accesses the RAM, the system needs to parse the RAM units.

In order to optimize the system for this RAM parsing, Huge page allows big chunks to be stored in memory. You can define a percentage of the memory in huge pages mode. In this case, the unit or chunk will be defined with a size of 1GB. For a Guest VM configured with 4 GB, the system allocates 4 chunks instead of 1,048,576 units.

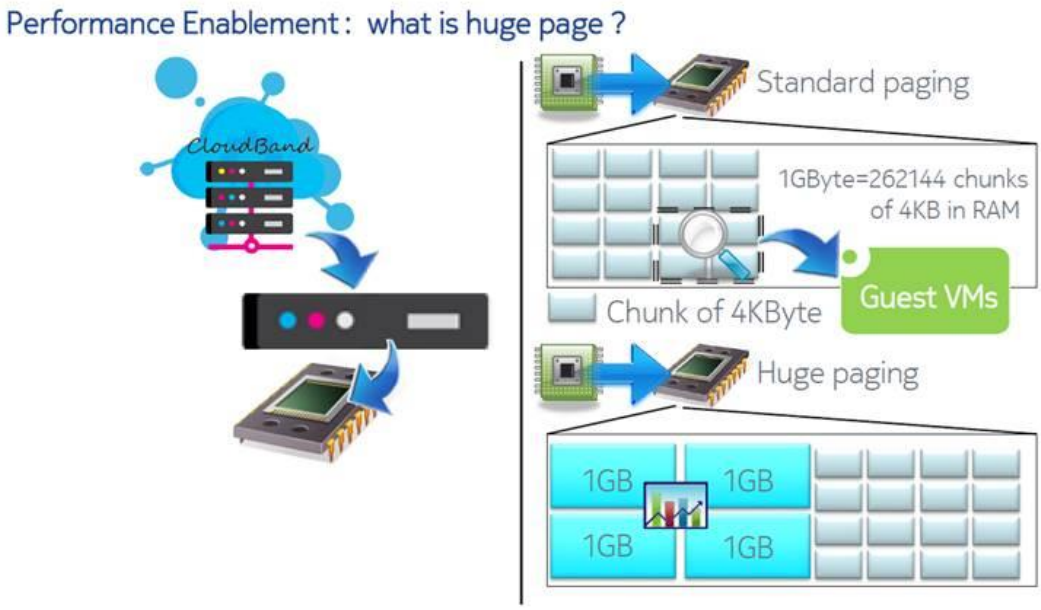


Figure 3.66 : Huge pages

Huge pages are a technology for increasing memory access speed in memory intensive application, which relies on CPU MMU features.

Huge pages must be allocated in host physical memory, then they can be allocated to VMs by the Nova scheduler.

For this deployment all **Ericsson VNFs in services zone will require 1G Huge Pages**. All servers assigned to Services Availability Zone will have huge pages enables at 70% of the total memory.

3.6.6.5.2 NUMA Awareness

Traditionally, a multi-processor system provides an equal access to the memory over the same bus. This architecture is also called SMP for Symmetric Multiprocessor. SMP was initially designed to manage RAM with CPU with the increase in the number of CPU cores. The high increase of CPUs and cores bring SMP to the limit. The single bus becomes a point of congestion. NUMA solves this issue and provides RAM distribution over a platform.

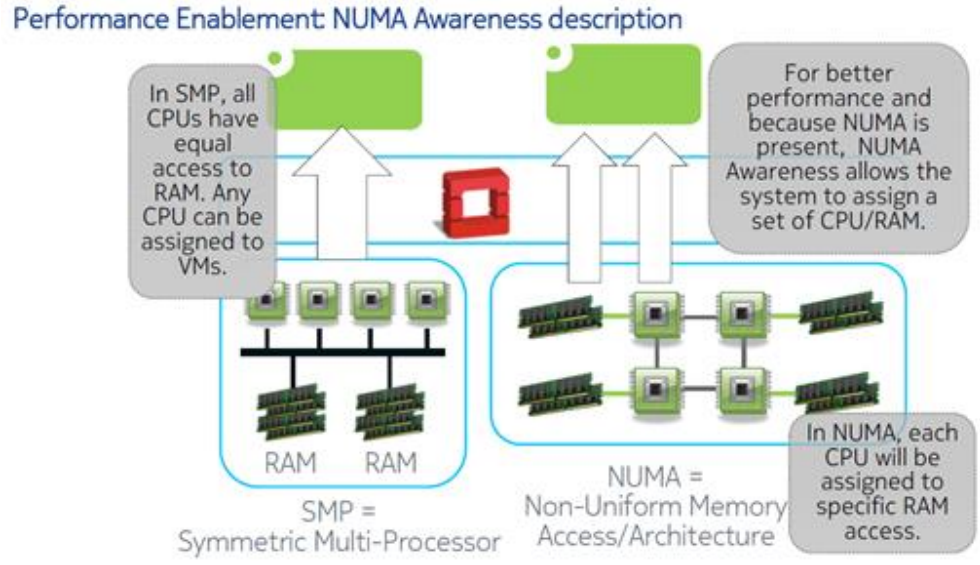


Figure 3.67 : NUMA awareness functionality

NUMA awareness in NCIR allows for the scheduling of workloads in a way that ensures they are placed based on the NUMA topology they requested, using flavors. For example, making sure that all VM cores and memory are scheduled to the same NUMA node.

NCIR will assign VM cores and memory from the same NUMA node by default. If user wants to use both NUMA node then this could be described in the flavor (hw:numa_nodes).

3.6.6.5.3 CPU Pinning

By default, instance vCPU processes are not assigned to any particular host CPU, instead, they float across host CPUs like any other process. The CPUs are a pool resource available for the deployment of Guest VMs.

Some workloads require real-time or near real-time behaviours, which is not possible with the latency introduced by the default CPU policy. For such workloads, it is beneficial to control which host CPUs are bound to an instance's vCPUs. This process is known as pinning. No instance with pinned CPUs can use the CPUs of another pinned instance, thus preventing resource contention between instances.

In NCIR, CPU pinning is implemented based on policies, which allows a guest VM to request pinning of its virtual cores to physical cores based on the constraint of being isolated/run together, etc. This is achieved through the use of flavors (property hw:cpu_policy=dedicated).

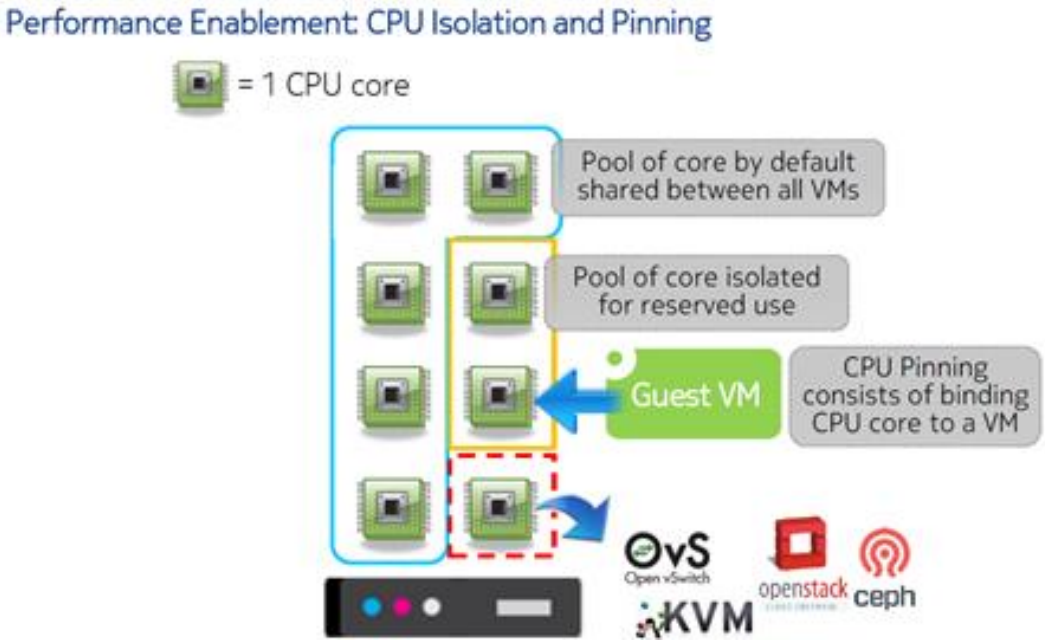


Figure 3.68 : CPU Pinning functionality

3.6.6.6 Host Grouping

A single Compute deployment can be partitioned into logical groups for performance or administrative purposes. OpenStack uses the following terms:

Host aggregates - A host aggregate creates logical units in a OpenStack deployment by grouping together hosts. Aggregates are assigned Compute hosts and associated metadata; a host can be in more than one host aggregate. Only administrators can see or create host aggregates.

An aggregate's metadata is commonly used to provide information for use with the Compute scheduler (for example, limiting specific flavours or images to a subset of hosts). Metadata specified in a host aggregate will limit the use of that host to any instance that has the same metadata specified in its flavour.

Administrators can use host aggregates to handle load balancing, enforce physical isolation (or redundancy), group servers with common attributes, or separate out classes of hardware. When you create an aggregate, a zone name must be specified, and it is this name which is presented to the end user.

Availability zones - An availability zone is the end-user view of a host aggregate. An end user cannot view which hosts make up the zone, nor see the zone's metadata; the user can only see the zone's name. End users can be directed to use specific zones which have been configured with certain capabilities or within certain areas.

For this deployment there will be 2 availability zone for physical separation.

Services Zone: All Ericsson 5G Core components will be deployed there

Management Zone: Ericsson ENM, NOKIA's CBAM, CBND and FlowOne will be deployed there.

Services zone will have totally 11 servers, the 2 storage/compute nodes, 6 compute nodes and 3 compute/controllers nodes

Management zone will have totally 7 servers and those will be the storage nodes. There will be two host aggregates with 4 and 3 servers respectively:

HA1: With CPU over-commitment ratio 1:1 and it will accommodate CBND, FlowOne and part of ENM

HA2: With CPU over-commitment ratio 3:1 and it will accommodate some components of ENM

3.6.6.7 NCIR Networking

Servers are connected to leaf switches using 100 Gb (4x25 Gb) breakout cables. Leaf-edge connections will be 100 Gb and Leaf-Firewall connection will use 10Gb (underlay) and 40Gb (overlay).

There is no need for spine switch in one rack configuration, leaf uplinks are connected directly to the edge router.

Server-leaf switch connectivity is Layer 2. Layer 3 gateways are configured on leaf switches. Leaf-spine-edge connectivity is Layer 3 routing, both for internal traffic among racks, and external traffic to the edge router.

NCIR supports SR-IOV connectivity including compute node with DPDK. The hardware configurations have two Mellanox ConnectX-4 2x25Gb NICs and one 1 Gb BMC interface. First NIC is used for kernel-based infrastructure traffic including storage. Second NIC is used by the DPDK vSwitch for VNF traffic. Both NICs are connected to leaf (or ToR) switches. The 1 Gb BMC interface is connected to a separate hardware management switch.

25 Gb ports are combined to active-active bonded interface with LACP per NIC, for redundancy and increased bandwidth.

Link monitoring service monitors both the physical links and the bond interface. Failure of the bond interface triggers auto-evacuation and isolation of the node.

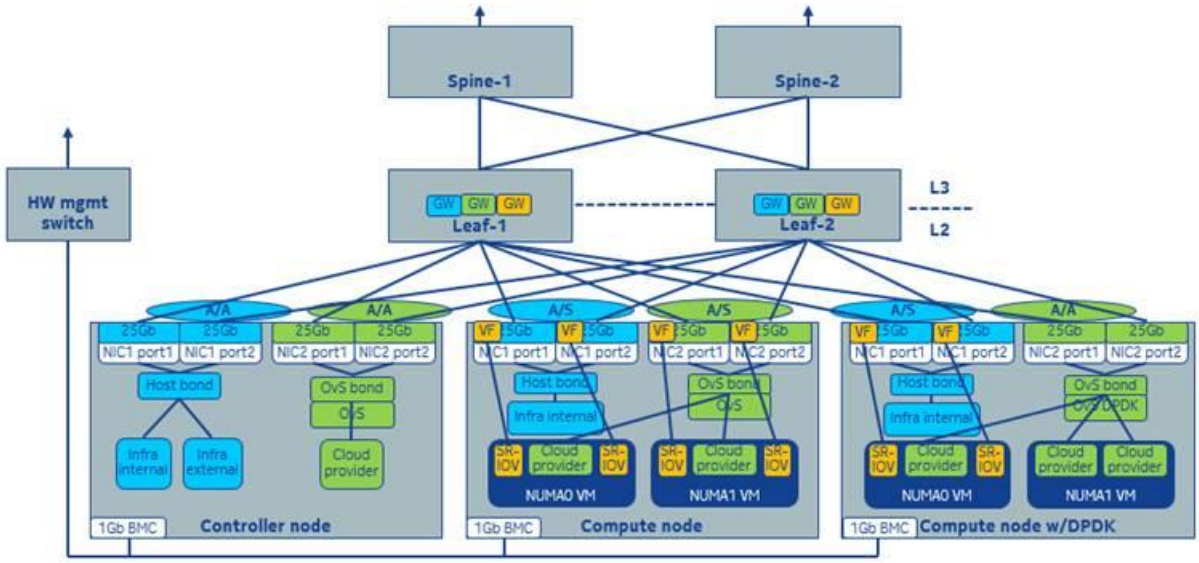


Figure 3.69 : Network fabric architecture

Networks are separated logically and physically for performance and security reasons.

The networks needed for NCIR are listed in the following:

Infra internal

- Internal OpenStack services/APIs
- SSH between OpenStack nodes
- Accessing Ceph from OpenStack services
- NTP between controller and compute nodes
- Deployment (Golden image installation)

Infra external

- External communication/API
- SSH to controllers (host OAM)
- NTP
- Infra DNS
- Deployment (Deployment image installation + IPMI control)
- Infra external needs to be routed to hardware management for deployment

Provider networks

- VM to external communication
- VM to VM communication
- Inter-VNF traffic

Infra storage cluster

- Ceph backend
- Ceph OSD replication

Hardware management

- Out-of-band physical network
- Not directly visible on host OS

The creation of tenant network is not necessary in NCIR.

Storage networking

There are different configuration options for storage in NCIR. In one rack cloud minimum configuration, storage is co-located in the combined controller/compute nodes. In this deployment the compute and storage nodes are co-located.

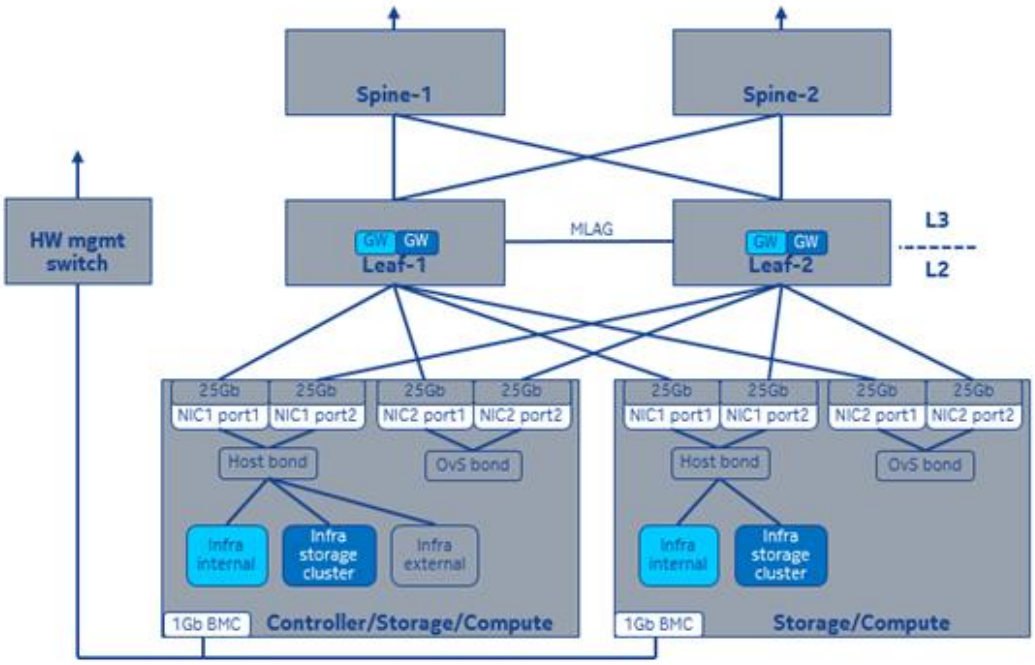


Figure 3.70 : Storage networking

3.6.7 SDN

Nuage Virtualized Services Platform (VSP) is a solution that in combination with Nuage datacenter fabric provides capability to virtualize datacenter network infrastructure and automatically establishes connectivity between compute resources upon their creation. Leveraging programmable business logic and a powerful policy engine, it provides an open and highly responsive solution that scales to meet the stringent needs of massive multi-tenant datacenters.

Nuage VSP is composed of three components:

- **Virtualized Services Directory (VSD)** is a programmable policy and analytics engine. It provides a flexible and hierarchical network policy framework that enables definition and enforcement of resource policies in a user-friendly manner.
- **Virtualized Services Controller (VSC)** is a scalable SDN controller. It functions as the robust network control plane for datacenters, maintaining a full view of per-tenant network and service topologies. Through VSC, network forwarding plane is programmed to establish connectivity for sources.
- **Accelerated VRS (AVRS)** runs inside the hypervisor and removes performance bottlenecks by offloading virtual switching from the networking stack. The CPU resources necessary for packet processing are drastically reduced, so that fewer cores are required to process network traffic at higher rates. AVRS is based on the DPDK technology from 6WIND fully integrated with Nuage VRS and the Linux environment, so that existing Linux applications do not need to be modified to benefit from packet processing acceleration. For the Linux application there is no difference between VRS and AVRS from the end user usage perspective. AVRS supports standard VMs using virtio drivers. AVRS also supports vhost with hugepages for zero-copy packet forwarding.

The Nokia high-level approach to the L2/L3 architecture targets making the L2/L3 network services-driven, i.e. make the transport network consumable and network services automated/abstracted from locations and physical devices. This is achieved through SDN/NFV evolution having "Underlay" and "Overlay" network layers with centralized control as depicted in Figure 3.71.

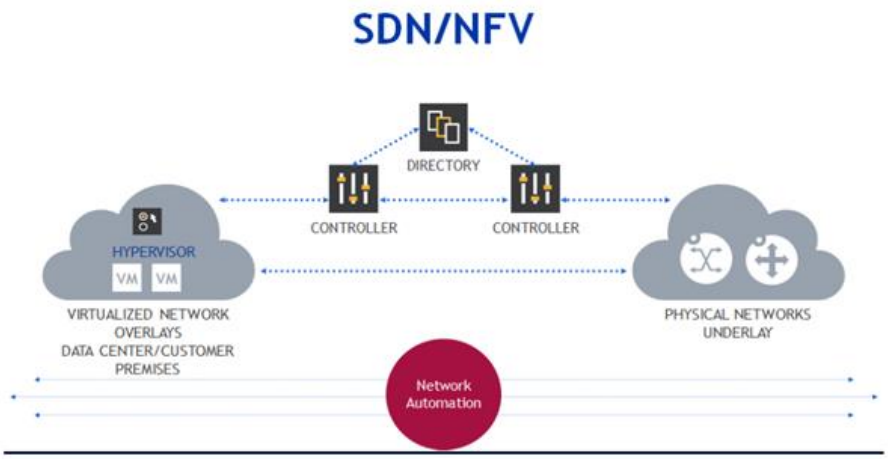


Figure 3.71 : Illustration of "Underlay" and "Overlay" network layers

The Nokia SDN solution is therefore tightly integrated with the AirFrame Data Center Hardware, the Data Center Fabric solution and the physical routing platforms.

The Nokia SDN proposal is based on Nuage solution. Our solution meets the requirements of modern datacenters by offering simplified IP fabric model, for easier operation and higher performance, together with overlay control plane operation for automated provisioning and better control on service availability. As the overlay control layer – the SDN control layer – complements the physical IP forwarding plane and manages the end-end connectivity of server connectivity, internal and external to datacenter, many of the functional requirements of traditional datacenter

Specifically, the Nuage solution combines the benefits and interoperability of BGP MPLS/VPNs with the programmability of Software Defined Networks (SDN). The Nuage Networks solution delivers automation, simplicity, programmability, and interoperability. A proven IP/MPLS networking toolset enables the extension of carrier-grade attributes associated with IP VPN services throughout the Cloud Infrastructure and allows the merger of new and existing datacenters through seamless and robust VPN services.

The Nuage Networks Virtualized Services Platform (VSP) has been designed using open standards such as OVS-DB, OpenFlow, and BGP E-VPN. The only requirement the overlay has of the underlay is it provides basic IP connectivity so every vendor (including even legacy hardware) is guaranteed to be compatible.

- It is based on the same SROS operating system as the Nokia 7750 Service Router (SR) family.
- It enables the dynamic and automatic provisioning of L2 and L3 services within the datacenter as well as across datacenters and existing IP VPN services.
- It introduces a distributed policy management approach, which brings a solution to the service provisioning problem.
- It is standards based and does not use any proprietary protocols.

3.6.7.1 Product details

As mentioned, Nuage Virtual Service Platform (VSP) is composed of three elements, the VSD, the VSC and VRS/AVRS as illustrated in Figure 3.72.

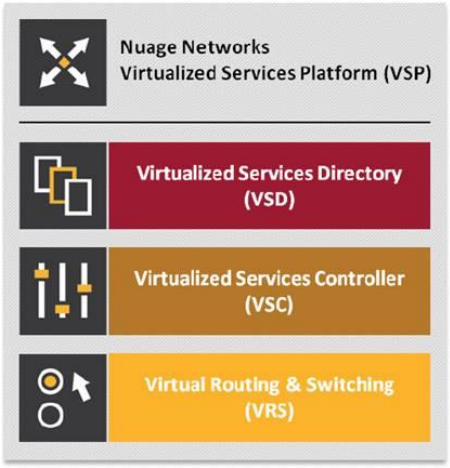


Figure 3.72 : Nuage Virtual Service Platform (VSP)

Virtualized Services Directory

The Virtualized Services Directory (VSD) resides in the Management Plane of the datacenter and provides the business and application logic that is distributed to the VSC as network configurations. The VSD is a programmable policy and analytics engine.

It provides a flexible and hierarchical network policy framework that enables IT administrators to define and enforce resource policies. It is a programmable policy and analytics engine on which service chain policies can be architected.

The VSD contains a multi-tenanted service directory which supports role-based administration of users, compute, and network resources. It manages network resource assignments such as IP and MAC addresses The VSD can be deployed as a standalone or clustered solution depending on scaling needs.

The VSD supports RESTful API's for communicating to the Cloud Providers management systems.

VSD represents event-driven policy management layer which enables zero-touch endpoint policy pull network provisioning driven by the creation of compute and storage resources in cloud management systems:

- Network primitive abstractions for policy creation of Connectivity (L2 and L3 VPN)
- Security
- Quality of Service
- Statistics collection and thresholding
- Service chaining
- Role based user access for tenant self-administration and creation of network connectivity
- Complete integration into cloud management systems o OpenStack, VMware, Cloudstack.

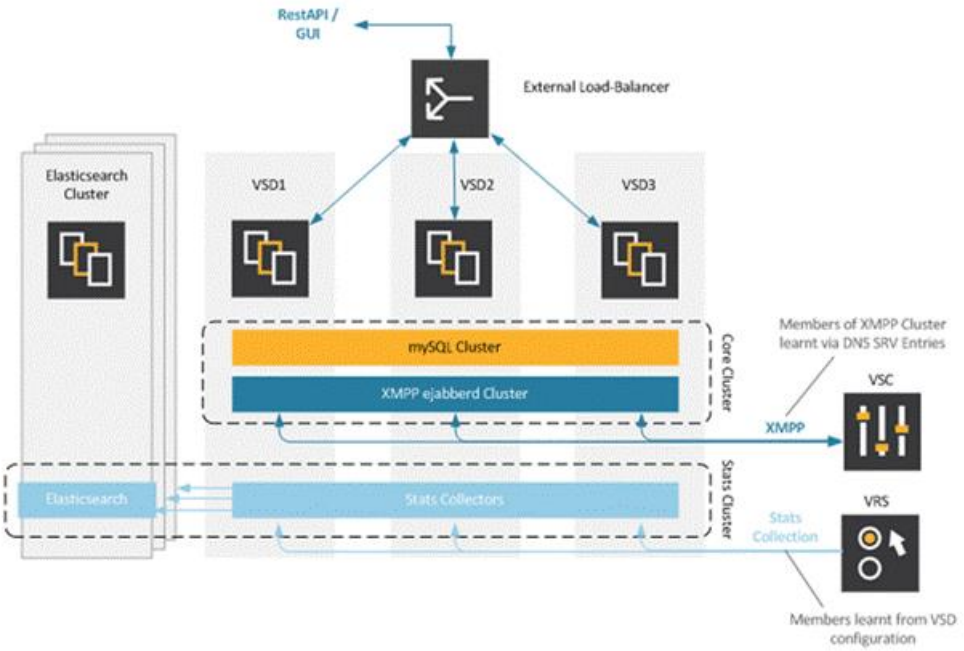


Figure 3.73 : Nuage Virtual Service Platform (VSP) architecture

One VSD entity may consists out of a cluster of 3 VSD VMs and 3 VSD Elastic Search VMs, which for High Availability reasons need to be hosted on 3 different physical servers. For 5G-VINNI, VSD will be deployed in a HA mode.

Virtualized Services Controller

The Virtualized Services Controller (VSC) is an SDN controller. It functions as the robust network control plane for DCs, maintaining a full view of per-tenant network and service topologies. The VSC resides in the Control Plane of the datacenter and provides the network control function. It co-ordinates and federates the setup and teardown of the network paths based on compute triggers received from the VRSs on the Hypervisors. Through the VSC, virtual routing and switching constructs are established to program the network forwarding plane using the OpenFlow™ protocol. Multiple VSC instances can be federated within and across DCs by leveraging MP-BGP—a proven and highly scalable network technology.

It efficiently passes these event triggers to the VSD via Extensible Messaging and Presence Protocol (XMPP) to query the authenticity and to get the application/tenant specific network configuration template to instantiate on the VRSs within the application domain.

The VSC has three main communication directions:

- Northbound: to the VSD via XMPP
- East/West: federation functions to other VSCs or IP / MPLS Provider Edge nodes via MP-BGP
- Southbound: to the VRSs via OpenFlow.

VSC is an SDN controller that programs the VRS endpoint forwarding tables via OpenFlow.

The VSC may consist of 2 VMs per NCIR cluster in an Active/Standby topology. In the 5G-VINNI Norway facility site VSC is deployed in HA mode (2 instances onsite).

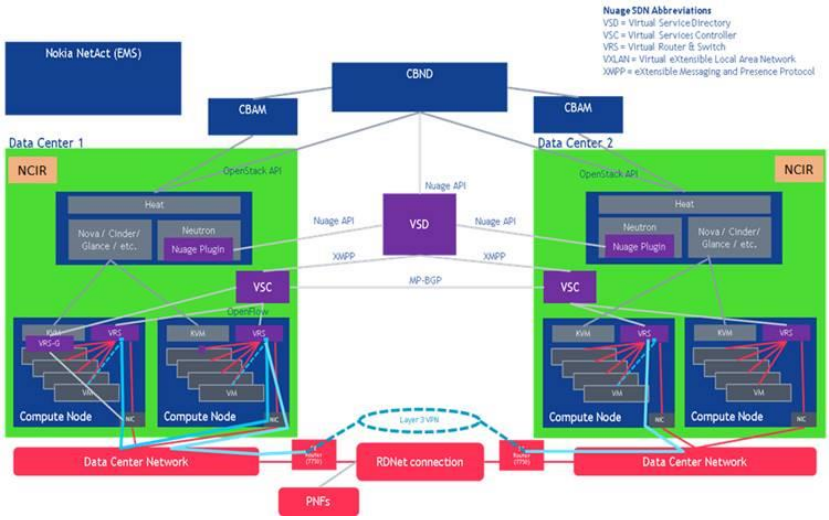


Figure 3.74 : Deployment of VSD and VSC

It is required to have the VSD and VSC operational as precondition to the CBIS overcloud installation. As such we need to host these Nuage components outside the NCIR cluster on dedicated servers. Both VSC and VSD will be deployed in a non-HA mode, thus one server (KVM) will be assigned for their deployment.

3.6.8 Firewalls

Physical firewalls will be used in Release 0 - Release 2. Virtual firewalls and the implementation of Security as a Service is considered for later releases. Further details on the virtual firewall will be specified later.

3.7 Defence Edge Cloud - NFVI and VIM

At the edge site of 5G VINNI the cloud infrastructure layer will be provided by NOKIA:

- **Hardware:** OpenEdge 19 (OE19) servers and rack
- **Networking:** Airframe Z9100 ON Leaf switch
- **Virtualization/VIM:** NCIR 19 FP2 (Openstack Rocky)
- The MANO components will be in Central site but they will be used for onboarding the VNFs in Edge site.
- **G-VNFM**: CBAM 19.5 (SOL001, SOL003)
- **NFVO**: CBND 19.5 (SOL003, SOL005)

3.7.1 NFVI

The Nokia Data Center Solution is based on ETSI reference model and aims at a modular and layered architecture with clear roles for each component. For the edge site, hardware is based on Nokia OpenEdge OE 19, that's is for servers and storage. Networking will be AirFrame Z9100 with 32x100Gb ports and VIM is NCIR 19.

It's an SDN-less solution, so networks will be managed by Openstack Neutron, which is a different solution than the Core site.

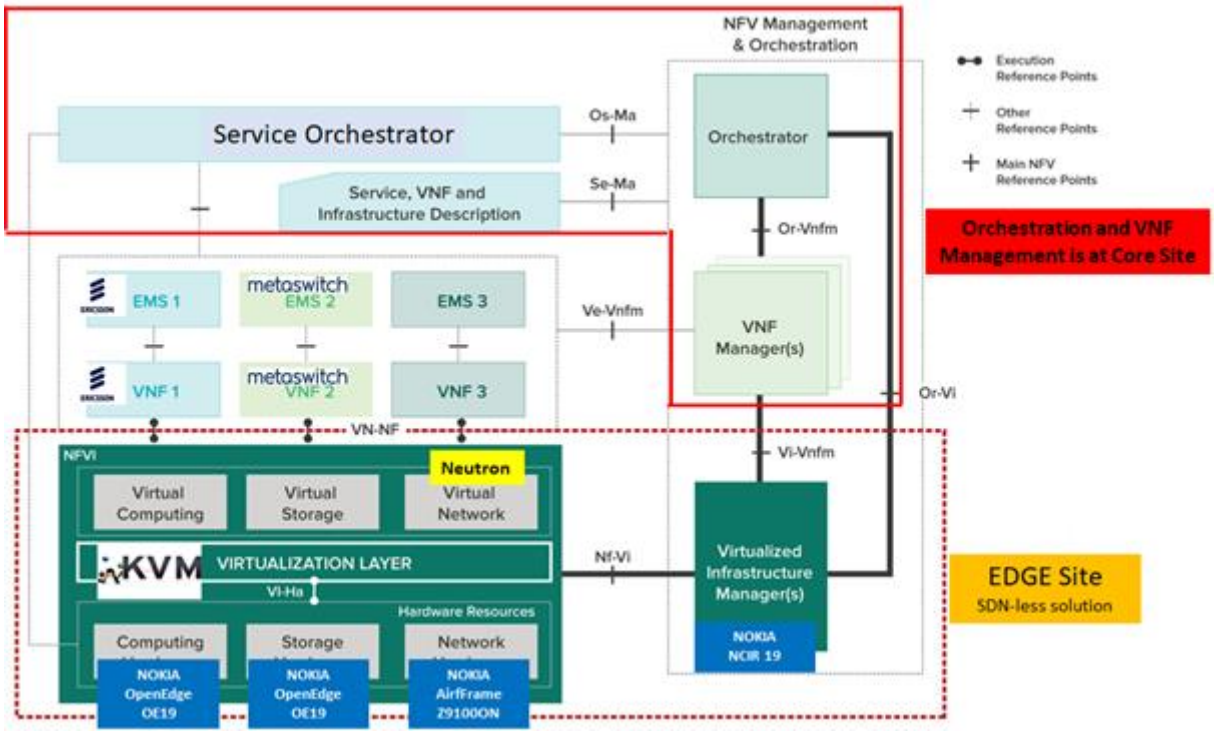


Figure 3.75 : Telenor 5G VINNI Edge Site based on ETSI NFV architecture

Building Blocks

Nokia OpenEdge OE19 uses the following hardware building blocks:

- Rack: provides mounting positions for server, switch, storage and power feed products
- Power shelf: Feeds power from the site power, with 4xAC DC PDUs
- OE Chassis: From 1 to 8 OE chassis can be accommodated in each rack
- Leaf switches: Z9100ON

Equipment Rack

OE compact rack 600x665 (WxD) has 36U height and the below characteristics:

- Both front/back and back/front airflows supported
- 2x DC PDUs or 4x AC PDUs (4 different types)
- Number of OE chassis is 1..8. Each chassis can be individually configured.
- The leaf switch(es) can be either Z9100 or 210WBX
- Dual leaf topology supports max 8 chassis
- Single leaf topology supports max 4 chassis
- Full power and networking cabling as factory integration (later also partial cabling to be supported)
- Max power consumption: 8x 2kW + 2x 0,5 kW = 17 kW
- Weight of a fully equipped rack: 537 kg

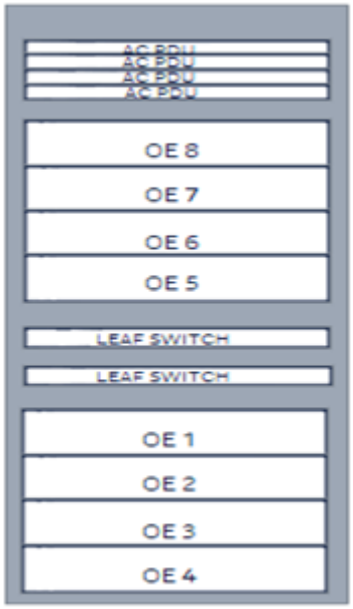


Figure 3.76: OpenEdge Rack

AirFrame Open Edge servers

Each Open Edge chassis has size of 3U and it can have 1U or 2U sleds.

Figure 3.77 : Open Edge chassis 3U with sleds

Figure 3.78 : Open Edge server 1U

Processor (single socket)

- Intel® Xeon® SP, up to 24cores, 2,4GHz

Memory

- DIMM slots: 6 typical (8 max)
- DIMM type: 16GB / 32GB / 64GB - DDR4 RDIMM 2933 MHz

Storage

- 2x 2,5” Hot-plug bays for NVMe and SATA devices 9,5/7mm
- 2x internal M.2 2280 or 22110 devices

Each chassis will have 1U or 2U sleds, 2xAC PSU and 1xRMC unit

Figure 3.79 : Open Edge chassis

Figure 3.80 : Open Edge RMC

Figure 3.81 : Open Edge AC PSU

For 5G VINNI Norway Edge site, it will be one chassis with 5x1U sleds/servers.

3.7.1.1 Hypervisor

The hypervisor is the same as used in the Central Cloud, except that AVRS is not used.

At the centre of NCIR Networking is a DPDK-Open Virtual Layer 2 Switch (OvS), running on the compute node hosts. It provides connectivity between virtual machines on the same compute node, and between virtual machines and external networks.

3.7.1.2 Computing

The OpenEdge servers will be used as compute nodes, controller nodes and storage nodes. Based on dimensioning requirements there will be 5x1U servers, in one 3U chassis.

All the 5 servers will act as compute nodes, 3 of them as controllers too and 2 of them as storage nodes. The allocation will be:

- 2 servers only as compute and storage nodes
- 3 servers as compute and controller nodes

The hardware configuration for the compute nodes is.

Table 3.13 : Edge Cloud compute server configuration

Compute nodes	Configuration
Server/Processor	AF 6212U Intel processor 24c 2.4GHz 165W (single socket)
Memory	6x32GB = 192GB (DDR4) RAM
Network	Totally 4 ports x 25Gb: 1 x AF 25GbE dual port OCP NIC card CX5 (2x25 Gb) 1 x AF 25GbE dual port LP-MD2 NIC card CX5 (2x25 Gb)
Storage	1 x AF SSD 480GB SATA 1dwpd M.2 2280* * In case of controllers and storage nodes we will have more disks allocated.

NCIR19 will require vCPU resources and this depends on the server role. As mentioned above, in this deployment we expect each server to act as in one of the below roles:

a) Compute and Controller
b) Compute and Storage

Host CPU isolation, it partitions physical CPUs between host system tasks (including OpenStack services) and virtual machines in order to protect critical system tasks from potential malfunctions, especially when a high load performance is required.

Dedicated CPU resources are allocated to host system services (OVS, Ceph, interrupt handling, SW agents, etc.). Those host resources are excluded from pool available for virtual workloads in nova scheduler.

Host CPU isolation is supported by NCIR and this is configurable. The number must be a multiplication of the CPU hyper threading configuration which is usually two.

NCIR allows configurable allocations of CPUs in three distinct allocation pools:

- Middleware CPUs for host processes (OS and Nokia middleware)
- OVS-DPDK CPUs for Poll mode threads
- VM CPUs

In nodes that have compute services, platform CPUs and OVS-DPDK CPUs are configured. The rest are allocated to the VM CPUs.

An example of the core allocation is the following:

- Middleware CPUs: 2 cores (4 threads)
- OVS-DPDK: 2 cores (4 threads) as minimum requirement.

In a hybrid solution, where compute and storage nodes exist together, physical resource separation is needed to guarantee the unobstructed functionality on high load situations.

For OS and Ceph configurations with two OSD disk, the platform requires: 1 additional cores (2 threads if HyperThreading is enabled) and additional memory.

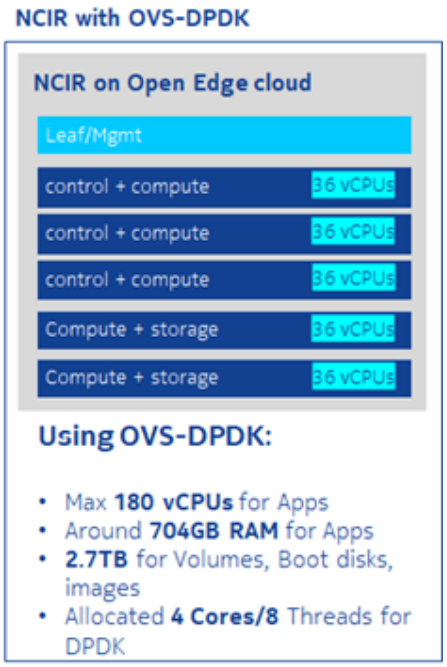


Figure 3.82 : Compute node's CPU isolation

There will be reserved 64GB memory in each controller node and 32GB for compute/storage node for the host, all rest is available for VNF use.

3.7.1.3 Physical Network

For 5G-VINNI Edge site it will be one switch to perform as leaf and management switch. Two Airframe Z9100ON switches will be used for resilience. Each OpenEdge chassis, using its RMC port, will be connected to one of the SFP+ port in Z9100 for management. That's a 10Gb connection.

Z9100 has also 32x100Gb ports for connectivity to the servers and uplinks.

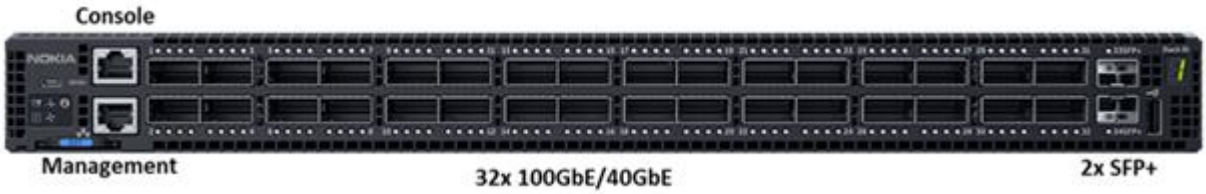


Figure 3.83 : Z9100 ON switch as Leaf and Management switch

Each OE chassis has one RMC (P5) and up to 5 servers with 4x25Gb ports (P1,P2,P3,P4).

Figure 3.84 : OE19 Chassis networking ports

Airrame Z9100 ON will take the role as Leaf and Spine switch in the IP Fabric architecture as well as the datacentre gateway.

The leaf switch is high performance and low latency L2/3/4 Ethernet switch with 32 QSFP28 ports in a 1U form factor. It provides connections between external networks and server nodes. Each QSFP28 port can be independently configured as 100GbE, 2 x 50GbE, 1 x 40GbE, 4 x 25GbE or 4 x 10GbE.

In Edge site, each QSFP port will have a splitter to 4x25Gb towards compute server's ports.

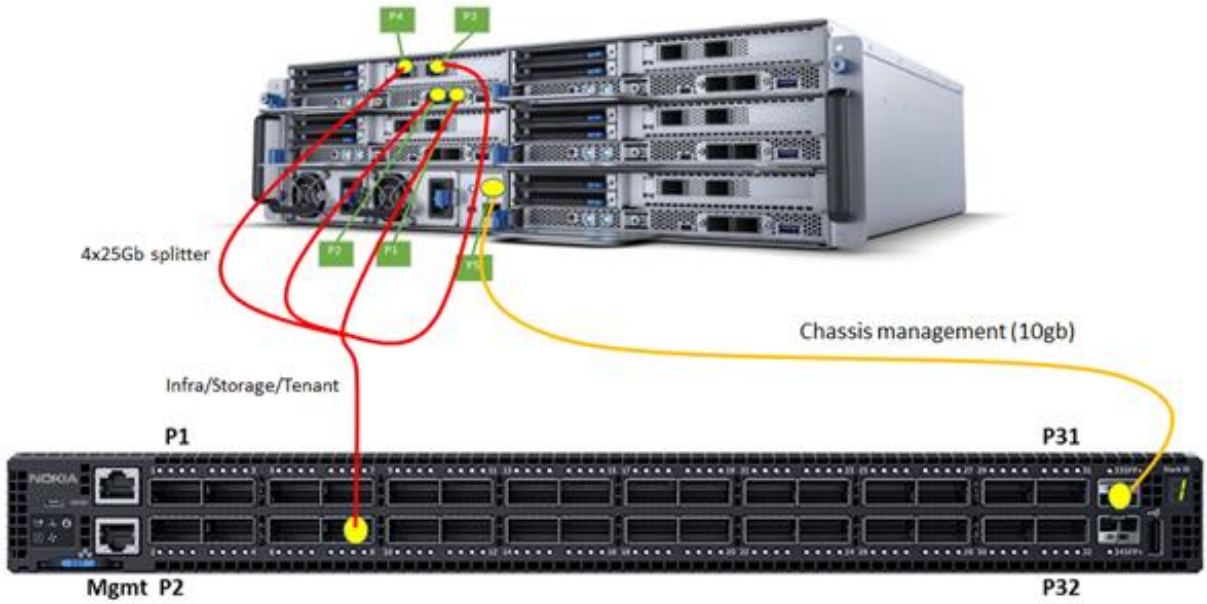


Figure 3.85 : Server connectivity using 4x25Gb splitter

Physical ports:

- 32 x 100GbE QSFP+ ports
- Supports various port breakout (100GbE, 2 x 50GbE, 1 x 40GbE, 4 x 25GbE or 4 x 10GbE)
- 2 x SFP+ ports

High availability

- Redundant hot-swappable power supply 1+1
- Hot-swappable fan tray N+1

Features

- MLAG
- OSPF, BGP4, ECMP
- VXLAN
- VTEP for L2 and L3

Each compute node is equipped with two NICs, each supporting 2 x 25Gbps ports. Compute node is connected to the leaf switch in the rack.

NIC1: It's used for kernel-based infrastructure traffic including storage

NIC2: It's used by the OVS-DPDK switch for VNF traffic

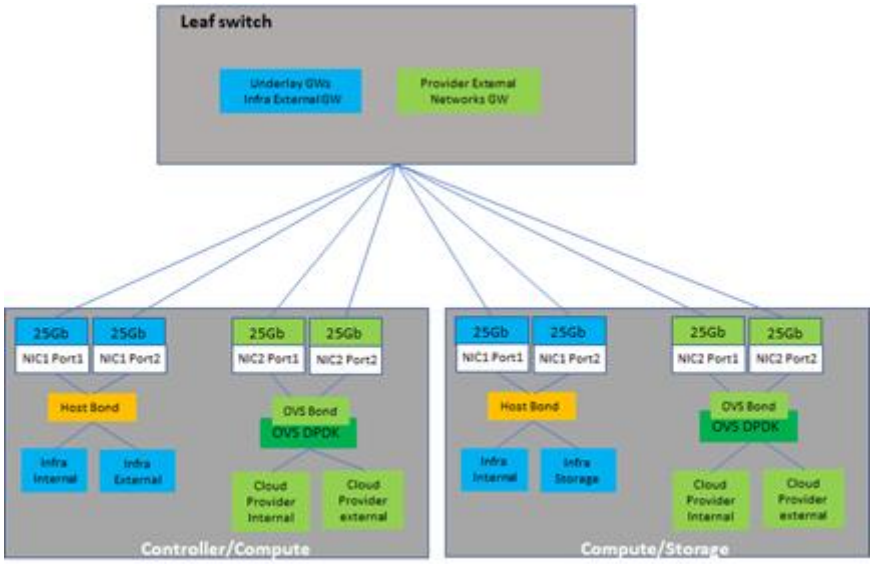


Figure 3.86 : Connectivity from compute servers to the leaf switch

3.7.1.3.1 Edge site External Connectivity when connecting DC Switches to CSR or CE router

There are no separate spine switches in this deployment (one rack solution), so 100Gb speed ports will be used to interconnect the leaf-switch towards the CSR or the Customer Edge (CE) router. In this setup the single switch takes the role of aggregator-router, leaf and spine switches. There is no requirement for resilience on CSR/CE router, so the leaf switch will be connected to one router using two different ports to secure the redundancy. The CSR/CE router is provided by Telenor. The connectivity between datacentre and the CSR/CE router is illustrated below. There is no resilience on node level, but it could on port level, for example connecting CSR/CE router and Z9100 switch with 10 Gb ports.

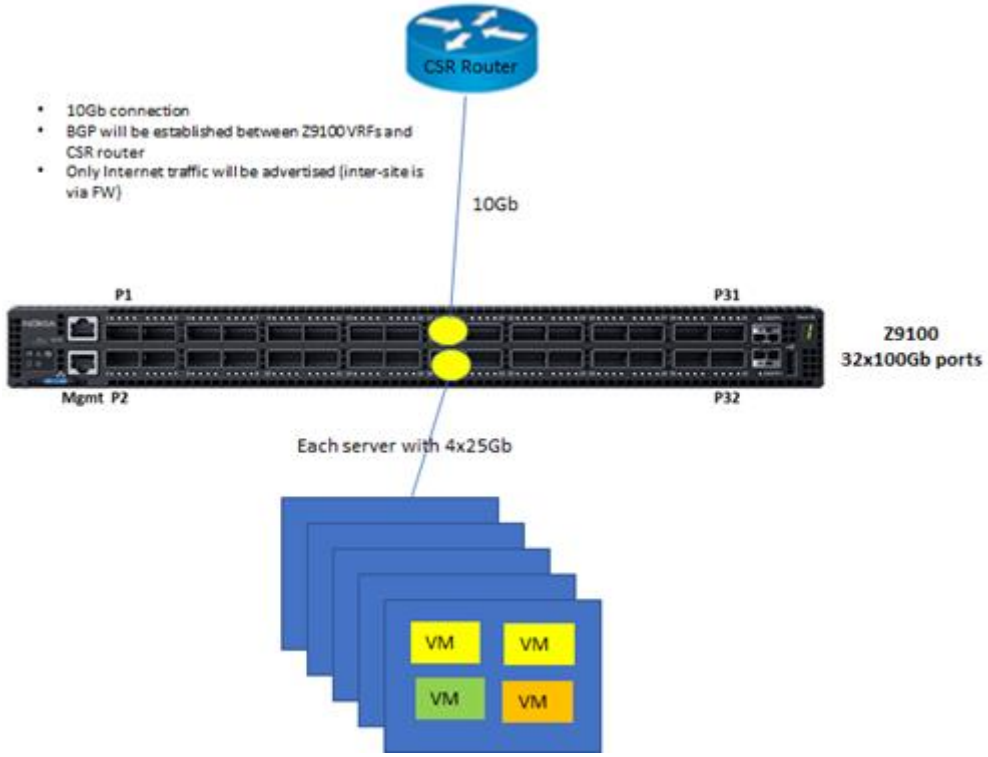


Figure 3.87 : CSR uplink connectivity from Z9100

Only internet traffic will be done via the CSR/CE router as below:

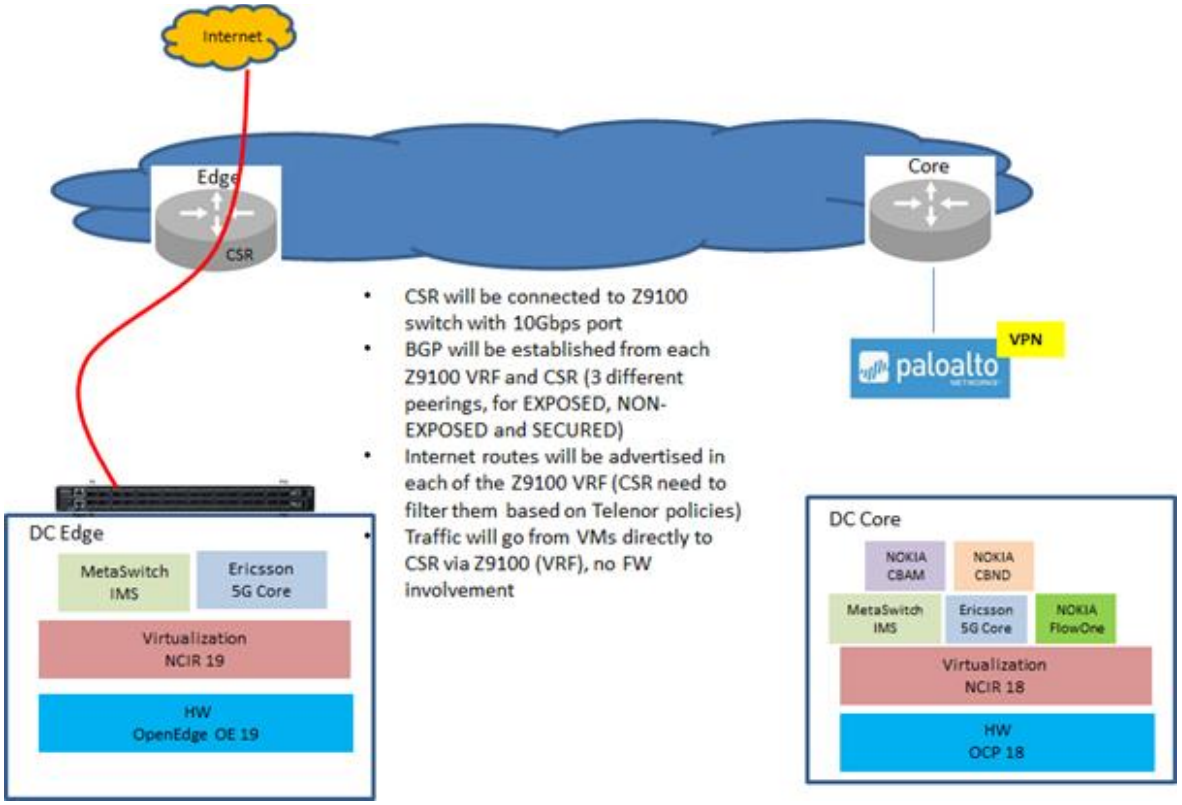


Figure 3.88: Overlay traffic to internet

The Z9100 switch will be connected also to PaloAlto FW for underlay and overlay traffic. Overlay traffic will cover inter-security class traffic (eg from EXPOSED to NONEXPOSED) and inter-site overlay traffic.

Physically it will be a 10Gb connection between FW and Z9100 switch and multiple VLANs will be used for the different traffic scenarios, such as BGP, underlay and overlay. Several VRFs will be configured in both sites and routes will be advertised by BGP.

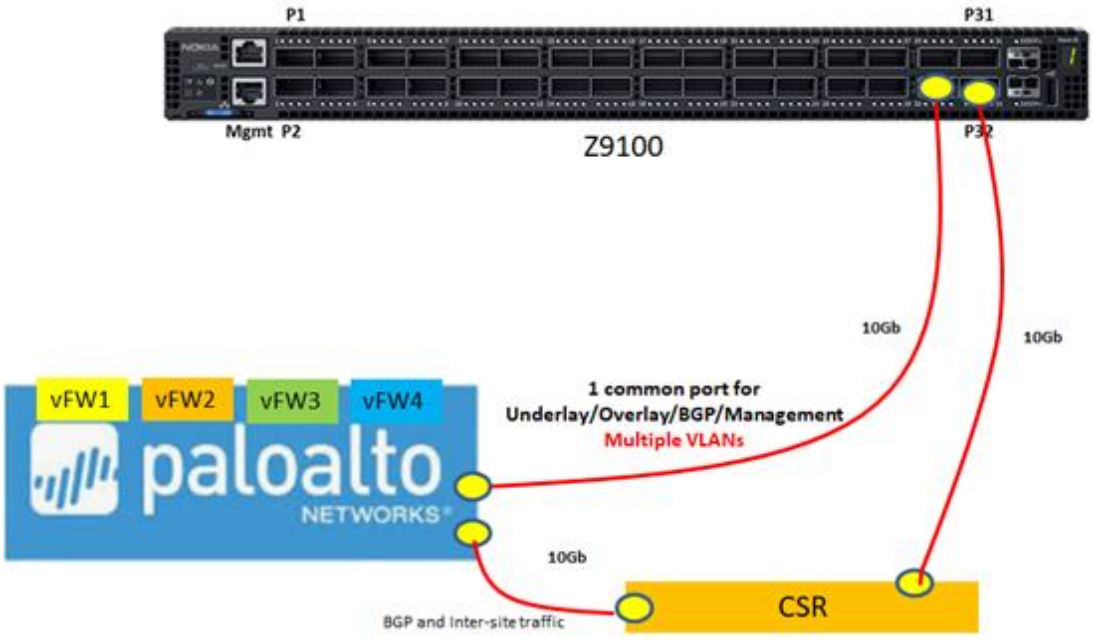


Figure 3.89: Physical connectivity between Z9100 and FW and CSR/CE

3.7.1.4 Storage

3.7.1.4.1 Storage Architecture

CEPH will be use as backend storage at the Edge, same as in Core site.

Cinder attached volume is mounted through CEPH-RBD. Same applies for VM root disk (ephemeral) which is also mounted through CEPH-RBD

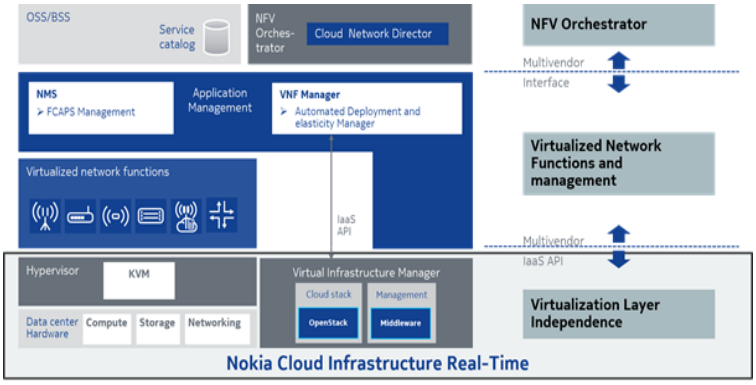


Figure 3.90: CEPH's clients

The CEPH clients are Cinder, Nova and Glance, for which the following settings will apply:

- Cinder Back End volumes will be attached through Ceph RADOS Block Device (Ceph-RBD).
- The VM root disk (ephemeral) will be mounted through Ceph-RBD.
- Images will also be stored in Ceph due to limited capacity of local disks .

3.7.1.4.2 Storage Implementation

When planning out the cluster, a number of considerations must be balanced, including failure domains and potential performance issues.

Compute nodes can contribute their disks in the CEPH storage cluster for the hyper-converged implementation or there is an option to dedicate several of the servers to act as storage nodes.

The Ceph deployment in the Norway Edge site is a hybrid hyper-converged solution for compute and storage servers.

The same type of Airframe OpenEdge servers is used for storage (and compute as well). In total we have 2 storage servers with 2x Data OSD disks in each one. Their hardware configuration is below:

Table 3.14 : Storage server configuration

Compute and Storage nodes	Configuration
Server/Processor	1 x AF 6212U Intel processor 24c 2.4GHz 165W (single socket)
Memory	6x32GB = 192GB (DDR4) RAM
Network	Totally 4 ports x 25Gb: 1 x AF 25GbE dual port LP-MD2 NIC card CX5 1 x AF 25GbE dual port OCP NIC card CX5
Storage	2 x AF SSD 1.92TB SATA 3dwpd 2.5 inch 1 x AF SSD 480GB SATA 1dwpd M.2 2280

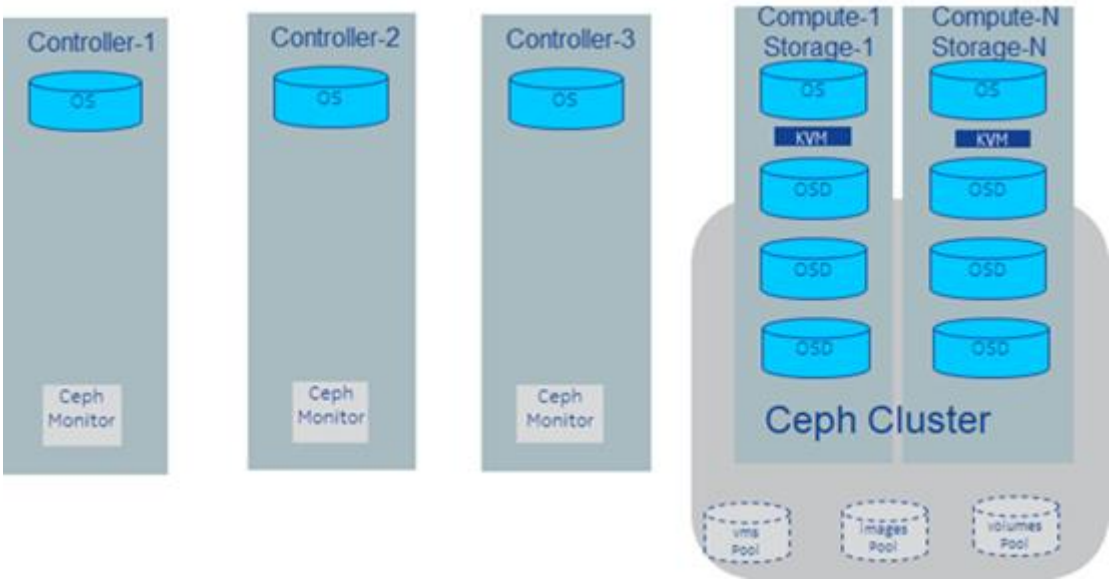


Figure 3.91 : CEPH cluster

The net storage requirements are 2.3 TB, which means the gross storage should be higher considering the data replication ratio.

CEPH and its CRUSH algorithm distributes objects and their replicas to OSDs. The number of replicas can be set, but it's recommended to have at the least the same number of storage servers.

Table 3.15 : Ceph replication factor for Edge Cloud

Settings	Description
CEPH Replication factor: 2	Each CEPH cluster should have a minimum of 2 Storage Servers, which is the case at the Edge Site. This is due to the CEPH replication factor of 2. Data will always be stored in 2 different servers for high availability

For the Norway Edge site deployment the allocation is:

- 2 servers to act as storage nodes (OSDs will reside there)
- 3 monitors that reside in the same servers with the controllers
- 4 disks for OSD data (2 disks in each server)

Table 3.16 : Ceph disk configuration for Edge Cloud.

Disk category	Description
OS/Boot disk	1 x SSD disk will be used for Host OS in each storage servers
OSD	Two 1.92 TB SSD disks will be used as OSD in each storage server. It will be totally 2 Disks x 2 Servers x 1.92TB raw data.

There are only 2 storage servers, so if one server fails, there will always be a backup in the surviving storage server, but CEPH monitors will not be able to create more copies in order to satisfy the need of 2 replicated copies. If a storage server fails then the problem will need to be rectified as soon as possible.

3.7.2 VIM

At the edge site only NCIR 19 VIM will be deployed and VNFM/NFVO from Core/Central Cloud site will be reused.

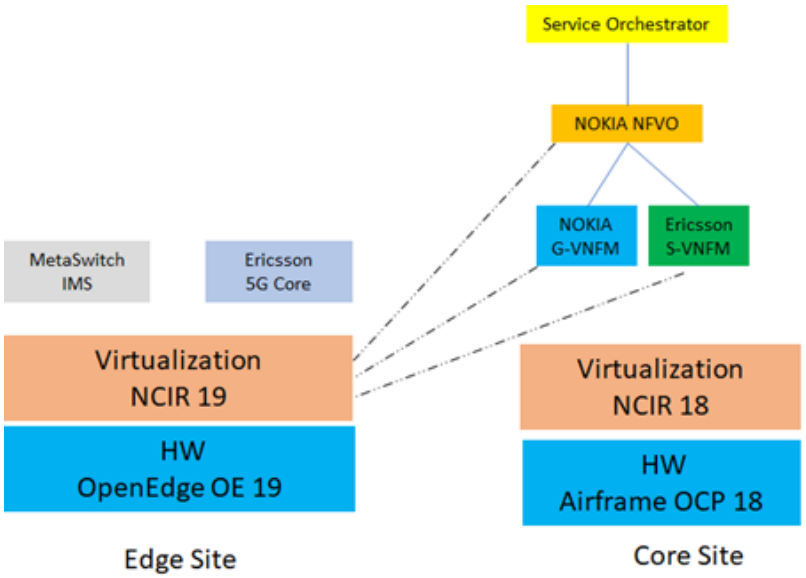


Figure 3.92 : New integration points from VNFM/NFVO at Core site

Ther VIM is Nokia Cloud Infrastructure Real-time (NCIR) as described for the Central Cloud site and the configurations are similar. Currently NCIR uses OpenStack Rocky, August 2018 baseline, and integrates the components/services listed below:

Table 3.17 : OpenStack software versions for Edge Cloud.

OpenStack components¶	
aodh	7.0.0
cinder	13.0.6
glance	17.0.7
horizon	14.0.2
ironic	11.1.2
keystone	14.0.1
neutron	13.0.2
nova	18.2.1

No SRIOV requirements exists for Edge site. All VMs will use DPDK-OVS.

3.7.2.1 Networking for Edge connected to CSR

Servers are connected to leaf switches using 100 Gb (4x25 Gb) breakout cables. Leaf-Firewall connection will use 10Gb and the same for Leaf-CSR router.

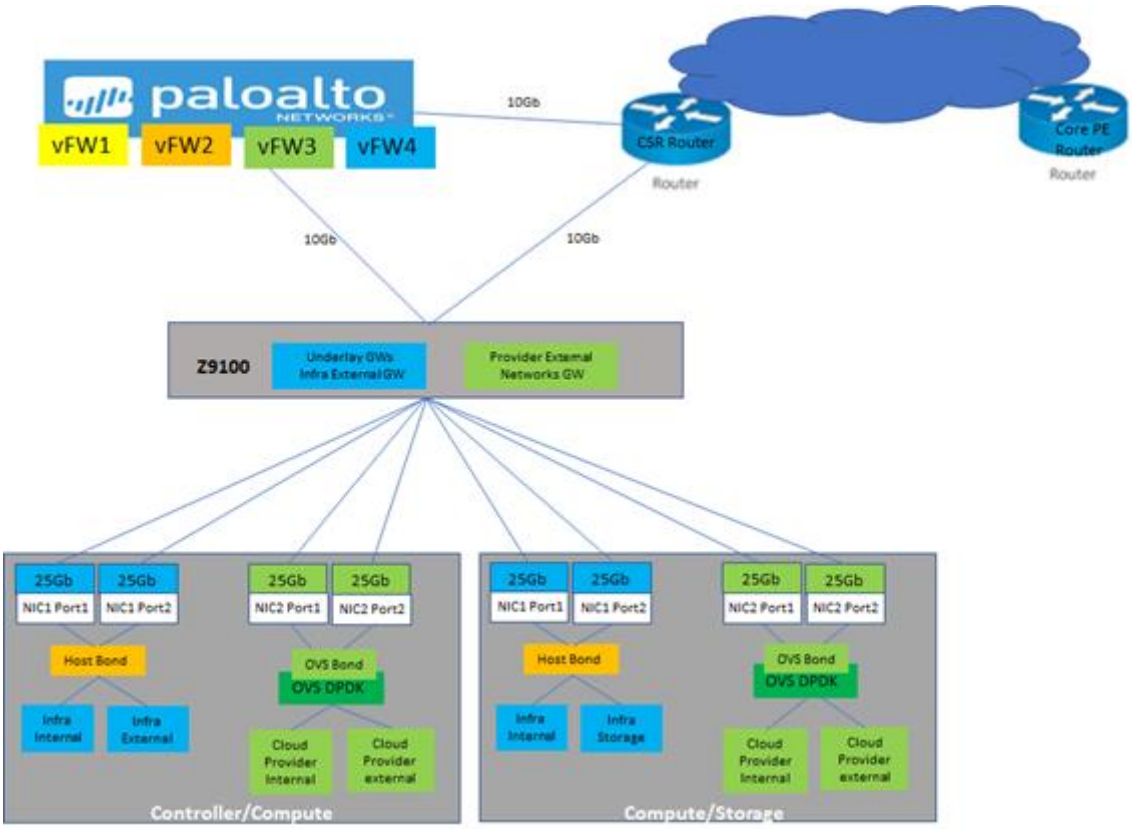


Figure 3.93 : NCIR connectivity to leaf switch

There is no need for spine switch in one rack configuration, leaf uplinks are connected directly to the edge CSR router.

Server-leaf switch connectivity is Layer 2. Layer 3 gateways are configured on leaf switches. Leaf-edge CSR connectivity is Layer 3 routing, for external traffic to the edge router (internet).

NCIR supports SR-IOV connectivity including compute node with DPDK. The hardware configurations have two 2x25Gb NICs, first NIC is used for kernel-based infrastructure traffic including storage, second NIC is used by the DPDKvSwitch for VNF traffic. Both NICs are connected to leaf (or ToR) switches. The OE19 server module has also a 10Gb interface for management that is connected to Z9100.

The 25Gb ports are combined to active-active bonded interface with LACPper NIC, for redundancy and increased bandwidth.

Link monitoring service monitors both the physical links and the bond interface. Failure of the bond interface triggers auto-evacuation and isolation of the node.

Networks are separated logically and physically for performance and security reasons.

The networks needed for NCIR are listed in the following:

Infra internal

- Internal OpenStack services/APIs
- SSH between OpenStack nodes
- Accessing Ceph from OpenStack services
- NTP between controller and compute nodes
- Deployment (Golden image installation)

Infra external

- External communication/API
- SSH to controllers (host OAM)
- NTP
- Infra DNS
- Deployment (Deployment image installation + IPMI control)
- Infra external needs to be routed to hardware management for deployment

Provider networks

- VM to external communication
- Tenant internal communication (VM to VM)
- Inter-VNF traffic

Infra storage cluster

- Ceph backend
- Ceph OSD replication

Hardware management

- Out-of-band physical network
- Not directly visible on host OS

Tenant networks

- Tenant internal communication (VM to VM)
- They are provisioned by the tenants

Storage networking

There are different configuration options for storage in NCIR. In one rack cloud minimum configuration, storage is co-located in the combined controller/compute nodes. In this deployment it's compute and storage nodes co-located.

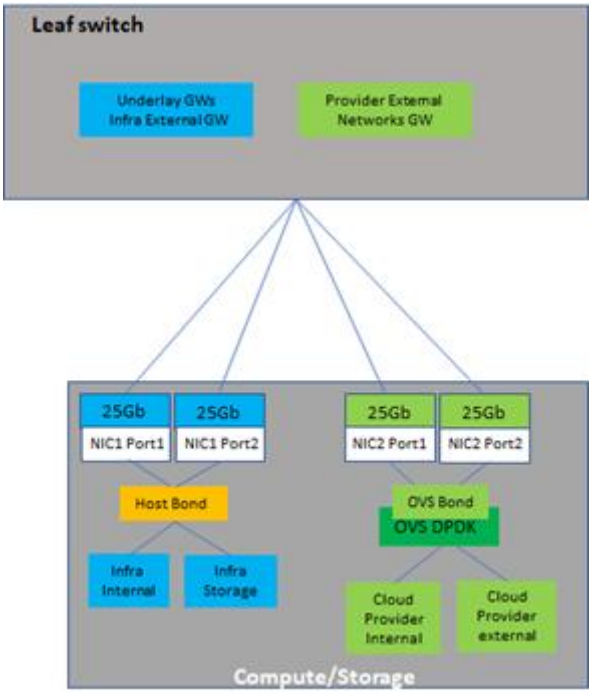


Figure 3.94 : Compute server connectivity to leaf switch

Telenor will assign VLANs for the different types of networks. The VLAN range is dependent on applications needs. Below is an indicative allocation, which can be adjusted based on the expected requirements:

- **0-512:** for underlay network and P2P connection (eg FW-Z9100, CSR-Z9100)
- **1000-1499:** for external provider networks, which are created by the provider (admin). Due to security requirements and isolation, further VLAN allocation needs to be done for each Z9100 VRF
- **1500-1999:** for internal/tenant networks, which will be assigned automatically to the users
- **2000- :** for other purposes.

For security reasons, three different security classes are used in the Norway facility site, such as EXPOSED, NON-EXPOSED and SECURED. Inter-class traffic will go via a vFW and intra-class will be routed directly from Z9100. For this reason three VRFs will be configured in Z9100 switch, which will receive other's classes routes via BGP from PaloAlto vFWs.

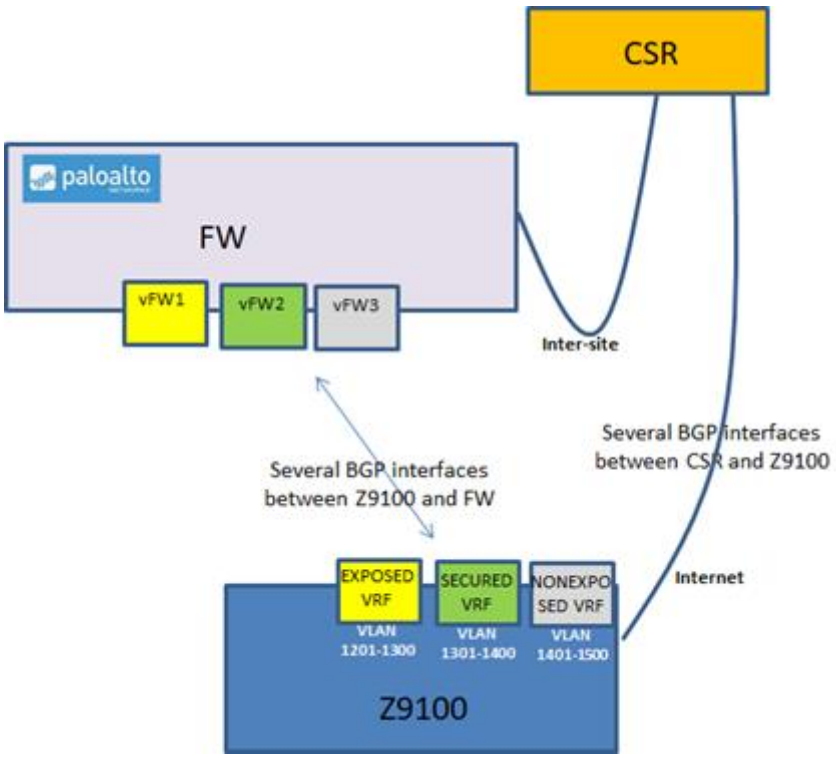


Figure 3.95 : Overlay connectivity

Finally, some VNFs use virtual IPs which has to be shared by several instances. In that case the Z9100 should add a static route with load-sharing between those instances in the corresponding VRF. Usually the virtual IP (eVIP) is provided from different subnet than the instances.

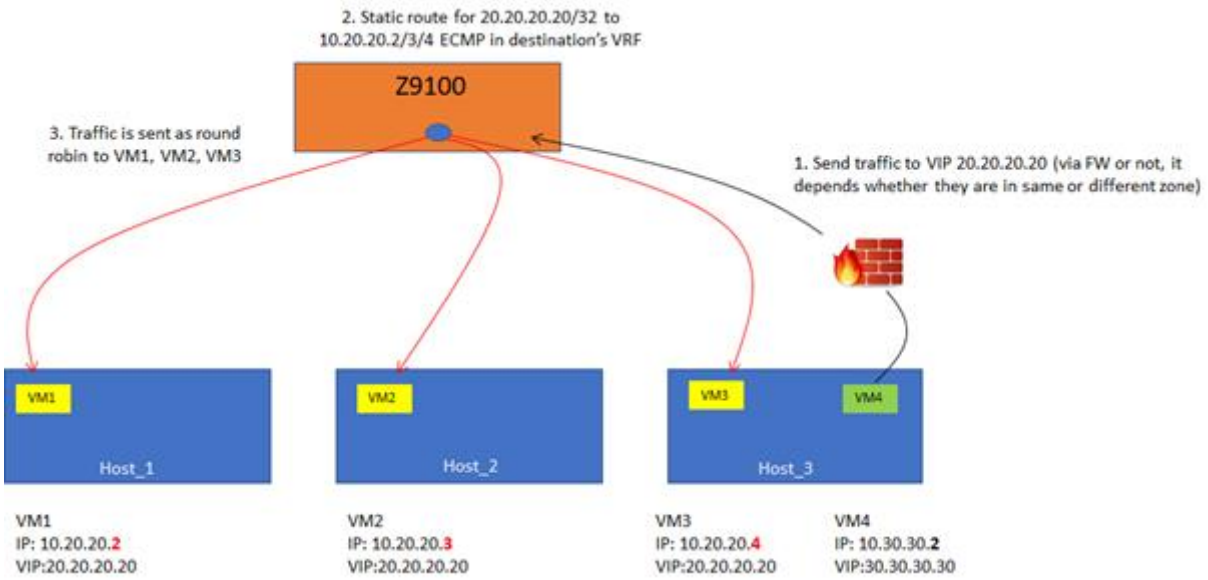


Figure 3.96 : eVIP and VM load-balancing via Z9100 switch

3.7.2.2 Networking for Edge connected to CE/PE

In 5G VINNI Norway Facility we developed two different designs for the connectivity of the Edge with the transport network, via the Provider Edge (PE) and Customer Edge (CE). This design is focused on reusing standard services as used today in the commercial transport network where the Edge and the RAN Part are near but completely separated. The other design, as described in Section 3.7.2.1, contained a common router (the CSR) between the RAN and the Edge in order to have direct connectivity without any PE involvement.

Figure 3.97 illustrate the networking design where the Edge is connected to CE/PE. This design from the transport network point of view allows the independence between RAN and Edge. This design has the advantage of using standard transport network products since RAN is set using the traditional settings, and the Edge is perceived as a traditional customer premises connected to the transport via a CE. In Figure 3.97 the paloalto firewall acts as the CE.

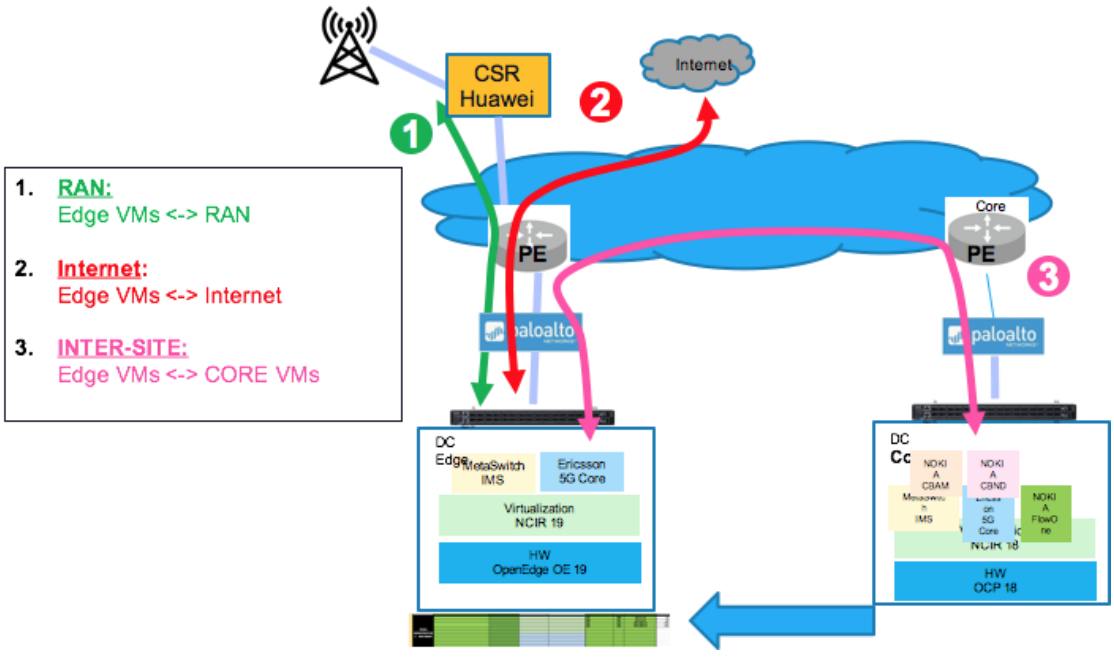


Figure 3.97 : Networking design where the Edge is connected to CE/PE.

Apart from being connected to the CE instead of the CSR, the other design details are similar to what was described in Section 3.7.2.1.

The design for Edge connected to CE/PE will be used initially in 5G-VINNI Norway Facility site since the transport services are available in the commercial transport network today. The design for connecting Edge to CSR is documented here for potential use in a second phase, where the intention is to guarantee performances (e.g. throughput, latency, jitter) regardless of the status of the last mile PE-CE connection.

3.8 Fishfarm Edge Cloud - NFVI and VIM

The cloud infrastructure solution for Fishfarm Edge cloud is similar to the Defense edge site, using OE19 servers and Z9100 switch. In this section, we will describe the differences between those two sites, regarding hardware, infrastructure and networking.

Cageeye/Sealab provide the cameras and analytics service for the Fish Farming site (part of ICT-19 project 5G-HEART).

In Cageeye/Sealab site, we will deploy analytics on the Edge cloud in order to analyse the feedback from the cameras, which monitor the fishes. The output will be sent via the 5G network and CPE to the core network in Central site and from there to Cageeye's central system.

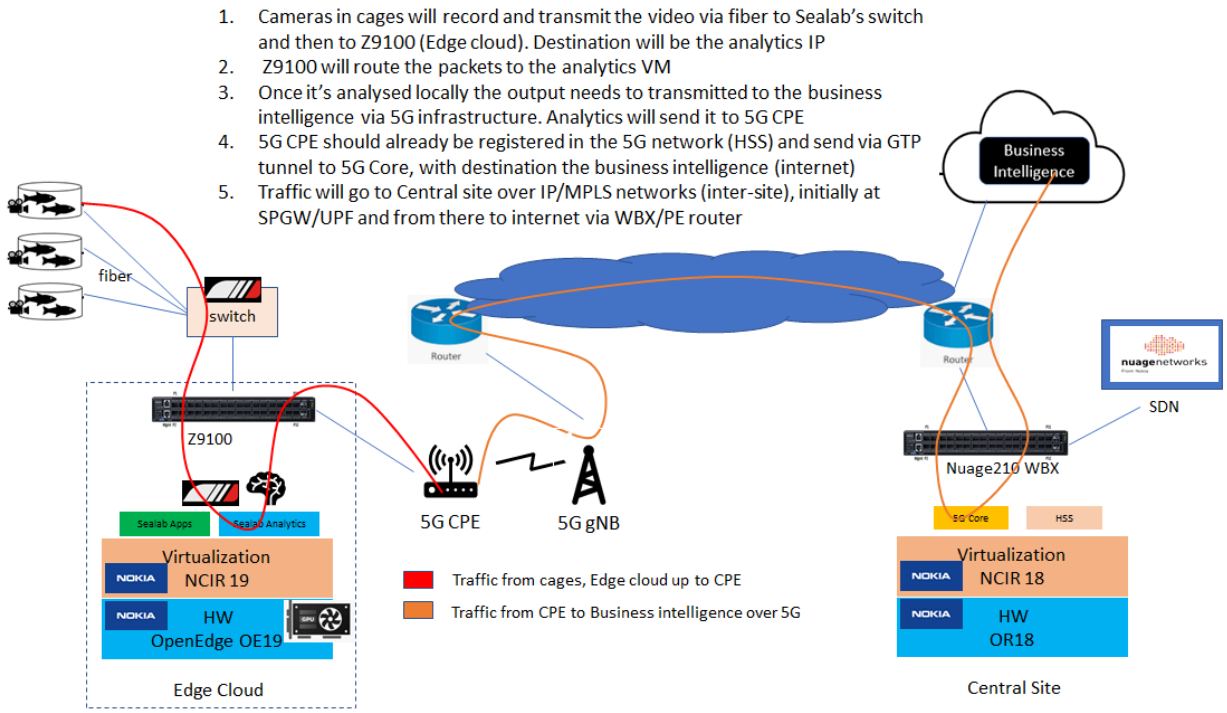


Figure 3.98 : Traffic Flow from analytics in Fish Farm Edge to Business Intelligence in customers' datacenter

Regarding the servers, the only difference between fish farm and defence edge cloud is the need of GPU. Two GPU cards (NVIDIA Tesla T4) are deployed in two of the servers using Tesla T4. Also, each server is using just 1 NIC card (2x25Gbps ports), where the first port is used for the infrastructure and the second port is used for tenant traffic (analytics). Both ports are connected to the Z9100 switch, which can support 32x100Gbps.

The hardware components are shown in Figure 3.99.

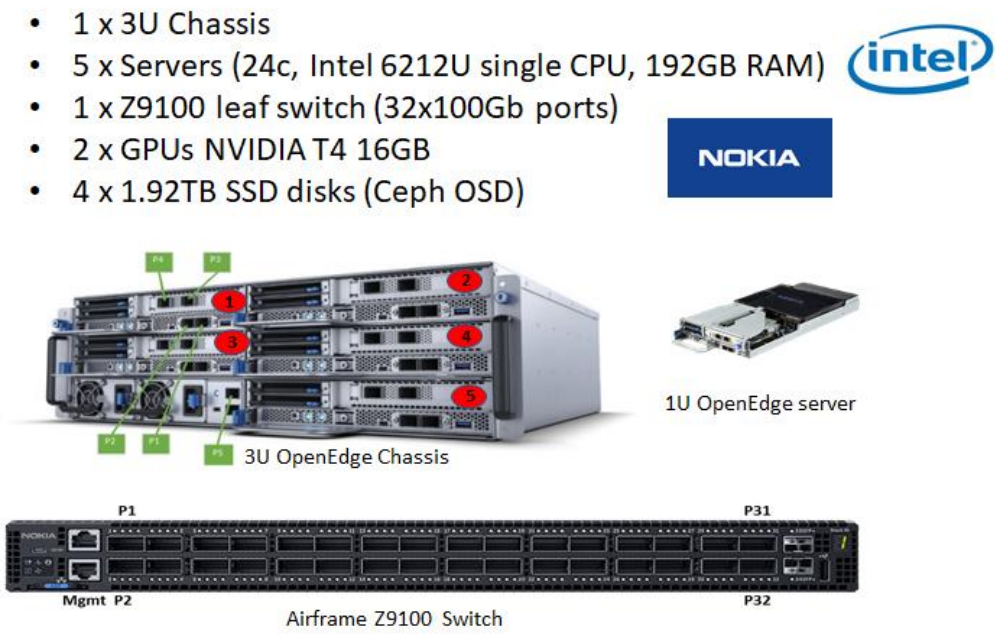


Figure 3.99 : Hardware configuration for Fish Farm Edge.

The solution is using CEPH as storage, with replication ratio of 2 and Nokia virtualization layer (NCIR19), which is based on Openstack's Rocky version.

The NFVI solution in this data centre is shown in Figure 3.100.

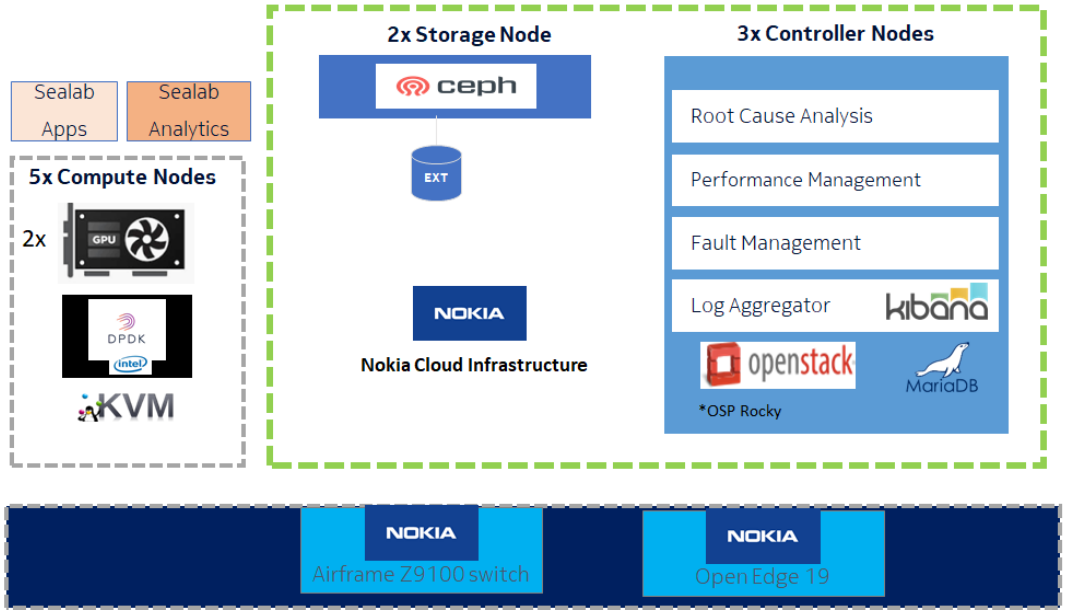


Figure 3.100 : NFVI for Fish Farm Edge Cloud (Nokia Airframe OE19, Z9100 and NCIR19).

For network acceleration, DPDK is enabled by assigning 2 cores from the CPU socket. The available resources in this edge site are 196vCPUs, 704GB RAM and 2.7TB of net storage, which includes images, boot disks and cinder volumes (Figure 3.101).

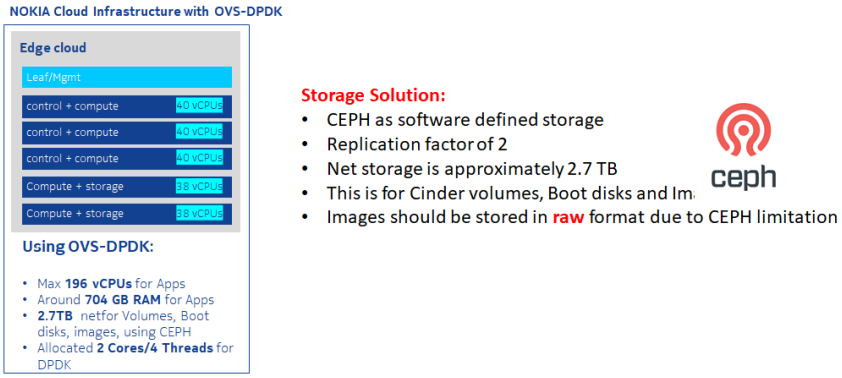


Figure 3.101 : Storage solution for Fish Farming Edge

There will be just one common availability zone for the analytics. There will be two types of VMs, one using GPU and one without.

Nova scheduler can deploy those 2 VMs that require GPU in the two specific servers by using the correct flavor (property pci_passthrough:allias is set to T4_Tesla:1) as shown in Figure 3.102.

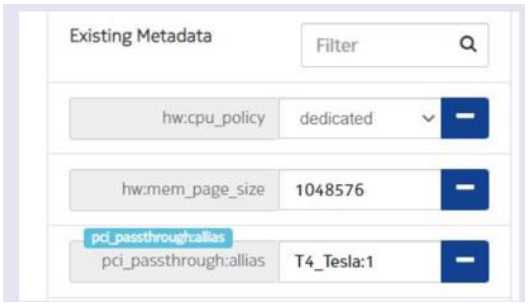


Figure 3.102 : Deployment of VMs in OpenStack on servers with GPU.

For networking, each server has its two ports connected to Z9100. The first one is used for infrastructure internal, infrastructure external and storage networks. The second port is for provider internal and external networks. Networking for Fish Farming Edge is illustrated in Figure 3.103.

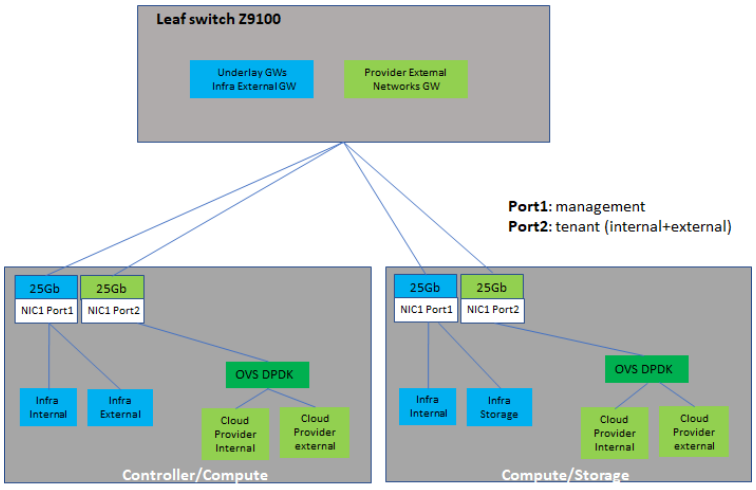


Figure 3.103 : Networking for Fish Farming Edge.

SDN is not used in fish farm edge site since we want to keep it simple with the small Edge Cloud setup. The VLAN networks that require L3 connectivity (external routing networks) will be created in Z9100.

The VLAN allocation is below:

- **0-512:** for underlay network and P2P connection (eg. FW-Z9100, CSR-Z9100)
- **1000-1499:** for external provider networks, which are created by the provider (admin).
- **1500-1999:** for internal/tenant networks, which will be assigned automatically to the users
- **2000- :** for other purposes.

The VLANs 1000-1499 are assigned automatically by Openstack whenever a tenant is trying to create a network. The VLANs 1500-1999 for external networks are created by the platform admin only who assigns the IP subnets in both Z9100 and Openstack.

The uplink from Z9100 leaf switch will be the Pileus VPN server (provided by Celerway), which is connected to PaloAlto's FW in Central site over the 4G network. The Pileus VPN server can have two SIMs and connect to different networks for availability, which is a good capability when the Edge is deployed in a very remote location. Between Z9100 switch and Pileus VPN there is a port allocated, configured in access mode, since Pileus does not use trunk.

There will be static routes defined in Z9100 to route internet and inter-site traffic to Pileus VPN, and from its side there will be static routes to underlay and overlay networks towards Z9100.

The cameras will be connected to a Cageeye switch first and then to Z9100, in order to transmit the recordings to the analytic VMs.

The CPE can be connected either to the camera's switch or in Z9100 directly.

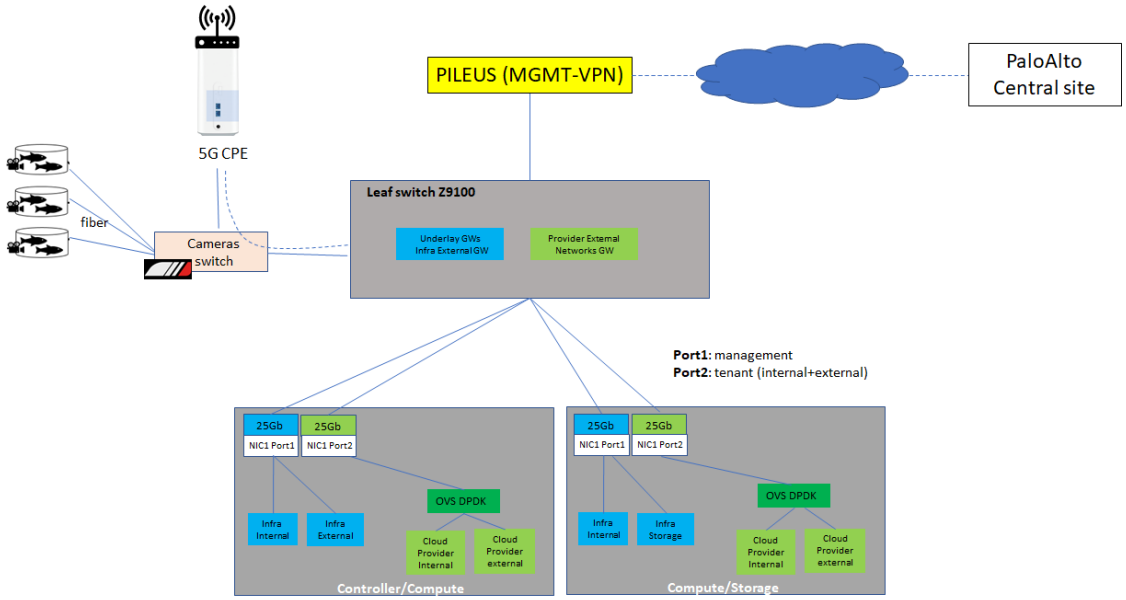


Figure 3.104 : Connecting customer equipment to the Fish Farm Edge and VPN setup for remote management.

Finally, VM analytics onboarding can be done either locally by using the NCIR GUI or it can be automated from G-VNFM (CBAM 19.5), which has been deployed in the Central site. In total, there will be 5 VMs, 2 VMs using GPU and 3 VMs without GPU.

The output will be transmitted from Edge cloud to the Cageeye central system via the 5G network slice (non-standalone eMBB based slice will be used initially). The slice used will be the existing eMBB slice based on NSA 5G. The orchestration system could also be used to deploy the application at the edge and the core network in the central site at the same time.

The orchestration flow is illustrated in Figure 3.105.

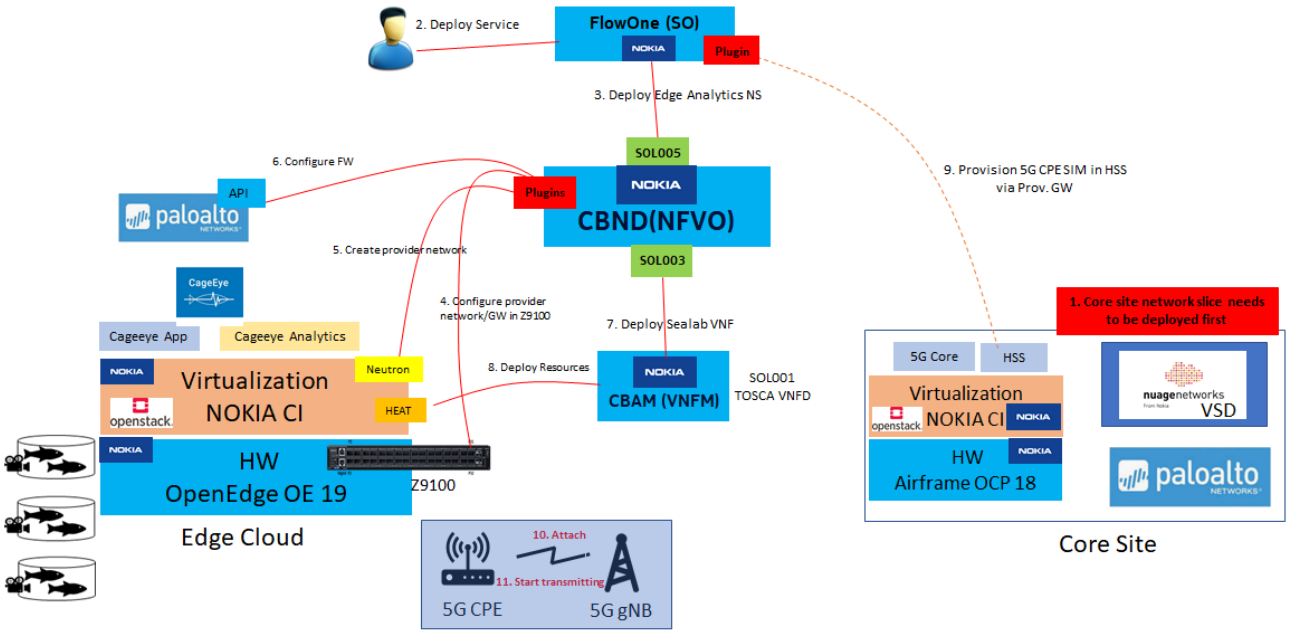


Figure 3.105 : Edge Cloud Onboarding and Provisioning Automation.

3.9 Service Orchestration, NFVO and G-VNFM

In section 4.3 figure 2 illustrates high level MANO solution architecture to be implemented in 5G VINNI project. NFV MANO framework consists of three main functional blocks:

a. NFV Orchestrator (NFVO) – Responsible for on-boarding new Network Services (NS) and Virtual Network Function (VNF) packages, resource management and validation and authorization of NFVI request. Nokia Cloudband Network Director (CBND) will form this functional unit.
b. VNF Manager (VNFM) – Responsible for overseeing life cycle management of VNF instances. Nokia Cloudband Application Manager (CBAM) and Ericsson ECM will from this functional unit.
c. Virtual Infrastructure Manager (VIM) – Controls and manage NFVI components including, Compute, Storage, Network resources. Nokia NCIR (Openstack based) will be used as a VIM.

Both CBND and CBAM have well-defined roles within a hierarchy of management functions in MANO as is shown in Figure 3.106.

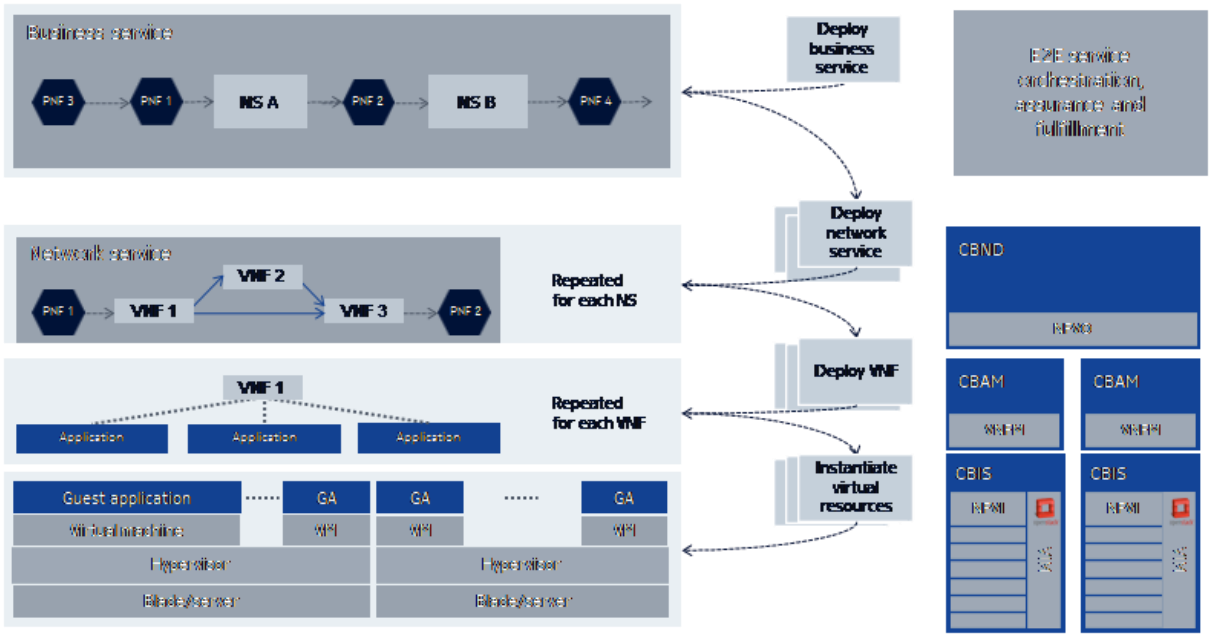


Figure 3.106 : Network services delivery functional flow

Note that in the Business layer, which is the layer above ETSI MANO, a service orchestrator is located, which instructs CBND to deploy network services and provides the service-specific parameters required for the implementation of these services. Note that FlowOne from Nokia will be used for realizing complex network services, involving network slicing and service lifecycle management.

3.9.1 VNF Manager

The functional architecture of the CloudBand Application Manager (CBAM) having the role as the VNFM is illustrated in Figure 3.107.

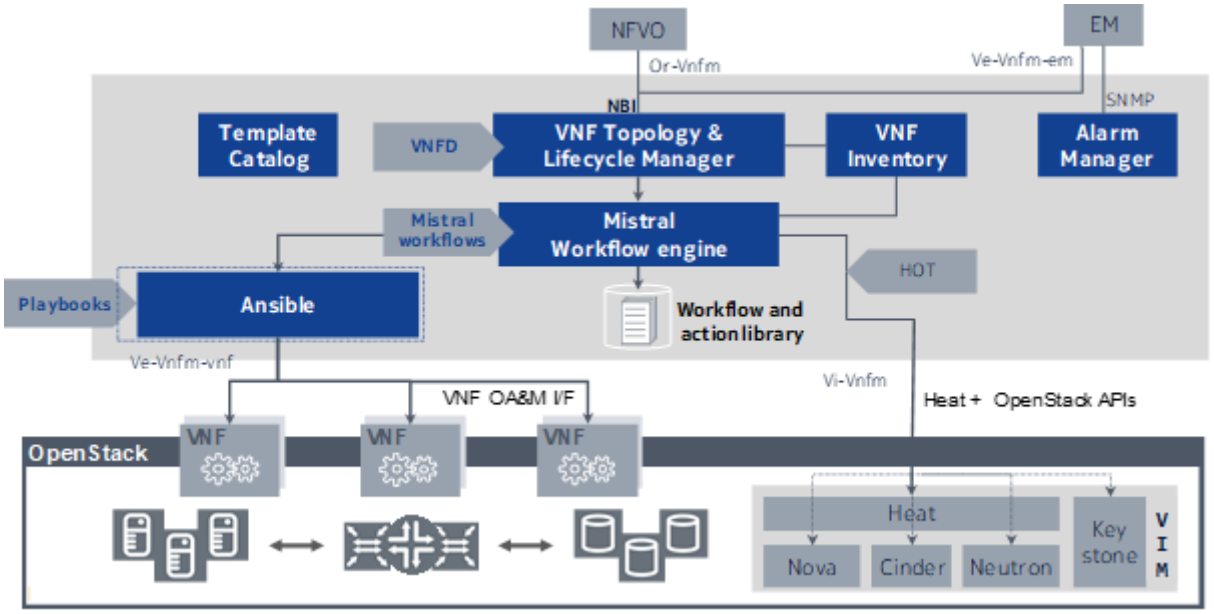


Figure 3.107 : CBAM functional architecture

The CBAM architecture is based on several internal architectural components:

- VNF Template Catalog provides storage for the VNF template packages delivered by the VNF vendors. The VNFD as part of the package describes the topology of the VNF and is used by the topology lifecycle manager (TLM) as basis for the lifecycle management operations.
- Lifecycle operations are triggered via the ETSI NFV IFA 007 compatible northbound HTTP(S) / REST based API. OpenStack Mistral is used as workflow execution engine to orchestrate all the elementary actions of the lifecycle workflows
- Mistral workflow and action including built-in workflows are enabled with VIM access through Heat
- Inventory micro-service is used to store the data models of the managed VNFs, their associated VIMs and subscribers of Lifecycle Change Notifications
- Ansible is used for the initial commissioning of VNFs and can also be used for supporting functionality in custom mistral workflows.

Release 19.5 of CBAM is deployed in the 5G-VINNI Norway facility site.

3.9.1.1 VNF Descriptors

To achieve the widest interoperability and to simplify on-boarding, Nokia has published and implemented detailed guidelines for the creation of VNF descriptor templates based on ETSI specifications. Where applicable we will adopt de-facto standard open technologies, such as OASIS TOSCA modelling language, as well as Mistral work flow, Ansible playbooks, etc. Currently it's TOSCA based and CBAM will include SOL001 in CBAM 19.5

3.9.1.2 VNFM Interfaces

Table 3.18 : VNFM Interfaces

Interface Name	Direction	Components	Responsible parties
Or-Vnfm[8]	Northbound	NFVO <-> VNFM	Nokia/Ericsson (SOL003)
Vi-Vnfm	Southbound	VNFM <-> VIM	Nokia/Ericsson (HEAT)
Ve-Vnfm-em/vnf	East-West	VNFM <-> EMS/VNF	Ericsson

3.9.1.3 Deployment Consideration

CBAM is deployed as HA pair per site. It has external connectivity to the VIMs on which it is performing Life Cycle Management of VNFs. The ports (http/s, ssh, mgmt.) are needed to be punched in to the firewall to allow connectivity to/from CBND & CBAM with other systems such as the VIM, EMS.

An 8-core vCPU with minimum of 32 GB RAM and 300 GB of virtual storage is recommended per node. A single 1 Gbps vNIC is required per VM.

3.9.2 NFV Orchestrator

NFVO is mainly responsible for resource orchestration and network services orchestration and their management. It visualizes and automates the lifecycle of network services, such as virtual EPC, including their forwarding graphs and service chain. It may also include provisioning of external

[8] For reference, see ETSI GS NFV-SOL 003

networks necessary for the VNFs, which may involve various types of networks like, L2 L3, SDN port mirroring, etc.

The logical architecture of CBND is shown in Figure 3.108. In terms of architecture, CBND can be divided in five main functional blocks:

1. Northbound API layer and GUI
2. Network Service Orchestration (NSO)
3. Resource Orchestration (RO)
4. Southbound API layer
5. CBND platform operations tools.

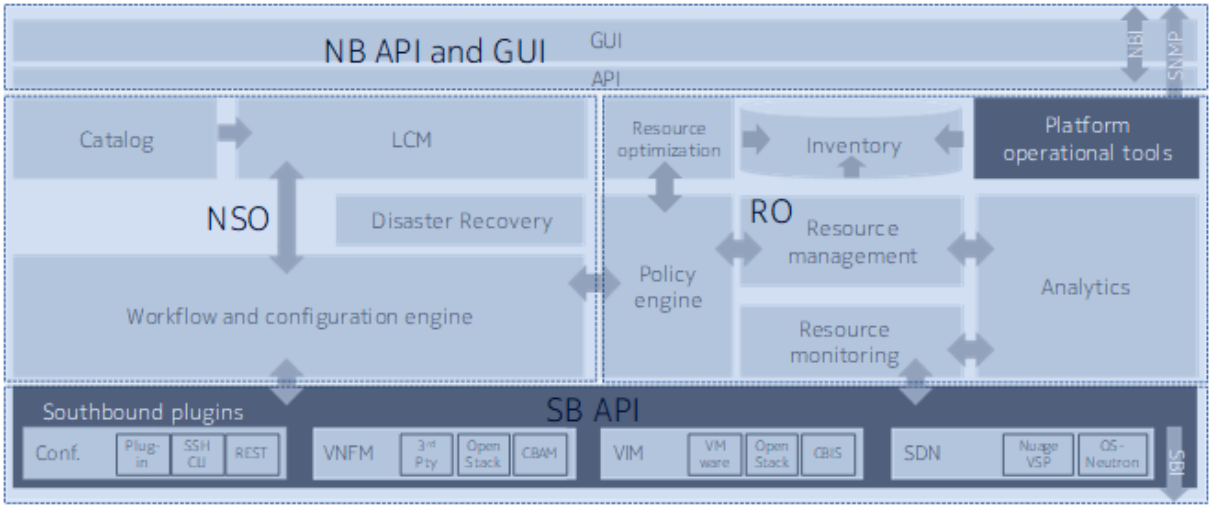


Figure 3.108 : CBND Logical Architecture

3.9.2.1 Northbound APIs layer and GUI

The northbound API layer exposes RESTful APIs that represents the full set of capabilities of CBND. It is mainly used for integration with higher layer systems (For example: Service Orchestrator, OSS), implementing the Os-Ma-nfvo interface and by the CBND GUI.

CBND GUI provides a visual representation of CBND functionalities and interacts directly with the northbound API layer. It provides access to the functions listed below:

- Managing Resources
- Managing VIMs
- Managing VNFMs
- Managing SDN Controllers
- Viewing network topology
- Managing Catalogs
- Managing Network services (NS Lifecycle Management)
- Managing alarms

The automation engine provided by the automation stream in the project uses the CBND workflow engine running customized workflows.

3.9.2.2 Network Service Orchestration (NSO)

This section provides operations to perform VNF and Network Service Lifecycle Management (LCM). It has a Catalog where all the Network Service artefacts are stored. These artefacts are e.g. Network Service Descriptor (NSD) and VNF Descriptor (VNFD). At a high level, below are the important roles that NSO assumes:

a. LCM interacts with Resource Optimization component to get recommendations for the VNF placement.
b. LCM stores the Network Service Record and VNF Record in the CNBD inventory database.
c. LCM interacts with the resource monitoring component to monitor VNF and NS KPIs and alarms. The NSO function logic is agnostic on the type of cloud and of the integrated objects and all southbound communication, e.g. with CBAM, is performed through the SB API layer.
d. Where applicable, LCM will interact with the internal mistral workflow engine to trigger multiple workflows like Instantiate, Scale, Terminate.

3.9.2.3 Resource Orchestration (RO)

The resource management function is responsible for administration of managed objects (VIMs, VNFMs, SDN-Controllers), resource monitoring including VNFs and NSs, resource topology and correlation, common inventory and policy-engine. CBND´s mission is to automate and optimize the management of NSs and VNFs and allow them to optimally run in a distributed NFV infrastructures environment.

e. The Resource Orchestration function (RO) ensures that the platform, as a pool of resources, are fully operational and that these resources are utilized by the NSs and VNFs in line with operator´s policies.
f. Resource related operational aspects (capacity planning, capacity management, monitoring, reporting, and so on) are performed in the context of VNFs/NSs and the associated control plane elements, such as VIM, SDN controllers, VNFM, and so on.

Managing physical and virtual level resources (IaaS) and operational aspects without direct VNFs and/or NSs context – like e.g. public cloud or IT cloud - are out of scope of CBND.

3.9.2.4 Platform operational tools

The platform operations tools provide the runtime environment to host and run CBND components. For these CBND components, it provides authentication and authorization, user management, security, logging and audit logging, self-monitoring and so on.

3.9.2.5 Southbound API layer

The southbound communication of CBND is enabled through the Southbound API layer where the VIM, VNFM, SDN-Controller and configuration plug-ins are installed. CBND provides a flexible and open architecture allowing external plugins to be developed and plugged in into the system.

Release 19.0 of CBND will be deployed in the 5G-VINNI Norway facility site.

3.9.2.6 NFVO Interfaces

Table 3.19 : NFVO interfaces

Interface Name	Direction	Components	Responsible parties
Or-Vnfm[9]	Southbound	NFVO <-> VNFM	Nokia/Ericsson (SOL003)
Or-Vi[10]	Southbound	NFVO <-> VIM	Nokia (Blueprint) Neutron

[9] For reference, see ETSI GS NFV-SOL 003

[10] For reference see ETSI GS NFV-IFA 005

Interface Name	Direction	Components	Responsible parties
Os-Nfvo	Northbound	Flowone<-> NFVO	Nokia (Blueprint/SOL005)

Orchestrator will also have an interface to Nuage VSD.

3.9.2.7 Deployment Consideration

CBND is deployed as HA cluster of 3 nodes per site. It has external connectivity to the VIM and VNFM (as well as OSS/BSS), on which it is performing life cycle management of VNFs as well as network services and resource management. Several ports (http/s, ssh, ejb, monitoring and mgmt. services, etc.) are needed to be punched in the firewall to allow connectivity to/from CBND & CBAM and OSS.

A 12-core vCPU with minimum of 28 GB RAM and 400 GB of virtual storage is recommended per node. Dual 1 Gbps vNIC are required per VM.

3.9.2.8 VNF Life cycle management

The deployment of lifecycle workflows during the integration of VNFs typically involves:

- process input parameters
- send 'start lifecycle change' notification to the NFVO and other interested parties
- request grant from the NFVO with additional VIM specific parameters
- receive grant from the NFVO with additional VIM specific parameter values
- manipulate the Heat stack
- perform initial configuration/commissioning of the VNF
- register or update the VNF-related information in the EMS
- send 'result lifecycle change' notifications to the NFVO and other interested parties.

Figure 3.109 shows the call flow encompassing various components in ETSI NFV architecture.

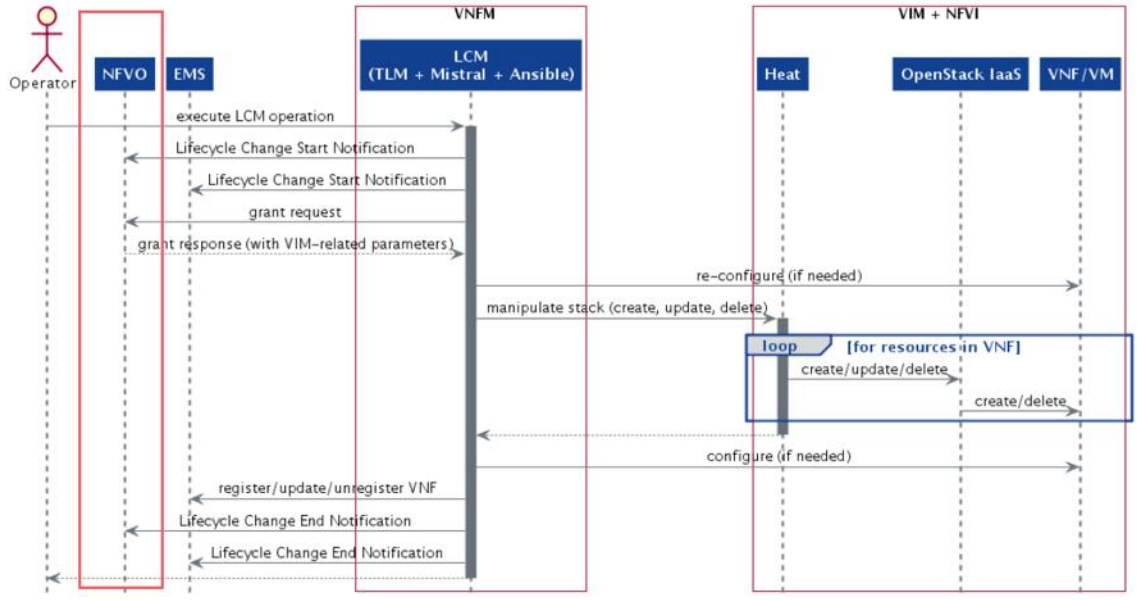


Figure 3.109 : VNF life cycle management call flow

3.9.2.9 Onboarding

The autonomous slice will be deployed in 2 sites, at Core and Edge. FlowOne as Service Orchestrator will trigger the slice deployment to NFVO (CBND 19.5) which will use both VIMs for resources.

For Ericsson 5G Core, Ericsson VNFM will be triggered which will deploy its VNFs in core (NCIR 18) and Edge site (NCIR 19).

For Metaswitch IMS, NOKIA G-VNFM will be triggered which will deploy the VNFs into core Sited and Edge site too.

During onboarding, CBND 19.5 will do the perform actions:

- Create external networks in Nuage VSD and NCIR at the Core Site
- Create provider networks in Z9100 and NCIR at Edge site
- Deploy the Ericsson VNFs via EVNFM
- Deploy the Metaswitch VNFs via CBAM
- Configure PaloAlto Firewall in Core site for the VNFs there
- Configure PaloAlto Firewall in Edge site for the VNFs there

3.9.2.10 NFVO Plugin Development towards VNFM

For managing / orchestrating network services which are composed of VNFs that are not from Nokia, integration between CBND and specific VNFMs are required. This integration effort enables network service development and integration for each VNFM on CBND.

3.9.2.10.1 CBND – Ericsson VNFM integration

CBND follows an Open Architecture where external systems like VIM, VNFM, SDN Controller and so on, can be integrated. Integration of these external systems into CBND happens through a plugin framework. The VNFM type plugin was developed, for the purpose of integrating Ericsson VNFM with Nokia CBND over Or-Vnfm interface described by ETSI NFV-SOL003 v.2.4.1.

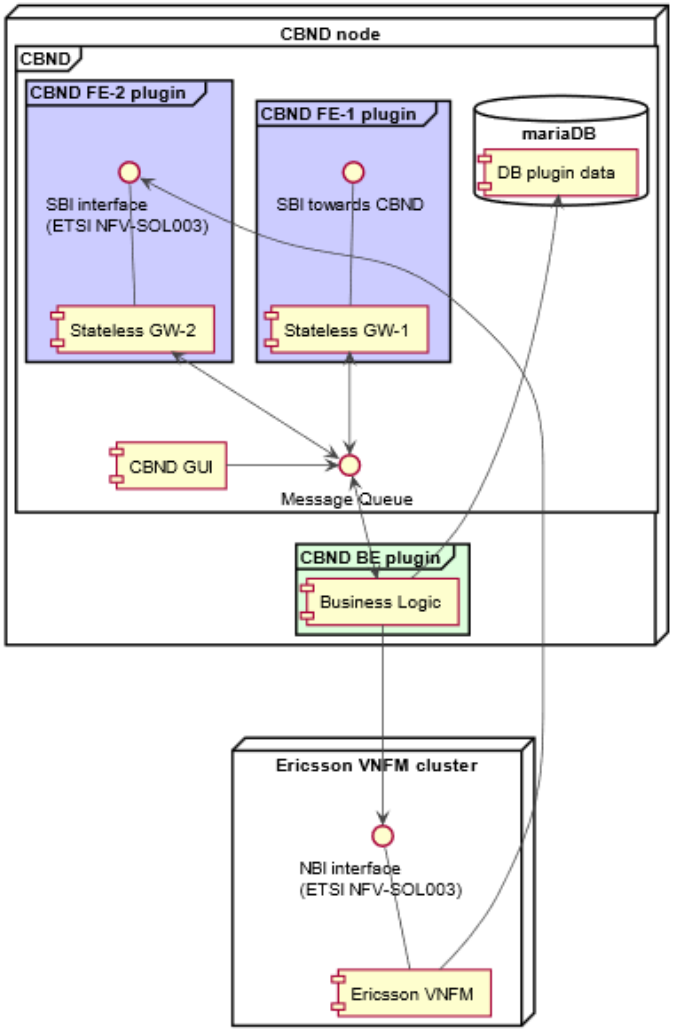


Figure 3.110 : Integration of Specific VNFM (Ericsson VNFM) with NFVO (Nokia CBND)

Nokia-Ericsson MANO integration solution consists of:

- CBND VNFM plugin
- CBND VNFM plugin tools
- MariaDB database provided by CBND Core to store persistent information
- "Message Queue" service provided by CBND Core
- The integration solution has been developed as stateless, all persistent artifacts are stored in MariaDB, which run in clustered mode. The solution can be run as part of HA CBND and standalone CBND.

3.9.2.10.2 CBND VNFM plugin

CBND VNFM plugin consist of 3 subsystems:

- CBND FE 1 plugin. This plugin provides REST API for CBND Core to query status of VNFMs and VNFs. It is deployed as part of the CBND REST API framework and inherits all capabilities of standard CBND REST APIs such as security, availability, resilience, etc.
- CBND FE-2 plugin. This plugin provides Southbound CBND REST API for Ericsson VNFM. It is deployed as part of the CBND REST API framework and inherits all capabilities of standard CBND REST APIs such as security, availability, resilience, etc.
- CBND BE plugin. This plugin implements key business logic for Ericsson VNFM integration. It is deployed as separate *cbndpluginserver* RHEL OS service.

- All subsystems communicate to each other via “Message Queue” service provided by the CBND Core.

3.9.2.10.3 CBND VNFM plugin tools

There are 2 auxiliary tools, which complement CBND VNFM plugin:

- **ericsson_vnfm_tool** interacting with Ericsson VNFM from terminal console. It allows requesting provisioned VNFDs to VNFM, check status of VNFs, terminates VNF, etc.
- **ericsson_db_tool** interacting with CBND VNFM plugin database. It allows listing of all artifacts stored in DB, provision VNFM users.

3.9.2.10.4 Architecture Functional view

The following functions have been developed and supported by CBND VNFM plugin:

- Network Service Instantiation
- Network Service Termination
- Network Service Scaling from CBND
- Network Service Scaling from VNFM
- Fetching status of Ericsson VNFM
- Fetching status of deployed VNFs

3.9.2.11 CBND - PaloAlto Firewalls integration

CloudBand Network Director (CBND) follows an Open Architecture where external systems like VIM, VNFM, SDN Controller and so on, can be integrated. Integration of these external system into CBND happens through plugin framework. The custom type plugin was developed, for the purpose of integrating PaloAlto Firewalls with Nokia CBND over proprietary REST interface.

The plugin supports the following scenarios:

- Update Firewall Configuration

The process for automated configuration of firewall rules for a NS is illustrated in Figure 3.111 and described as follows:

a) User Deploy Firewall Configuration NS (this can be part of Network NSD, VNF NSD or dedicated Firewall NSD)
b) CBND interacts with Panorama EMS and send new configuration for firewall(s)
c) Panorama EMS reconfigure requested firewall(s)

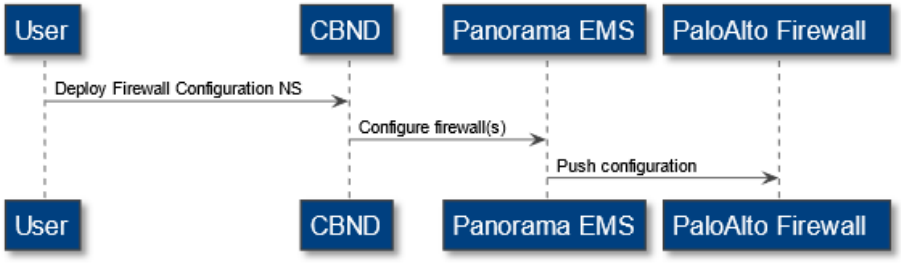


Figure 3.111 : Configuration of firewall rules for Network Service (NS)

3.9.3 Orchestration in 5G StandAlone (SA) Architecture

In the following we describe how orchestration is done for the 5G SA architecture

3.9.3.1 An NFVO layer for both virtualized and cloud native functions

The current release of NFVO is CBND 19.5 and it can support only the SOL003 to G-VNFM or the plugin towards Ericsson VNFM. For CNF deployment, NFVO should support Kubernetes APIs and this is only available from the next release, CBND 20.5 which is available.

We have also deployed a second instance of NFVO (CBND20.5) in the Central site, but Ericsson requires the CNFs to be deployed by the Extended VNFM (E-VNFM).

There are two possible ways to deploy slices with CNFs in 5G-VINNI Norway facility site now:

a) by using CBND 20.5 or newer and have direct interface with Kubernetes VIMs. An example is in the Edge site
b) by using CBND19.5 (or newer) and the current interface to E-VNFM, which will then have an interface to Ericsson CaaS.

For Ericsson CNFs, we will use the second option, as it is shown below:

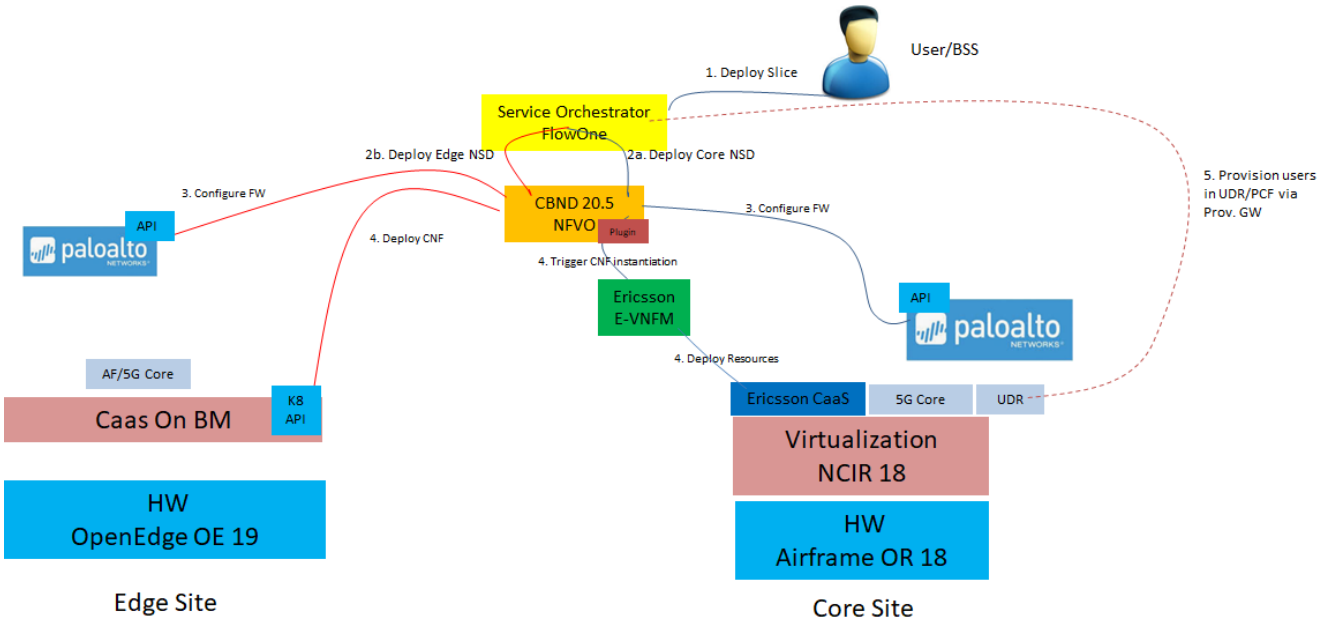


Figure 3.112 : Orchestration of Ericsson SA 5G Core CNFs

3.9.3.2 Ericsson Extended VNFM (EVNFM)

Ericsson Evolved Virtual Network Function Manager (EVNFM) provides Life Cycle Management (LCM) support for Containerized Network Functions (CNFs) and Virtual Network Functions (VNFs) according to the European ETSI MANO specifications. Currently, the ETSI standards do not support CNFs. EO EVNFM aligns to the existing standards as closely as possible and includes the necessary changes to support CNFs.

The EVNFM is a CNF and is to be deployed on top of an existing Kubernetes cluster.

The EVNFM supports both small-stack-deployments via the EVNMF GUI and full-stack-deployments triggered from NFVO via SOL 003 interface.

3.9.3.2.1 CNF Life Cycle Management (LCM)

The current version of EVNFM 20.2 can do the following for VM based and CNF based functions:

- Package onboarding
- Onboarding of cloud native Virtual Network Function (VNF) packages
- The following Life Cycle Management operations:
- Instantiate

- Terminate
- Scale
- Upgrade (CNF support only)
- User Interface

The EVNFM Northbound interface towards the NFVO (SOL003/Or-Vnfm) are similar as deployed in previous VNF-LCM handling the VM based NSA network functions. The initial approach is then to reuse previously created wrapper on EVNFM side and the CBND VNF LCM plugin on NFVO side in the integration between EVNFM and CBND (NFVO).

From the NVFO side there should then be no change in the SOL003/Or-Vnfm interface regarding LCM of VNF and CNF. The VNVFDID provided in the VNFD will identify the network function as a VNF or a CNF. This mapping is done in the EVNFM during the onboarding process.

3.9.3.2.2 CNF Onboarding

A prerequisite for CNF LCM activities is that the CNF package are onboarded in the EVNFM. Initially this will be done manually in EVNFM, when the NFVO-EVNFM integration is verified and CNF LCM activities verified. Next step will be to also perform onboarding triggered from NVFO.

EO EVNFM can do the following:

- Onboard a CSAR package that complies with the ETSI SOL 001 and SOL 004 specifications.
- Parse the package to locate Docker images, the Virtual Network Function Descriptor (VNFD), the Helm charts, and other files.
- Persist files in appropriate repositories to enable Life Cycle Management use cases (Helm charts, Docker images).

This release of EO EVNFM supports a type A1 CSAR package format that complies with ETSI SOL 004 specifications. The TOSCA metadata directory is mandatory at the root of the package. The TOSCA.meta file must exist, where different files within the package can be referenced through entries.

3.9.4 Network slicing orchestration using design authority VNF

During slice deployment, the templates, such as VNFD and NSD, need several parameters as input in order for the orchestrator to create networks in SDN and openstack, add firewall policies or pass configuration information to the VNFM.

That kind of information exists in design documents (e.g. LLD) and they are usually extracted manually in json files that are used as input in the Service Orchestrator, NFVO or VNFM. That procedure may be complicated and human errors may lead to a non-operating network slice or failed deployment. Ideally, that procedure could be automated and use a single source of truth.

One of the innovative ideas that has been created and implemented in 5G-VINNI, it is the Design Authority VNF, which is a VM that has the below capabilities, it:

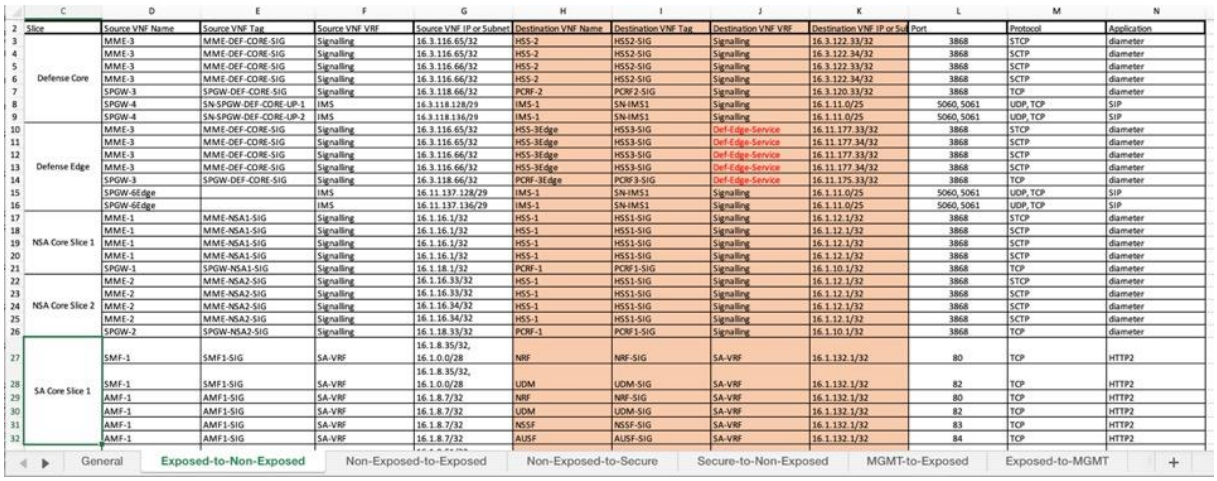
- has a database (e.g MariaDB) with multiple tables with design information
- read the LLD (excel format) and add the data in database tables
- expose APIs, so any remote system, such as Service Orchestrator, can query and get specific design information

This is not a productised solution, but it was built to demonstrate the idea in the 5G-VINNI Norway facility site.

The design documents that have been used, are:

- IP design, which holds information regarding subnets/networks per VNF and slice
- Connectivity matrix, which holds information for firewall tagging per VNF and slice

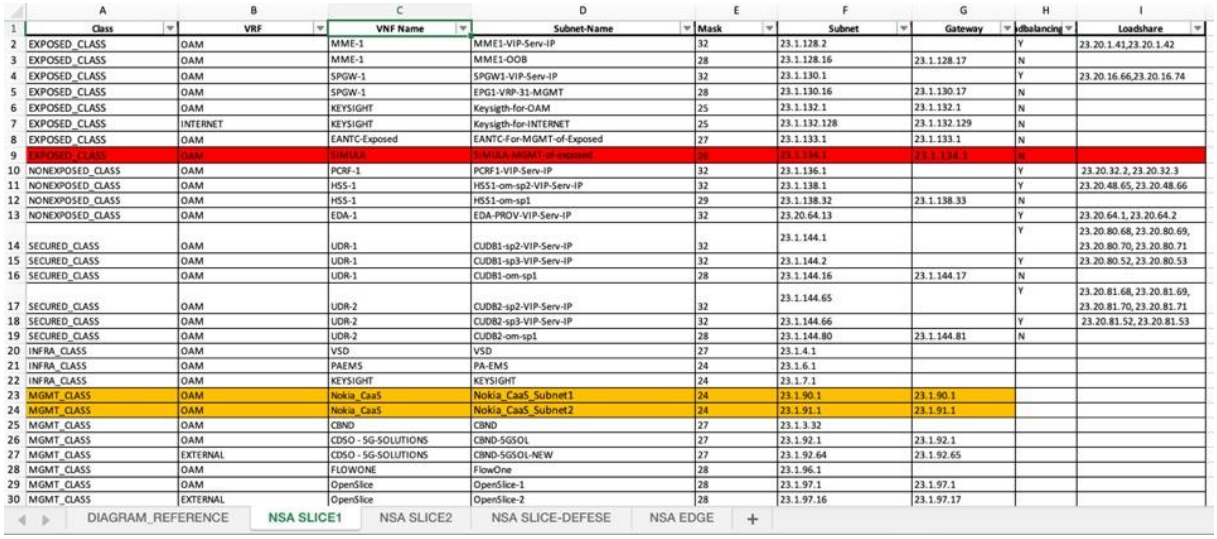
Examples of those design documents are shown in Figure 3.113 and Figure 3.114.



Slice	Source VNF Name	Source VNF Tag	Source VNF VRF	Source VNF IP or Subnet	Destination VNF Name	Destination VNF Tag	Destination VNF VRF	Destination VNF IP or Sul	Port	Protocol	Application
	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.65/32	HSS-2	HSS2-SIG	Signalling	16.3.122.33/32	3868	SCTP	diameter
	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.65/32	HSS-2	HSS2-SIG	Signalling	16.3.122.34/32	3868	SCTP	diameter
	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.66/32	HSS-2	HSS2-SIG	Signalling	16.3.122.33/32	3868	SCTP	diameter
Defense Core	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.66/32	HSS-2	HSS2-SIG	Signalling	16.3.122.34/32	3868	SCTP	diameter
	SPGW-3	SPGW-DEF-CORE-SIG	Signalling	16.3.118.66/32	PCRF-2	PCRF2-SIG	Signalling	16.3.120.33/32	3868	TCP	diameter
	SPGW-4	SN-SPGW-DEF-CORE-UP-1	IMS	16.3.118.128/29	IMS-1	SN-IMS1	Signalling	16.1.11.0/25	5060, 5061	UDP, TCP	SIP
	SPGW-4	SN-SPGW-DEF-CORE-UP-2	IMS	16.3.118.136/29	IMS-1	SN-IMS1	Signalling	16.1.11.0/25	5060, 5061	UDP, TCP	SIP
	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.65/32	HSS-3Edge	HSS3-SIG	Def-Edge-Service	16.11.177.33/32	3868	SCTP	diameter
	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.65/32	HSS-3Edge	HSS3-SIG	Def-Edge-Service	16.11.177.34/32	3868	SCTP	diameter
	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.66/32	HSS-3Edge	HSS3-SIG	Def-Edge-Service	16.11.177.33/32	3868	SCTP	diameter
Defense Edge	MME-3	MME-DEF-CORE-SIG	Signalling	16.3.116.66/32	HSS-3Edge	HSS3-SIG	Def-Edge-Service	16.11.177.34/32	3868	SCTP	diameter
	SPGW-3	SPGW-DEF-CORE-SIG	Signalling	16.3.118.66/32	PCRF-3Edge	PCRF3-SIG	Def-Edge-Service	16.11.175.33/32	3868	TCP	diameter
	SPGW-6Edge		IMS	16.11.137.128/29	IMS-1	SN-IMS1	Signalling	16.1.11.0/25	5060, 5061	UDP, TCP	SIP
	SPGW-6Edge		IMS	16.11.137.136/29	IMS-1	SN-IMS1	Signalling	16.1.11.0/25	5060, 5061	UDP, TCP	SIP
	MME-1	MME-NSA1-SIG	Signalling	16.1.16.1/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
	MME-1	MME-NSA1-SIG	Signalling	16.1.16.1/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
NSA Core Slice 1	MME-1	MME-NSA1-SIG	Signalling	16.1.16.1/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
	MME-1	MME-NSA1-SIG	Signalling	16.1.16.1/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
	SPGW-1	SPGW-NSA1-SIG	Signalling	16.1.18.1/32	PCRF-1	PCRF1-SIG	Signalling	16.1.10.1/32	3868	TCP	diameter
	MME-2	MME-NSA2-SIG	Signalling	16.1.16.33/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
	MME-2	MME-NSA2-SIG	Signalling	16.1.16.33/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
NSA Core Slice 2	MME-2	MME-NSA2-SIG	Signalling	16.1.16.34/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
	MME-2	MME-NSA2-SIG	Signalling	16.1.16.34/32	HSS-1	HSS1-SIG	Signalling	16.1.12.1/32	3868	SCTP	diameter
	SPGW-2	SPGW-NSA2-SIG	Signalling	16.1.18.33/32	PCRF-1	PCRF1-SIG	Signalling	16.1.10.1/32	3868	TCP	diameter
	SMF-1	SMF1-SIG	SA-VRF	16.1.8.35/32, 16.1.0.0/28	NRF	NRF-SIG	SA-VRF	16.1.132.1/32	80	TCP	HTTP2
SA Core Slice 1	SMF-1	SMF1-SIG	SA-VRF	16.1.8.35/32, 16.1.0.0/28	UDM	UDM-SIG	SA-VRF	16.1.132.1/32	82	TCP	HTTP2
	AMF-1	AMF1-SIG	SA-VRF	16.1.8.7/32	NRF	NRF-SIG	SA-VRF	16.1.132.1/32	80	TCP	HTTP2
	AMF-1	AMF1-SIG	SA-VRF	16.1.8.7/32	UDM	UDM-SIG	SA-VRF	16.1.132.1/32	82	TCP	HTTP2
	AMF-1	AMF1-SIG	SA-VRF	16.1.8.7/32	NSSF	NSSF-SIG	SA-VRF	16.1.132.1/32	83	TCP	HTTP2
	AMF-1	AMF1-SIG	SA-VRF	16.1.8.7/32	AUSF	AUSF-SIG	SA-VRF	16.1.132.1/32	84	TCP	HTTP2

General | Exposed-to-Non-Exposed | Non-Exposed-to-Exposed | Non-Exposed-to-Secure | Secure-to-Non-Exposed | MGMT-to-Exposed | Exposed-to-MGMT

Figure 3.113 : Example Low Level Design (LLD) document



Class	VRF	VNF Name	Subnet-Name	Mask	Subnet	Gateway	Idbalancing	Loadshare
EXPOSED_CLASS	OAM	MME-1	MME1-VIP-Serv-IP	32	23.1.128.2		Y	23.20.1.41,23.20.1.42
EXPOSED_CLASS	OAM	MME-1	MME1-OOB	28	23.1.128.16	23.1.128.17	N	
EXPOSED_CLASS	OAM	SPGW-1	SPGW1-VIP-Serv-IP	32	23.1.130.1		Y	23.20.16.66,23.20.16.74
EXPOSED_CLASS	OAM	SPGW-1	EPG1-VRP-31-MGMT	28	23.1.130.16	23.1.130.17	N	
EXPOSED_CLASS	OAM	KEYSIGHT	Keysigth-for-OAM	25	23.1.132.1	23.1.132.1	N	
EXPOSED_CLASS	INTERNET	KEYSIGHT	Keysigth-for-INTERNET	25	23.1.132.128	23.1.132.129	N	
EXPOSED_CLASS	OAM	EANTC-Exposed	EANTC-For-MGMT-of-Exposed	27	23.1.133.1	23.1.133.1	N	
EXPOSED_CLASS	OAM	SIMULA	SIMULA-MGMT-of-exposed	26	23.1.134.1	23.1.134.1	N	
NONEXPOSED_CLASS	OAM	PCRF-1	PCRF1-VIP-Serv-IP	32	23.1.136.1		Y	23.20.32.2, 23.20.32.3
NONEXPOSED_CLASS	OAM	HSS-1	HSS1-om-sp2-VIP-Serv-IP	32	23.1.138.1		Y	23.20.48.65, 23.20.48.66
NONEXPOSED_CLASS	OAM	HSS-1	HSS1-om-sp1	29	23.1.138.32	23.1.138.33	N	
NONEXPOSED_CLASS	OAM	EDA-1	EDA-PROV-VIP-Serv-IP	32	23.20.64.13		Y	23.20.64.1, 23.20.64.2
SECURED_CLASS	OAM	UDR-1	CUDB1-sp2-VIP-Serv-IP	32	23.1.144.1		Y	23.20.80.68, 23.20.80.69, 23.20.80.70, 23.20.80.71
SECURED_CLASS	OAM	UDR-1	CUDB1-sp3-VIP-Serv-IP	32	23.1.144.2		Y	23.20.80.52, 23.20.80.53
SECURED_CLASS	OAM	UDR-1	CUDB1-om-sp1	28	23.1.144.16	23.1.144.17	N	
SECURED_CLASS	OAM	UDR-2	CUDB2-sp2-VIP-Serv-IP	32	23.1.144.65		Y	23.20.81.68, 23.20.81.69, 23.20.81.70, 23.20.81.71
SECURED_CLASS	OAM	UDR-2	CUDB2-sp3-VIP-Serv-IP	32	23.1.144.66		Y	23.20.81.52, 23.20.81.53
SECURED_CLASS	OAM	UDR-2	CUDB2-om-sp1	28	23.1.144.80	23.1.144.81	N	
INFRA_CLASS	OAM	VSD	VSD	27	23.1.4.1			
INFRA_CLASS	OAM	PAEMS	PA-EMS	24	23.1.6.1			
INFRA_CLASS	OAM	KEYSIGHT	KEYSIGHT	24	23.1.7.1			
MGMT_CLASS	OAM	Nokia_CaaS	Nokia_CaaS_Subnet1	24	23.1.90.1	23.1.90.1		
MGMT_CLASS	OAM	Nokia_CaaS	Nokia_CaaS_Subnet2	24	23.1.91.1	23.1.91.1		
MGMT_CLASS	OAM	CBND	CBND	27	23.1.3.32			
MGMT_CLASS	OAM	CDSO - 5G-SOLUTIONS	CBND-5GSOL	27	23.1.92.1	23.1.92.1		
MGMT_CLASS	EXTERNAL	CDSO - 5G-SOLUTIONS	CBND-5GSOL-NEW	27	23.1.92.64	23.1.92.65		
MGMT_CLASS	OAM	FLOWONE	FlowOne	28	23.1.96.1			
MGMT_CLASS	OAM	OpenSlice	OpenSlice-1	28	23.1.97.1	23.1.97.1		
MGMT_CLASS	EXTERNAL	OpenSlice	OpenSlice-2	28	23.1.97.16	23.1.97.17		

DIAGRAM_REFERENCE | NSA SLICE1 | NSA SLICE2 | NSA SLICE-DEFESE | NSA EDGE

Figure 3.114 : Example Low Level Design (LLD) document

The first step is to add those design documents in the VNF's database by converting the files into database tables as illustrated in Figure 3.115. The second step is to expose several APIs and provide the needed data to the Service Orchestrator and NFVO as illustrated in Figure 3.116.

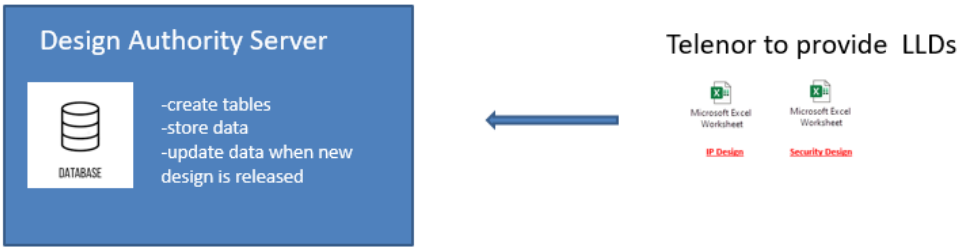


Figure 3.115 : Add Design documents int Design Authority Server databases.

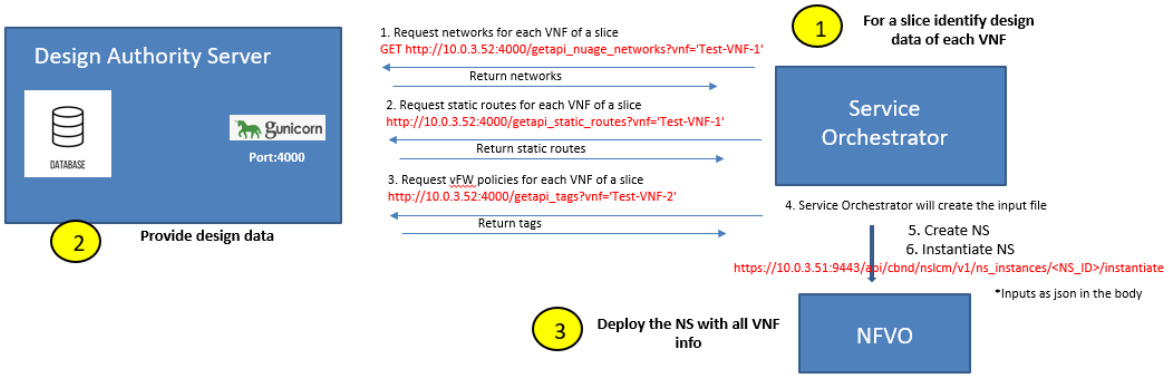


Figure 3.116 : Expose APIs for systems components to retrieve data.

Finally, either the Service Orchestrator or the NFVO can use those APIs to get the information and build the input files for the network services in an automated way. Whenever there is updated design document then the existing tables in design authority VNF have to be updated, so the orchestrators will receive the latest info regarding the Slices, NSs and VNF that they need to deploy.

The final orchestration flow is illustrated in Figure 3.117, where orchestrator first gets the data and use the SOL005 interface towards the NFVO.

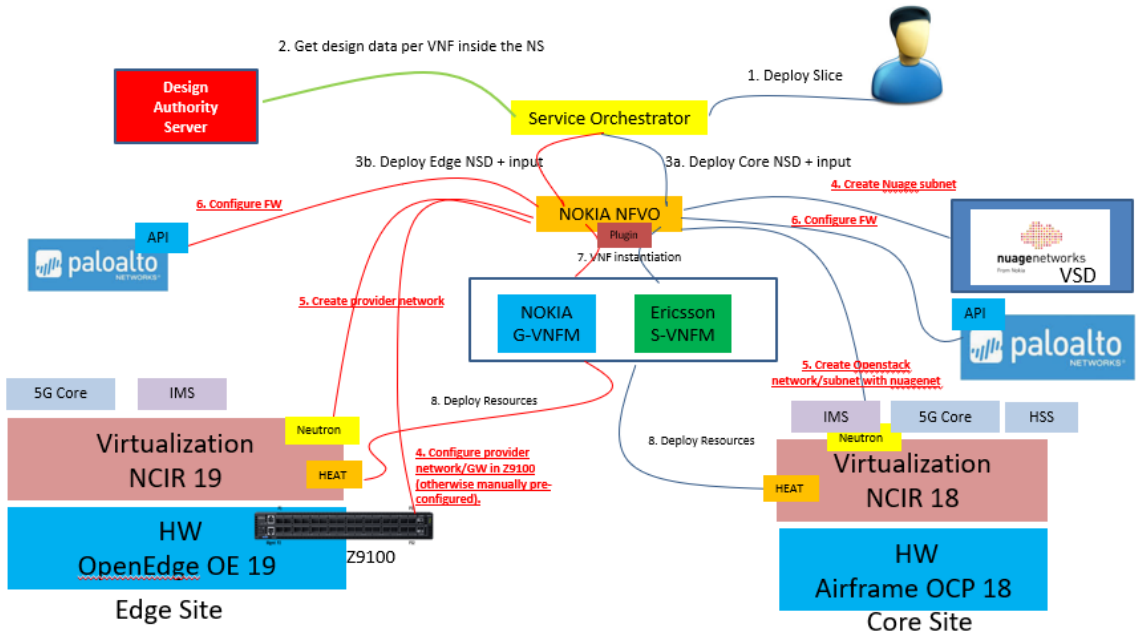


Figure 3.117 : Orchestration flow with Design Authority server.

The Design authority VNF help achieving fully automated network slicing, especially in a dynamic environment where users/administrators want to deploy slices with one-click.

3.9.5 SDN

Nuage Virtualized Services Platform (VSP) is a solution that in combination with Nuage datacenter fabric provides capability to virtualize datacenter network infrastructure and automatically establishes connectivity between compute resources upon their creation. Leveraging programmable business logic and a powerful policy engine, it provides an open and highly responsive solution that scales to meet the stringent needs of massive multi-tenant datacenters.

Nuage VSP is composed of three components:

- **Virtualized Services Directory (VSD)** is a programmable policy and analytics engine. It provides a flexible and hierarchical network policy framework that enables definition and enforcement of resource policies in a user-friendly manner.
- **Virtualized Services Controller (VSC)** is a scalable SDN controller. It functions as the robust network control plane for datacenters, maintaining a full view of per-tenant network and service topologies. Through VSC, network forwarding plane is programmed to establish connectivity for sources.
- **Accelerated VRS (AVRS)** runs inside the hypervisor and removes performance bottlenecks by offloading virtual switching from the networking stack. The CPU resources necessary for packet processing are drastically reduced, so that fewer cores are required to process network traffic at higher rates. AVRS is based on the DPDK technology from 6WIND fully integrated with Nuage VRS and the Linux environment, so that existing Linux applications do not need to be modified to benefit from packet processing acceleration. For the Linux application there is no difference between VRS and AVRS from the end user usage perspective. AVRS supports standard VMs using virtio drivers. AVRS also supports vhost with hugepages for zero-copy packet forwarding.

The Nokia high-level approach to the L2/L3 architecture targets making the L2/L3 network services-driven, i.e. make the transport network consumable and network services automated/abstracted from locations and physical devices. This is achieved through SDN/NFV evolution having “Underlay” and “Overlay” network layers with centralized control as depicted in the figure below.

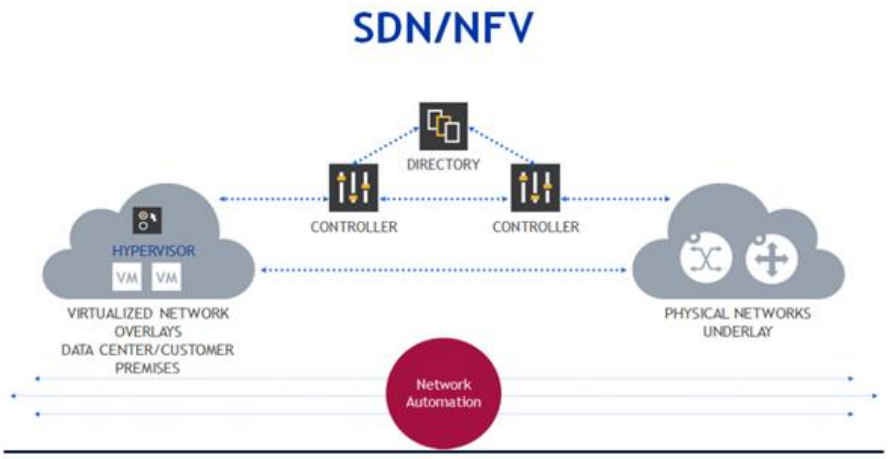


Figure 3.118 : Illustration of “Underlay” and “Overlay” network layers

The Nokia SDN solution is therefore tightly integrated with the AirFrame Data Center Hardware, the Data Center Fabric solution and the physical routing platforms.

The Nokia SDN proposal is based on Nuage solution. Our solution meets the requirements of modern datacenters by offering simplified IP fabric model, for easier operation and higher performance, together with overlay control plane operation for automated provisioning and better control on service availability. As the overlay control layer – the SDN control layer – complements the physical IP forwarding plane and manages the end-end connectivity of server connectivity, internal and external to datacenter, many of the functional requirements of traditional datacenter

Specifically, the Nuage solution combines the benefits and interoperability of BGP MPLS/VPNs with the programmability of Software Defined Networks (SDN). The Nuage Networks solution delivers automation, simplicity, programmability, and interoperability. A proven IP/MPLS networking toolset enables the extension of carrier-grade attributes associated with IP VPN services throughout the Cloud Infrastructure and allows the merger of new and existing datacenters through seamless and robust VPN services.

The Nuage Networks Virtualized Services Platform (VSP) has been designed using open standards such as OVS-DB, OpenFlow, and BGP E-VPN. The only requirement the overlay has of the underlay is it provides basic IP connectivity so every vendor (including even legacy hardware) is guaranteed to be compatible.

- It is based on the same SROS operating system as the Nokia 7750 Service Router (SR) family.
- It enables the dynamic and automatic provisioning of L2 and L3 services within the datacenter as well as across datacenters and existing IP VPN services.
- It introduces a distributed policy management approach, which brings a solution to the service provisioning problem.
- It is standards based and does not use any proprietary protocols.

3.9.5.1 Product details

As mentioned, Nuage Virtual Service Platform (VSP) is composed of three elements, the VSD, the VSC and VRS/AVRS as illustrated In the figure below.

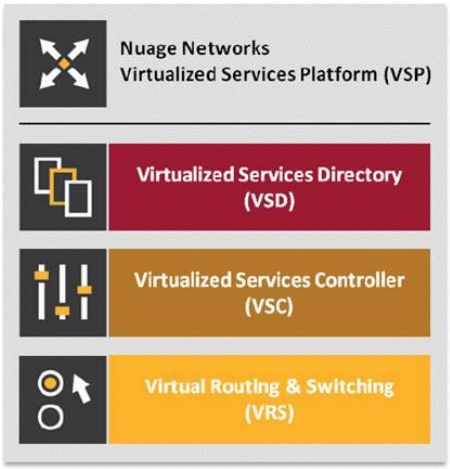


Figure 3.119 : Nuage Virtual Service Platform (VSP)

Virtualized Services Directory

The Virtualized Services Directory (VSD) resides in the Management Plane of the datacentre and provides the business and application logic that is distributed to the VSC as network configurations. The VSD is a programmable policy and analytics engine.

It provides a flexible and hierarchical network policy framework that enables IT administrators to define and enforce resource policies. It is a programmable policy and analytics engine on which service chain policies can be architected.

The VSD contains a multi-tenanted service directory which supports role-based administration of users, compute, and network resources. It manages network resource assignments such as IP and MAC addresses The VSD can be deployed as a standalone or clustered solution depending on scaling needs.

The VSD supports RESTful API's for communicating to the Cloud Providers management systems.

VSD represents event-driven policy management layer which enables zero-touch endpoint policy pull network provisioning driven by the creation of compute and storage resources in cloud management systems:

- Network primitive abstractions for policy creation of Connectivity (L2 and L3 VPN)
- Security
- Quality of Service

- Statistics collection and thresholding
- Service chaining
- Role based user access for tenant self-administration and creation of network connectivity
- Complete integration into cloud management systems o OpenStack, VMware, Cloudstack.

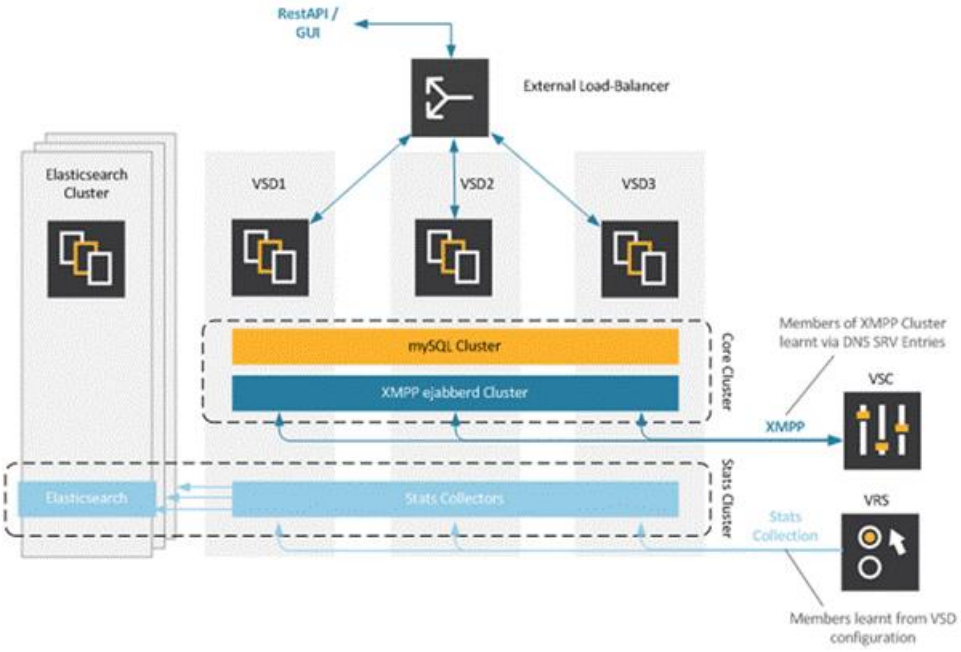


Figure 3.120 : Nuage Virtual Service Platform (VSP) architecture

One VSD entity may consists out of a cluster of 3 VSD VMs and 3 VSD Elastic Search VMs, which for High Availability reasons need to be hosted on 3 different physical servers. For 5G-VINNI, VSD will be deployed in a HA mode.

Virtualized Services Controller

The Virtualized Services Controller (VSC) is an SDN controller. It functions as the robust network control plane for DCs, maintaining a full view of per-tenant network and service topologies. The VSC resides in the Control Plane of the datacenter and provides the network control function. It co-ordinates and federates the setup and teardown of the network paths based on compute triggers received from the VRSs on the Hypervisors. Through the VSC, virtual routing and switching constructs are established to program the network forwarding plane using the OpenFlow™ protocol. Multiple VSC instances can be federated within and across DCs by leveraging MP-BGP—a proven and highly scalable network technology.

It efficiently passes these event triggers to the VSD via Extensible Messaging and Presence Protocol (XMPP) to query the authenticity and to get the application/tenant specific network configuration template to instantiate on the VRSs within the application domain.

The VSC has three main communication directions:

- Northbound: to the VSD via XMPP
- East/West: federation functions to other VSCs or IP / MPLS Provider Edge nodes via MP-BGP
- Southbound: to the VRSs via OpenFlow.

VSC is an SDN controller that programs the VRS endpoint forwarding tables via OpenFlow.

The VSC may consist of 2 VMs per NCIR cluster in an Active/Standby topology. In the 5G-VINNI Norway facility site VSC is deployed in HA mode (2 instances onsite).

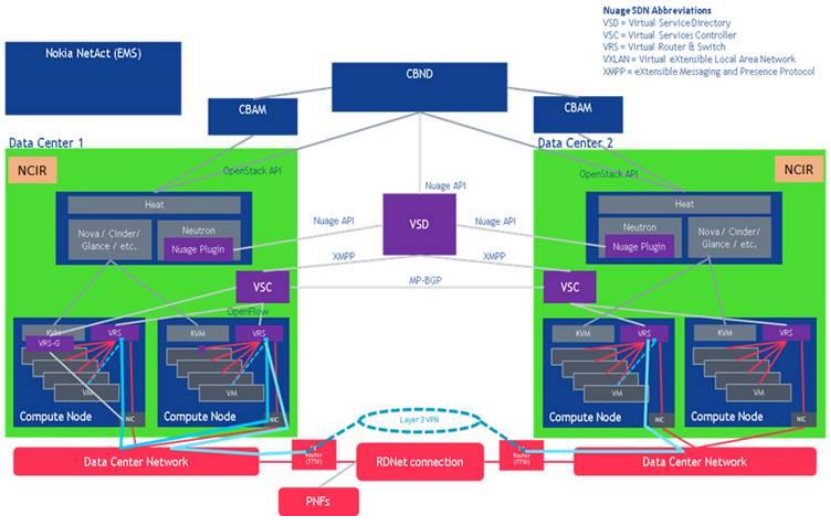


Figure 3.121 : Deployment of VSD and VSC

It is required to have the VSD and VSC operational as precondition to the CBIS overcloud installation. As such we need to host these Nuage components outside the NCIR cluster on dedicated servers. Both VSC and VSD will be deployed in a non-HA mode, thus one server (KVM) will be assigned for their deployment.

3.9.6 Network service (NS) development and integration

The Network Service as per ETSI NFV is defined as the collection of VNFs linked together by 1 or more VNF Forwarding Graphs which specify the connectivity between the various pairs of VNFs.

Figure 3.122 shows hierarchical representation of the MANO stack, exhibiting different elements in the individual layers and how do they participate in forming the Network Service.

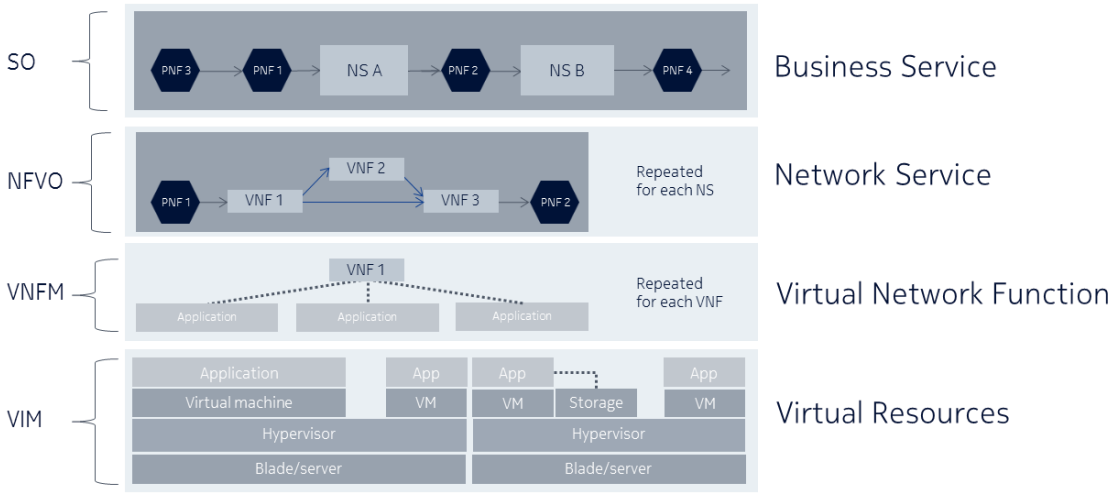


Figure 3.122 : Network Service creation and its flow

3.9.7 Service Orchestration

3.9.7.1 High Level Requirements

This section describes the high level design for the Norway facility site E2E Service Orchestration for the 5G-VINNI Release 0.

The overall target for this release is for the E2E Service Orchestration is

- Deployment of the E2E Orchestration MVP

- Process management for E2E service orchestration, automating where possible, and using Flowone to manage manual steps where they are required
- Northbound integration supporting Service Ordering, Service Activation and Configuration and Service Catalog Management
- Southbound integration to NFVO
- Southbound integration to UDM for provisioning of UE

3.9.7.2 Application Architecture

Nokia FlowOne solution is taking care of the E2E service orchestration function. E2E service orchestration is taking responsibility for:

- Centralized SOM, all service delivery is managed in one place.
- Service lifecycle management for network slices and for UE provisioning, taking care of the correct delivery sequence when delivery order contains multiple hybrid services and steps.
- Service Model, contains models on how different services are delivered and their resources reserved along different delivery processes. The system can expose service model and its detailed information via API to external systems for e.g. enabling product service mapping with versioning.
- Install Base, external or internal and manages existing subscriptions and their services and resources up-to-date information.

The Nokia Flowone architecture for Release 0 is illustrated in Figure 3.123.

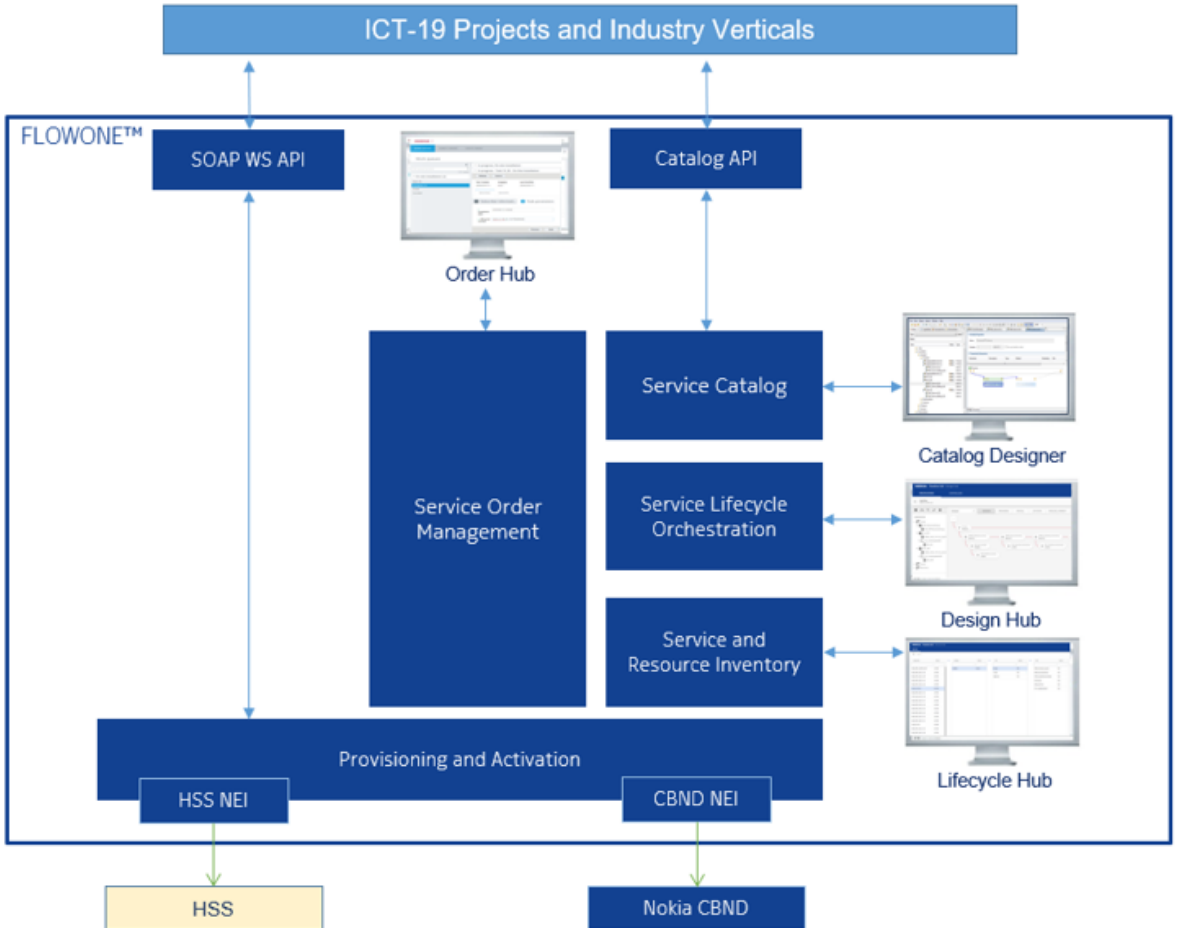


Figure 3.123 : Flowone Architecture for Release 0

The list of Flowone modules that will be deployed as part of Release 0 are listed and descried in Table 3.20.

Table 3.20 : FlowOne modules deployed as part of Release 0.

Component	Description
FlowOne Design Hub	User interface for designing service specification
FlowOne Lifecycle Hub	User interface for accessing the service inventory
FlowOne Order Hub	User interface to handle fallouts/error management
Service Lifecycle Orchestrator	Functionality for managing onboarding of network services and VNF's
Catalog Designer	User interface for designing service specification
Nokia Order Management	Nokia Order Management has the capabilities to control and monitor the progress of the service order from receipt to activation, through all the necessary physical an electronic workflow stages.
Nokia Catalog	Provides the service definitions and decompositions to more detailed service and resource level spedifications
Service and Resource Inventory	In this project, Flowone Service and Resource Inventory will be the master for network slice instances and UE subscriptions
Provisioning and Activation	Provides southbound integration capabilities to Cloudband NFVO and Ericsson HSS

3.9.7.3 Integrations

Interfaces will only be established across the ALLEGRO and PRESTO management reference points as shown in Figure 3.124. The integrations are described in Table 3.21.

Figure 3.124 : Interfaces across ALLEGRO and PRESTO management reference points

Table 3.21 : ALLEGRO and PRESTO integrations

System			Reference Point	Description
Facility Site	Vendor	Name/ Function		
Norway facility site	Unknown	CUS	ALLEGRO	Supporting basic Service Ordering Management, Service Activation and Configuration, and Service Catalogue Management operations
Norway facility site	Nokia	CBND	PRESTO	Supporting Network Service (NS) Lifecycle Management and Network Service Descriptor (NSD) Management operations across the ETSI NFV-MANO Os-Ma-Nfvo reference point
Norway facility site	Ericsson	HSS	PRESTO	Supporting UE provisioning operations towards the Ericsson HSS

The planned integrations are listed in Table 3.22.

Table 3.22 : Planned integrations.

Reference Point	From	To	Interface	Operation	Protocol	Type	Process	Operation	Description
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone SOA WS API	Create	SOAP	Asynch.	Instantiation, Configuration and Activation	Create NSI	API used for creating network slice instances
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone SOA WS API	Delete	SOAP	Asynch.	Decommissioning	Delete NSI	API used for terminating network slice instances
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone SOAP WS API	Modify	SOAP	Asynch.	Run-time	Modify NSI	API used for activating network slice instances
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone SOA WS API	Create	SOAP	Asynch.	Run-time	Create UE	API used for adding UE services to a network slice instance
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone SOA WS API	Delete	SOAP	Asynch.	Decommissioning	Delete UE	API used for deleting UE services to from network slice instance
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone SOAP WS API	Modify	SOAP	Asynch.	Run-time	Modify UE	API used for activating/suspending UE services
ALLEGRO (CUS:SOF)	CUS	Flowone	Flowone Catalog API	Retrieve Service Catalog information	SOAP	Synch.	Preparation	Retrieve Service Catalog information	API used for retrieving catalog data from the service catalog
PRESTO	Flowone	Nokia	CBND NEI	Instantiate NS	REST	NEI	Instantiation,	Instantiate NS	Re-use existing off-the-

(SOF:ICM)/ Os-Ma-nfvo		Cloudband Network Director					Configuration and Activation		shelf CBND integration
PRESTO (SOF:ICM)/ Os-Ma-nfvo	Flowone	Nokia Cloudband Network Director	CBND NEI	Terminate NS	REST	NEI	Decommissioning	Terminate NS	Re-use existing off-the-shelf CBND integration
PRESTO (SOF:ICM)/ Os-Ma-nfvo	Flowone	Nokia Cloudband Network Director	CBND NEI	Query NSD	REST	NEI	Run-time	Query NSD	Re-use existing off-the-shelf CBND integration
PRESTO (SOF:ICM)/ Os-Ma-nfvo	Flowone	Nokia Cloudband Network Director	CBND NEI	Read NSD	REST	NEI	Run-time	Read NSD	Integration via EDA. Re-use existing JAVA_HSS_CAI3G_V1 1.4.0
PRESTO (SOF:ICM)	Flowone	Ericsson HSS	Ericsson HSS NEI	Create UE	TBD	NEI	Run-time	Create UE	Integration via EDA. Re-use existing JAVA_HSS_CAI3G_V1 1.4.0
PRESTO (SOF:ICM)	Flowone	Ericsson HSS	Ericsson HSS NEI	Suspend UE	TBD	NEI	Run-time	Suspend UE	Integration via EDA. Re-use existing JAVA_HSS_CAI3G_V1 1.4.0
PRESTO (SOF:ICM)	Flowone	Ericsson HSS	Ericsson HSS NEI	Re-activate UE	TBD	NEI	Run-time	Re-activate UE	Integration via EDA. Re-use existing JAVA_HSS_CAI3G_V1 1.4.0
PRESTO (SOF:ICM)	Flowone	Ericsson HSS	Ericsson HSS NEI	Delete UE	TBD	NEI	Decommissioning	Delete UE	Integration via EDA. Re-use existing JAVA_HSS_CAI3G_V1 1.4.0

Examples of existing HSS methods:

<TASK_TYPE>create_subscriber<NE_TYPE>HSS</NE_TYPE><ACTION>CREATE_EPSMULTISC</ACTION><IMSI1>*IMSI1</IMSI1><EPS_PROFILE_ID>*EPS_PROFILE</EPS_PROFILE_ID><EPS_ROAMING_ALLOWED>TRUE</EPS_ROAMING_ALLOWED><EPS_EXT_ACCESS_RESTRICT>*EXT_ACCESS</EPS_EXT_ACCESS_RESTRICT><MSISDN1>*MSISDN1</MSISDN1><GET_FLAG>1</GET_FLAG>

<TASK_TYPE>delete_subscriber</TASK_TYPE><NE_TYPE>HSS</NE_TYPE><ACTION>DEL_EPSMULTISC</ACTION><IMSI1>*IMSI1</IMSI1>

<TASK_TYPE>modify_subscriber</TASK_TYPE><NE_TYPE>HSS</NE_TYPE><ACTION>SET_EPSMULTISC</ACTION><IMSI1>*IMSI1</IMSI1><EPS_PROFILE_ID>*APN_PROFILE</EPS_PROFILE_ID>

<TASK_TYPE>create_subscriber</TASK_TYPE><NE_TYPE>HSS</NE_TYPE><ACTION>CREATE_IMSICHANGEOVER</ACTION><MSISDN1>*MSISDN1</MSISDN1><NIMSI>*IMSI2</NIMSI><IMSI1>*IMSI6</IMSI1>

3.9.8 Services

E2E service orchestration will provide service orchestration for two categories of customer facing services,

- 5G network slice instances
- UE subscription to the network slice instance

3.9.8.1 Network Slice Services

Nokia Flowone will support the delivery of the following types of network slices,

- eMBB
- mMTC
- URLCC

Table 3.23 provides an overview of the composition of each network slice. In addition to the mobile components, a slice type will also consist of transport connectivity for the entire slice with the Telco cloud at one end and the RAN elements at the other.

Table 3.23 : Decomposition of mobile network functions into network slices.

Slice type	RAN	MME	Core	PCRF	HSS	CUDB
eMBB	Shared physical RAN	Dedicated	Dedicated (no CUPS)	Shared	Shared	Shared
mMTC		Dedicated	Dedicated (no CUPS)			
URLCC		Dedicated	Dedicated (CUPS)	Dedicated	Dedicated	Dedicated

The implementation of the network slice types where different components are related to each slice type is illustrated in Figure 3.125.

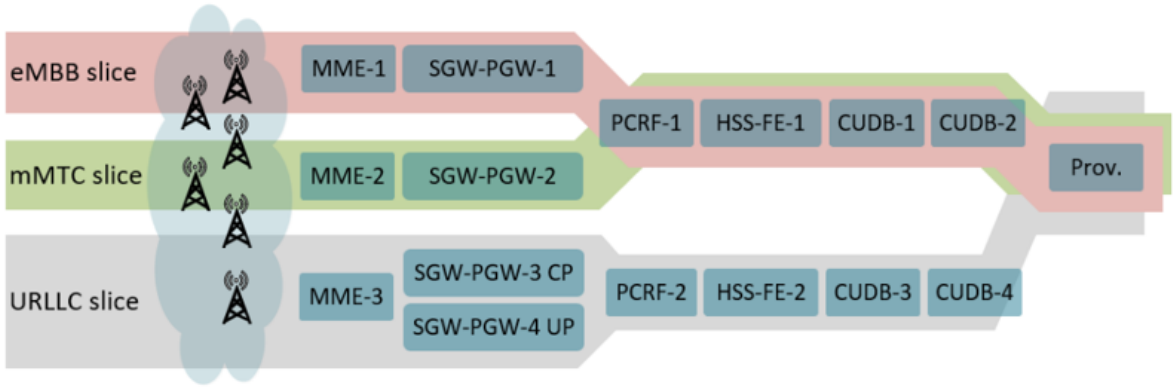


Figure 3.125 : Implementation of Network Slice Types (Release 0) where components are mapped into the Network Slice Types

The types of actions that can be performed on the different components for each slice type are listed in Table 3.24. An 'X' implies that the implemented solution will perform the corresponding action type on the corresponding component in an automated way, as part of the service fulfilment process flow. A 'M' implies such a process needs to be carried out manually.

Table 3.24 : Actions on components of network slice types

Service or Service Component	Action Types						
	Verify	Instantiate	Configure	Activate	Modify	De-activate	Terminate
eMBB		X	X	X	X	X	X
mMTC		X	X	X	X	X	X
URLCC		X	X	X	M	X	X
Dedicated MME		X	M	M	M	M	X
Shared RAN			M	M	M	M	
Dedicated Core		X	M	M	M	M	X
Shared PCRF	M	X	M	M	M	M	X
Dedicated PCRF		X	M	M	M	M	X
Shared UDM	M	X	M	M	M	M	X
Dedicated UDM		X	M	M	M	M	X
Shared HSS	M	X	M	M	M	M	X
Dedicated HSS		X	M	M	M	M	X

3.9.8.2 UE services

The UE services are presented in Table 3.25. An 'X' implies that the implemented solution will perform the corresponding action type on the corresponding component in an automated way, as part of the service fulfilment process flow. A 'M' implies such a process needs to be carried out manually.

Table 3.25 : UE Services

UE services and Subscriptions	Action Types						
	Add	Suspend	Re-activate	Delete	Apply	Modify	Remove
UE	X	X	X	X			
Subscription					M	M	M

3.9.9 Business Process Areas

Flowone will support activities in the four phases of the network slice lifecycle described by 3GPP. These phases are:

- Preparation phase
- Instantiation, Configuration and Activation phase
- Run-time phase
- Decommissioning phase

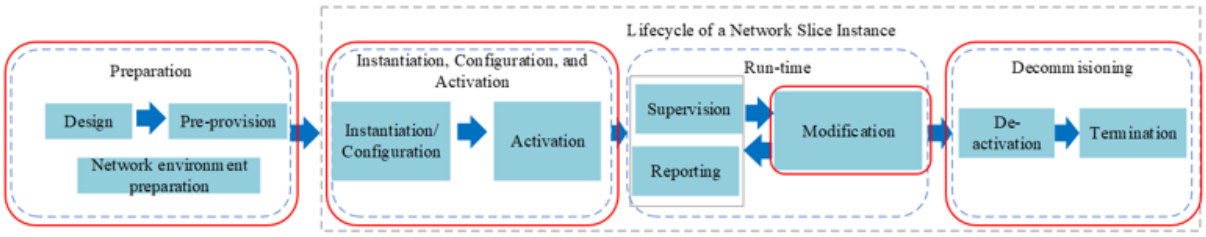


Figure 3.126 : Life cycle of network slice instance

Table 3.26 provides a short overview of Nokia Flowone's role in these phases.

Table 3.26 : Nokia Flowone role in Network Slice life-cycle management (LCM) phases

Phase	Nokia Flowone support
Preparation	Nokia Flowone will onboard network service descriptors and VNF descriptors from Cloudband Network Director, as well as service templates from RAN, Core and other domain managers. It will also onboard catalog items from the E2E service catalogs of peer E2E service orchestrators. These will be used to compose service definitions in the E2E service catalog and exposed through the northbound API

Phase	Nokia Flowone support
Instantiation, Configuration and Activation	Nokia Flowone will receive service requests from northbound systems for the instantiation, configuration and activation of network slice services. The catalog driven order process will then decompose these requests and, based upon the E2E service de-composition, enrich the request, orchestrate requests to Cloudband Network Director, RAN/ Core/domain managers, and to peer E2E service orchestrators. This will also include provisioning of UE during the preparation phase or the activation phase, dependent upon whether the serivce request is for a dedicated network slice. This will also include requesting any other network functions that are part of the service request
Run-time	During runtime Flowone will be limited to the modification of the network slice instance. Modification requests will be limited to the provisioning and de-provisioning of UE on the network slice instance. Closed loop operations will not be supported.
Decommissioning	Nokia Flowone will receive deactivation requests from the northbound systems. As appropriate it will request the re-configuration of shared/dependent resources. During decommissioning Nokia Flowone will also deprovision UE from the network slice if they are still active on the network slice to be decommissioned

The four phases can be de-composed into sub-processes as illustrated in Figure 3.127. The sub-processes outlined in green will be supported in Release 0.

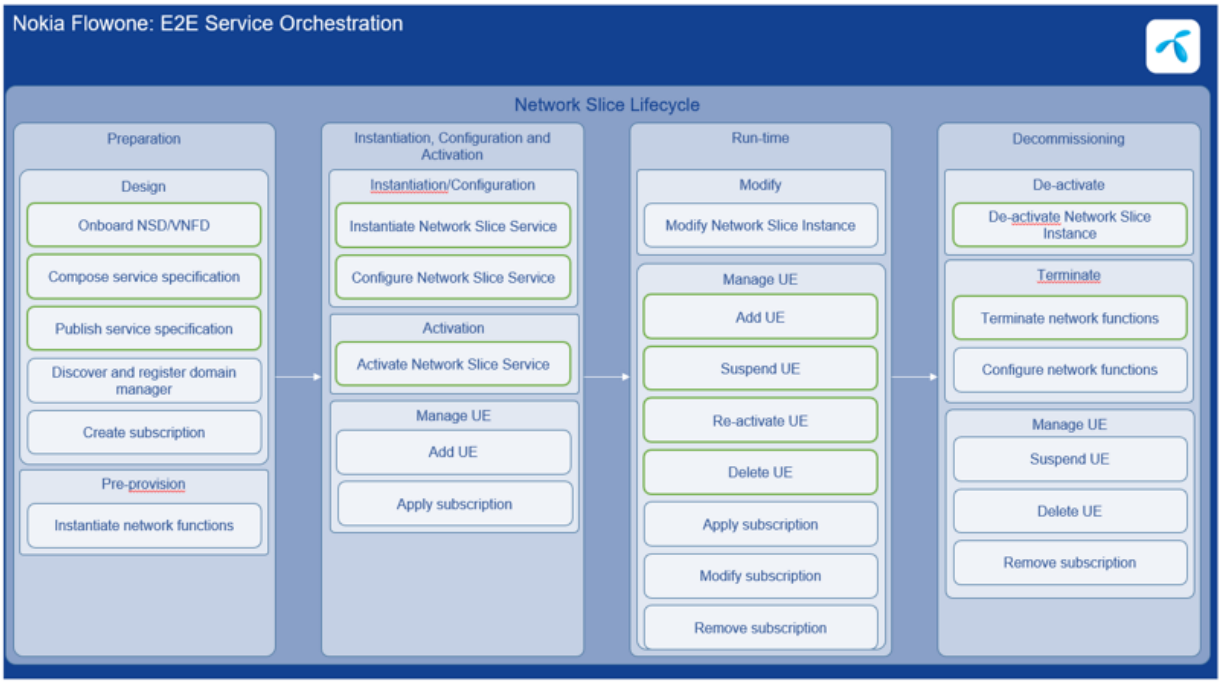


Figure 3.127 : Sub-processes of each phase of LCM with the processes highlighted in green are supported in Rel: 0 and 1 of 5G-VINNI.

Table 3.27 provides a description of Flowone's role in the sub-processes.

Table 3.27 : Role of Flow one in each sub-process

Network Slice Lifecycle Phase	Activity	Description
Preparation	Onboard NSD/VNFD	Flowone will onboard the NSD and VNFD from Nokia Cloudband NFVO. The resource facing service specifications (TOSCA-based or otherwise) are onboarded into Catalog. FlowOne SLO automatically generates a Catalog item to represent an onboarded resource.
	Compose service specification	Design and lifecycle management of service specifications. Component resource facing services and customer facing services are combined to create the full E2E orchestration flow.
	Publish service specification	Publishing a completed service specification. Once a service specification design is completed in Catalog Designer, it can be exposed to northbound customer systems.
Instantiation, Configuration and Activation	Instantiate Network Slice Service	Receiving order request for a network slice instance from customer systems. Creating all resources dedicated to the NSI.
	Configure Network Slice Service	
	Activate Network Slice Service	Activation step to activate the network slice instance.
Run-time	Add UE	
	Suspend UE	
	Re-activate UE	
	Delete UE	
Decommissioning	De-activate Network Slice Instance	Deactivation of the network slice by taking the NSI out of active duty.
	Terminate network functions	Deleting the slice from the network.

3.9.9.1 Preparation Phase

The preparation phase for a network slice instance involves:

- Onboarding of new NSD and VNFD from the NFVO and service templates or operations from the domain controllers for the RAN, Core and SDN domains
- Design and lifecycle management of service specifications in the service catalog
- Publishing a service specifications Northbound and East/Westbound
- Pre-provisioning of resources that are a pre-requisite for network slice instances

Flowone is involved in all of the stages, from onboarding, through service specification to publishing the service specifications in the service catalog. The NSD's and VNFD's are onboarded using Flowone Design Hub and stored as resource facing services in the Flowone Service Catalog. The Design Hub and Catalog Designer are then used to create the service chaining and compose the low level resource facing services into higher level customer facing services. This process also includes creating the flow of tasks to provisioning the Network Slice Instance, including any requests to the service inventory, data enrichment and mapping the flow of parameters between provisioning tasks. This information is stored in the Service Catalog. Once the service specification is created and tested it is published from the Service Catalog using Catalog Designer and can be onboarded by ICT-19 projects or industry verticals.

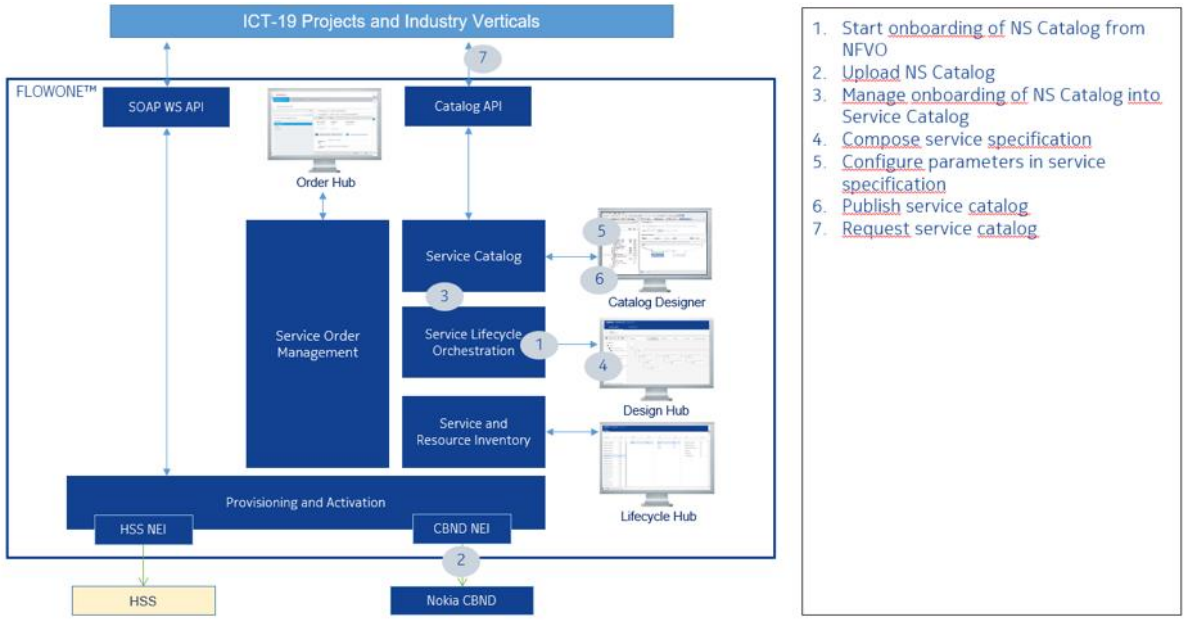


Figure 3.128 : Network Slice preparation phase

3.9.9.2 Instantiation, Configuration and Activation

During the Instantiation, Configuration and Activation phase an order is received for a new Network Slice Instance. The service orchestrator receives the order and orchestrates the instantiation of all of the elements required to create the Network Slice Instance. Once instantiated the Network Slice Instance can be configured and then activated.

During the Instantiate Network Slice Service Flowone will receive the service order from ICT-19 project or industry vertical through the Flowone SOA WS API. The order will be managed by Flowone Order Management. First the order is validated. If the order is valid, Flowone Order Management retrieves the service specification from the Flowone Service Catalog, decomposes the specification and dynamically builds the workflow for instantiating the network slice instance. Flowone Order Management then executes the workflow requesting new dedicated mobile core through the Cloudband NFVO. When the mobile core has been instantiated further configuration tasks and any

connectivity tasks will be performed manually. The flow of the manual tasks will be managed using Flowone Order Management. Users will use Order Hub in order to register the completion of each manual task. Once the network slice instance has been created the Flowone Order Management will update Flowone Service and Resource Inventory with the service information, including the resource facing services that the network slice instance is composed of.

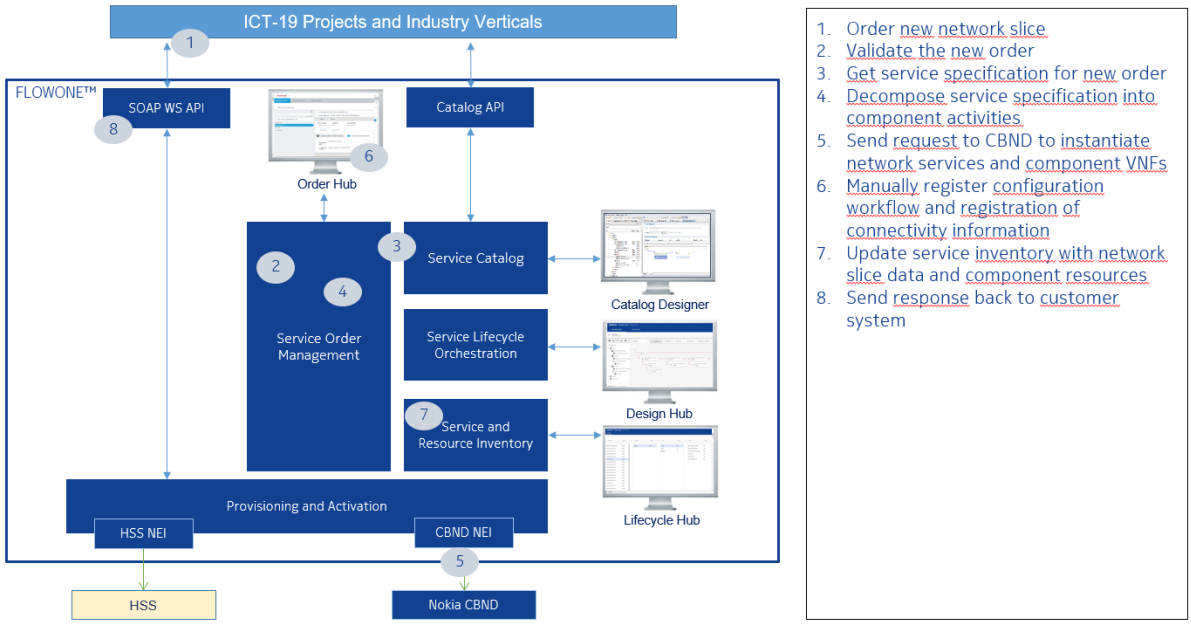


Figure 3.129 : Order process for Network Slice

3.9.9.3 Manual Order Handling and Fallout

User Interface: Order Hub UI.

Purpose: Registration of manual activities in the workflow

Order Hub will be used for generating manual tasks in the delivery flow. Each task will be used to register relevant resource facing service information during the instantiation, configuration and activation process. The registered data will be updated in Flowone Service and Resource Inventory

3.9.9.4 Run-time

During run-time Flowone will be used for adding UE to the slice, suspending UE from the slice or deactivating the UE. The process for adding a UE to a network slice instance is initiated through a service request from the ICT-19 project or industry vertical. The order will be managed by Flowone Order Management, which first validates the order. If the order is valid, Flowone Order Management retrieves the service specification from the Flowone Service Catalog, decomposes the specification and dynamically builds the instantiation workflow for the service. Flowone Order Management then executes the workflow. Where specified in the workflow Flowone Order Management will request information from the Flowone Service and Resource Inventory – such as the NSSI for the slice that the UE will be added to. The UE is added to the slice by provisioning it in the UDM. When the UE has been added to the slice the Flowone Order Management will update Flowone Service and Resource Inventory with the service information.

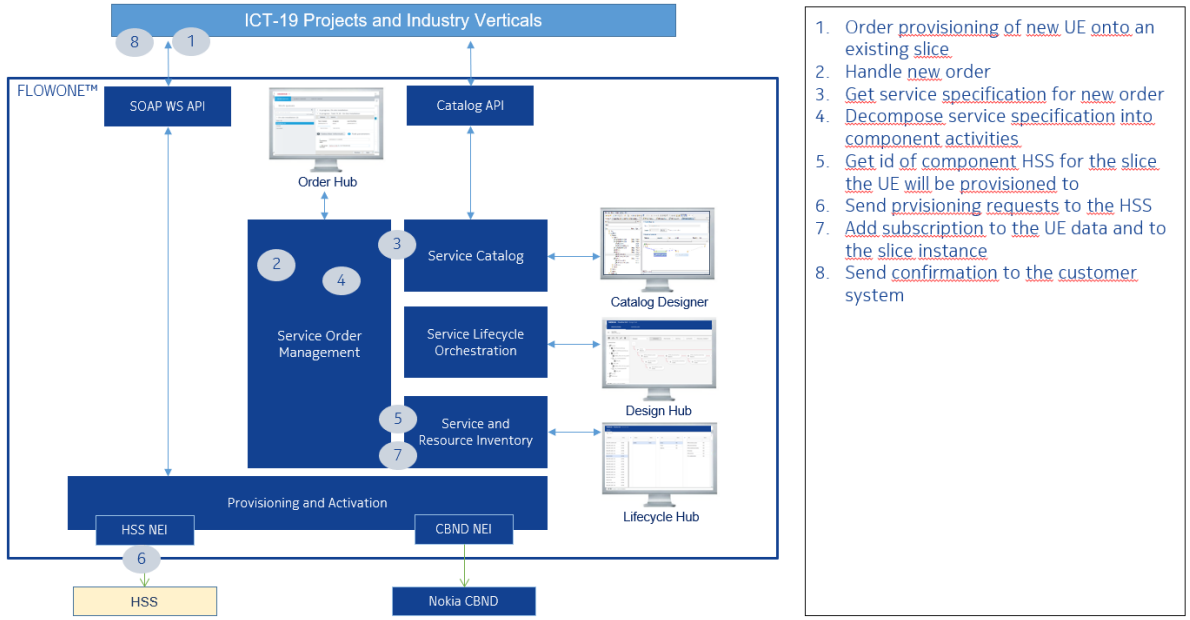


Figure 3.130 : Process of adding UE to Network Slice in Flowone

3.9.9.5 Decommissioning

Decommissioning a network slice instance includes deactivation, taking the slice out of active service, terminating any resources that are dedicated to the network slice instance and re-configuring any shared or dependent resources. After decommissioning the NSI will no longer exist. If UE's are assigned to the network slice instance when it is decommissioned, the UE's will have to be suspended from the slice.

The decommissioning process is initiated by an ICT-19 project or industry vertical. The request is sent as an order to Flowone where is it is handled by Flowone Order Management. Flowone Order Management will first validate the order. If the order is valid it retrieves the service specification from the Flowone Service Catalog, decomposes the specification and dynamically builds the instantiation workflow for the service. Flowone Order Management then executes the workflow. All UE's will have already been suspended from the network slice. The information concerning the resource facing services will be retrieved from Flowone Service and Resource Inventory and the request sent to Cloudband NFVO to terminate the mobile core of the network slice instance. All other activities that are required for the termination of the network slice instance will be performed manually. When all terminations and updates are made the record of the network slice instance will be deleted from Flowone Service and Resource Inventory. Finally, a termination notification will be sent to the customer system of the ICT-19 project or industry vertical, or to the requesting peer service orchestration function. The flow of the manual tasks will be managed using Flowone Order Management. Users will use Order Hub in order to register the completion of each manual task. Once the network slice instance has been terminated the Flowone Order Management will update Flowone Service and Resource Inventory and delete the service information for the network slice instance.

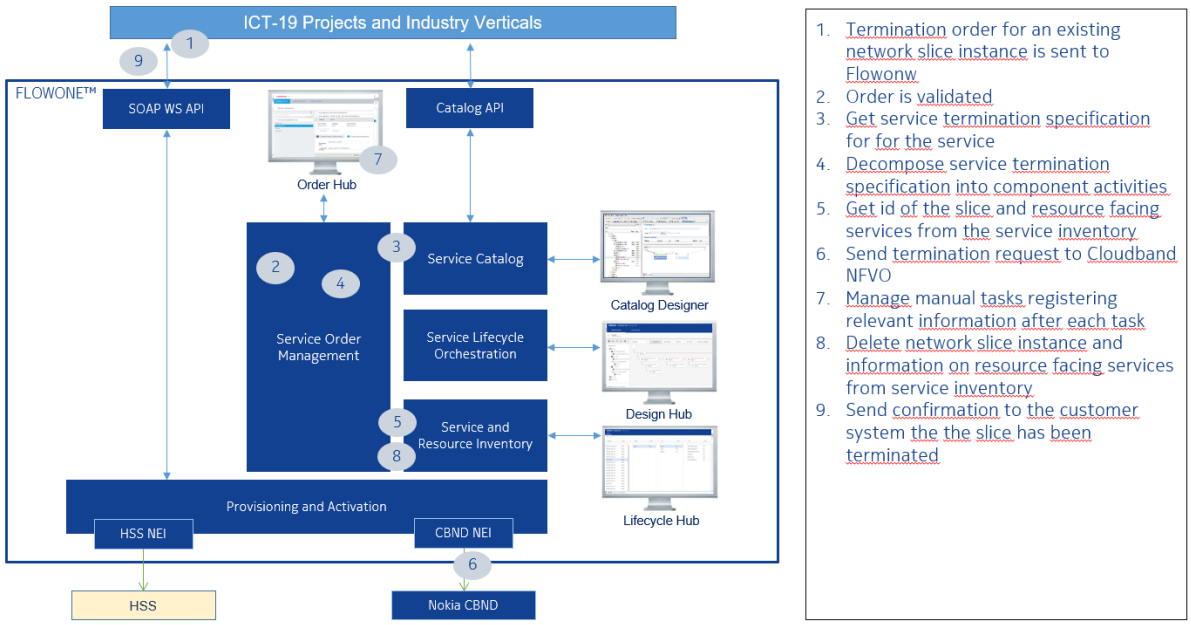


Figure 3.131 : Decommissioning process for Network Slice

3.9.10 Inventory Management

Flowone Service and Resource Inventory will be the master for managing service information concerning network slice instances and UE subscriptions. This section describes the information that is to be presented and stored in Flowone Service and Resource Inventory.

The Service Inventory will contain the classes/entities listed in Table 3.28.

Table 3.28 : Classes/entities in Service Inventory

Class / entity	Description
Subscriber	This instance object will not be used to document the actual subscriber information. Rather, this object will be used to 'group' related subscriptions. Each 'Subscriber' object instance will equate to one Main service. If a consumer/business has more than one Main service, each Main service will be documented as a new 'Subscriber' • Subscriber ID (provided with the Order – not a key and not mandatory) • Subscription identifier or Agreement No. (for Main Service) • Related Subscriptions
Subscription	• Subscription identifier • IMSI • Subscription type (identification of subscription type to facilitate CFS ID change. Determined by BST logic).
CCFS	
CFS	Derived by Nokia FlowOne for each CCFS Subscribed component ID or Agreed component ID
RFS	Derived by Nokia FlowOne for each CFS

3.9.10.1 Flowone Service and Resource Inventory Data Model

The high level Flowone Service and Resource Inventory data model is depicted in Figure 3.132.

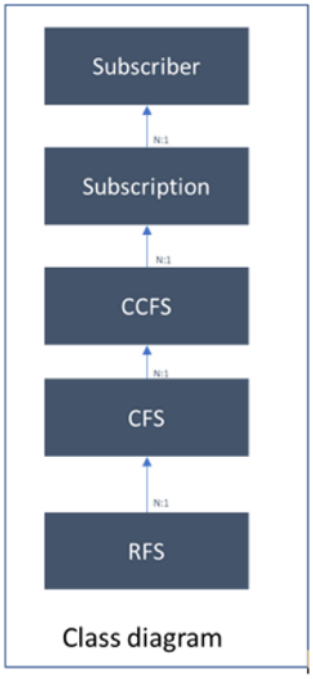


Figure 3.132 : Service and Resource Inventory model in Flowone

- RFS layer: The lowermost layer of the mode, the Resource Facing Service (RFS), is related to the network resources. Each network command is mapped to one or more RFS in the service model.
- CFS layer: RFSs in the previous layer are grouped to represent a Customer Facing Resource (CFS).
- CCFS layer: CFSs in the previous layer are groups to represent a Composite Customer Facing Resource (CCFS). This layer will be used to establish a 1:1 mapping to product catalogue CFS ID.
- Subscriber/Subscription layer: The subscriber and subscription(s) are defined at this level. A service representation may be defined for which the CFSs and RFSs are identified. The Subscriber class will be used to group subscriptions related to one Main service.

3.9.10.2 Instance diagrams

The network slice service specifications will be modelled as customer facing services in the Flowone Service Catalog. The customer facing services will be composed of re-usable components. The service specifications will follow the model for services in Flowone Service and Resource Inventory.

The illustration in Figure 3.133 provides a conceptual view of how the model will look.

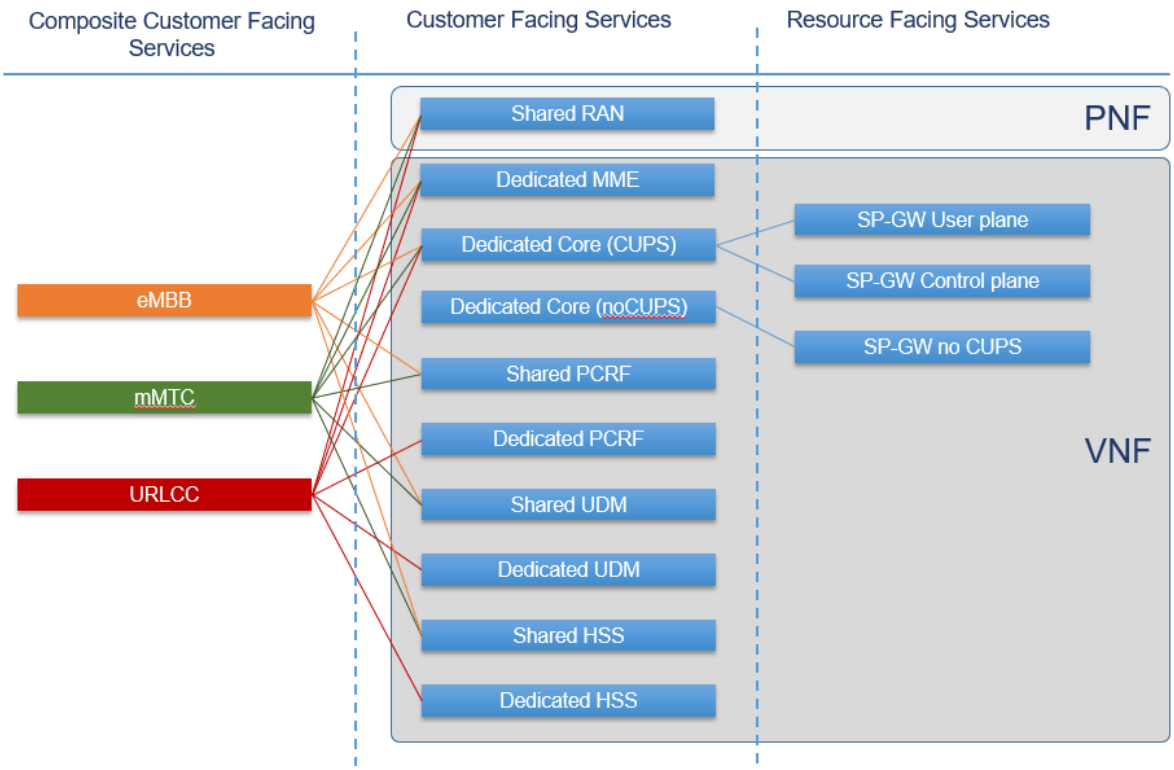


Figure 3.133 : Modelling of customer facing service in FlowOne

3.9.11 User Interface, Reports and Data Export/Import

3.9.11.1 User Interfaces

User Interfaces (UI) in Release 0:

- OrderHub – Web UI. Primary function via UI to handle manual tasks.
- Order Management – Web UI available but not required by any user groups
- Catalog Designer – Thick client. Primary function to design new services & publish new services (CCFSs).
- InstantLink – Web UI. Primary function via UI is to monitor provisioning tasks.
- Lifecycle Hub – Web UI. Primary function via UI is to interrogate subscriptions (Flowone Service and Resource Inventory master for active subscriptions).

3.9.12 End-to-end network slicing automation

Operators may have several slices to be deployed in one site or multiple sites. Even in a small environment, like Telenor's 5G VINNI, we have initially planned for 5 slices that are used for different purposes, like eMBB, mIOT, URLCC. Some of them use 5G Core SA and some non stand-alone. In the future we may have more slices used by the verticals. This could be expanded to 10, 20 or even 100 slices in the future, where we should be able to terminate what we don't use and then deploy a new slice. We should also be able to restore the previous slice if it is needed.

The **'One click'** deployment sounds the ideal scenario for network slicing onboarding, but if we want to achieve this, we have to prepare a lot of things in advance. Some of the me will be described in this chapter.

Automation is really important for any network size and if we templetize the network slices, we can deploy the same service even in different sites, by just updating the environmental parameters (eg site names, IP addresses, application names etc).

First is the templatization phase, where operators may plan the potential slices and based on those can build a list of network services and theirs VNFs. Several templates needs to be prepared for the services, so we can be used for onboarding.

The second phase is the level of automation and decide what needs to be orchestrated in order to automate the service deployment. In this phase the interfaces have to be considered as well.

3.9.12.1 Dynamic templates

Templates may include VNFDs, NSDs and services templates in Service Orchestrator. Those usually are parameterized, so they can create the services dynamically.

5G-VINNI Norway facility site deploy three NSA slices as illustrated in Figure 3.134.

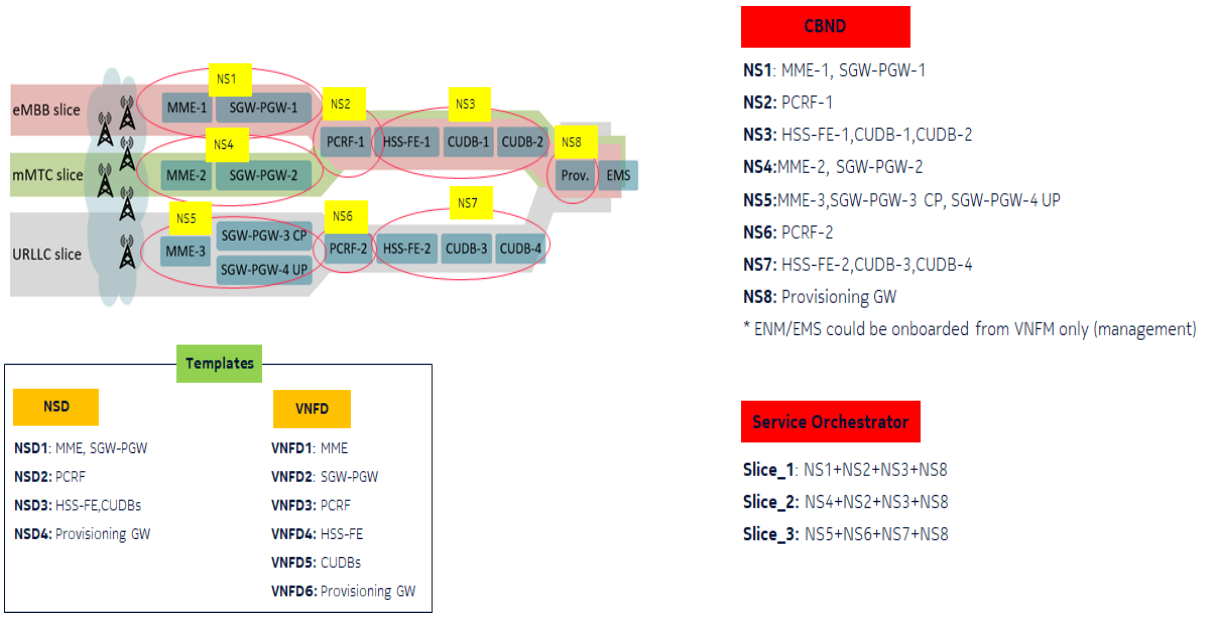


Figure 3.134 : NSA Slices in Norway Facility site

The VNFM will manage the VNFDs and it can view each VNF without knowing under which network service is. NFVO will give a higher view by grouping the VNFs (or other elements) into a network service. Finally, Service orchestrator will see the network slices that use one or more network services. Some of those network services might be common in different slices.

The first step is the VNF supplier to prepare the VNFD per VNF type in a dynamic way, so they can be reused multiple times, by using different input files.

The network services will be consisted of several VNFs. Operators may decide what is the most appropriate grouping, since the aim is to repeat the network service several times.

In our case we use 4 different network services templates

NSD1: includes MME and SPGW. The requirement was that each slice will have its own pair of MME-SPGW and be isolated

NSD2: PCRF only, because in some case PCRF will be common, but in some other cases it will dedicated instance

NSD3: includes HSS and CUDB, since those are always paired

NSD4: it's only the provisioning GW, This may be deployed once per site.

The template of NSD1 can be reused for all 3 slices, but NSD2 only during the deployment of slice-1 and slice-3.

The service orchestrator will have different view, since it sees each slice individually with its own network services. If the first slice is deployed, service orchestrator will create and deploy the network services NS1 (MME/SPGW) + NS2 (PCRF) + NS3 (HSS/CUDB) + NS8 (ProvGW). All those network services are logically bundled into one slice.

Now if operators or users wants to deploy the second slice, Service Orchestrator will identify that only NS4 (new MME/SPGW) needs to deployed by CBND, but the new slice will be composed of the existing NS2,NS3,NS8 and the newly deployed NS4.

3.9.12.2 Orchestration and interfaces

When we create a network slice or service, most may think that this includes the VNF onboarding only, but in reality there are more aspects to this.

Automating the network slice deployment means that the service is deployed and that users can use it immediately. The aim is to achieve this with one click.

The deployed VNFs alone cannot offer a service, because a service needs also to consider:

- networking, that covers the connectivity between the VNFs, using L3 routed networks
- connectivity to other DCs (transport)
- other nodes or PNFs that may be part of the service
- firewall policies, because by default the communication between VNFs in different security zones is not allowed.
- user provisioning: for the service may be ready to be used, users should be provisioned as well.

The challenge in this phase is that the ecosystem has different components that may come from different vendors. Some of these may use open source or standard APIs/interfaces, but some of them proprietary APIs.

Wherever it is possible we tried to use standard interfaces, such as:

- **SOL003**: between NFVO (CBND19.5) and G-VNFM (CBAM 19.5) to deploy the VNFs
- **SOL005**: between NFVO (CBND19.5) and Service Orchestrator (FlowOne) to create and deploy the network services
- **TMF 641**: between Service Orchestrator and BSS (OpenSlice) to deploy the network slices
- **Neutron API**: between NFVO (CBND19.5) and VIM (NCIR18) for creating the networks in Openstack
- **Heat API:** between VIM (NCIR) and VNFM (CBAM 19.5) for deploying the Openstack resources/stack regarding the VNFs.

In the 5G-VINNI Norway facility site, both orchestrators, NFVO and Service Orchestrator need to have interfaces to the nodes as shown in Figure 3.135.

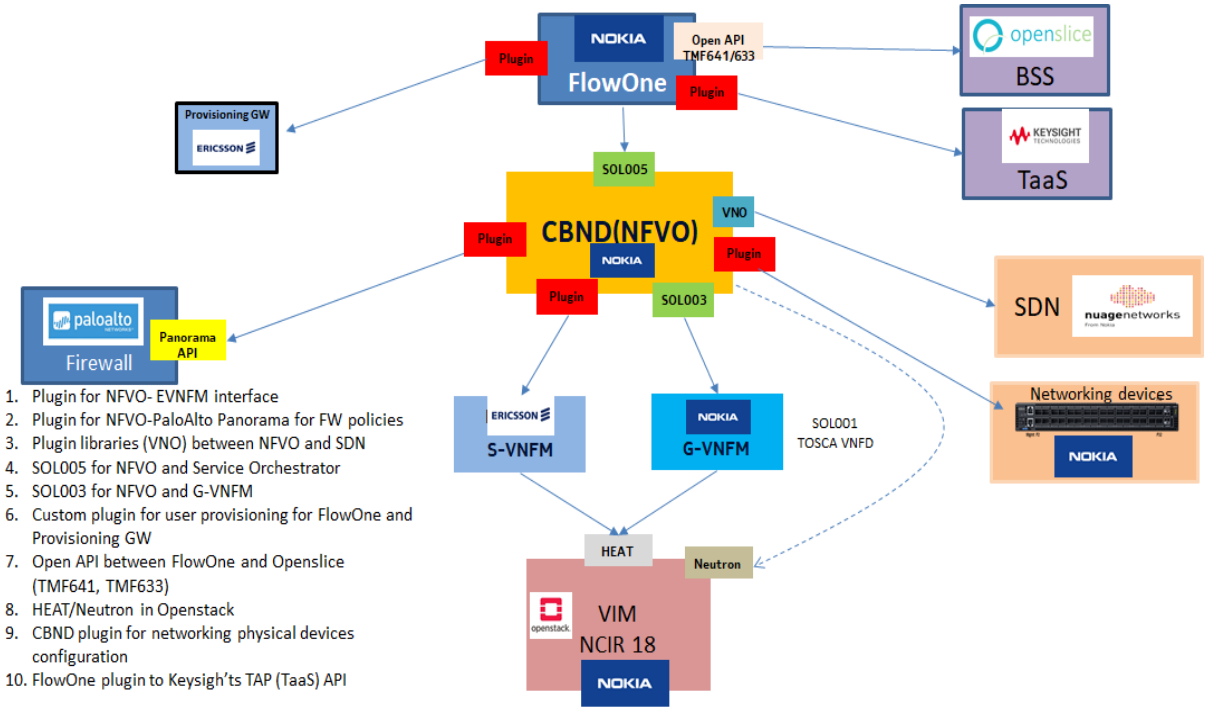


Figure 3.135 : Orchestration interfaces in Norway facility site

As can be seen, there are also proprietary interfaces that have been developed for automating the network slices:

- **NFVO to Ericsson S-VNFM**: this is an interface built on top of SOL003, since S-VNFM has some proprietary interfaces as well. A plugin was developed in Nokia's NFVO to deploy Ericsson VNFs
- **NFVO to Nuage SDN:** Nuage SDN exposes an API for network creation in VSD. In 5G-VINNI Norway facility site there is also a need to create static routes for load-balancing the traffic to Ericsson VNFs. Those also need to be created in Nuage SDN. This can be automated by triggering the correct API calls from CBND, using the VNO plugin (Virtual Network Orchestrator).
- **NFVO to Nokia's physical switch:** In central site we use Nuage SDN, but in Edge sites we deployed physical switches (SDN-less solution). The external networks need to be created in physical switches. We developed a plugin in CBND to allow the orchestrator to configure networks and static routes inside the airframe switch (Z9100).
- **NFVO to PaloAlto firewall:** As mentioned, VNFs will by default not be allowed to talk to each other by security policy, because they are deployed in different security zones. The traffic goes via the FW, hence, the required security policies need to be added in PaloAlto's Panorama EMS prior the service realization. A plugin was developed in NFVO (Nokia CBND) that is tagging the VNF's IP in the firewall in order to allow the traffic between them.
- **Nokia Service Orchestrator to Ericsson Provisioning GW:** for the NSA slices, we use the DECOR. The subscribers should be provisioned with the right DECOR label in HSS, so during registration the core networks knows which slice the user wants to use. A plugin was developed in Nokia's FlowOne, which defines, updates and deletes the users in HSS via Ericsson's provisioning GW. Once the slice is deployed the next step is the service orchestrator to provision the users for that slice.

Finally, operators and users need to make sure that the network slice has been deployed successfully and it can satisfy the initial requirements. In this case, a group of test cases can be automated in a remote node and executed by the Service orchestrator at the end. The plan is to use Keysight's TAP

for verifying the network slice (TaaS - Test-as-a-Service). A plugin needs to developed in FlowOne that will use the TAP's exposed API.

In the future, we may need to develop more plugins and consider new slices as well. This may include the 5G Core and SA slices, where service orchestrator needs to define the slice details in 5G core components (instead of DECOR).

In order to orchestrate the SA slices based on CNFs the NFVO should consider deployment of CNFs via CaaS and VNFs via VNFM. Potentially there might be a hybrid slice (VNF/CNF) in the 5G-VINNI Norway facility site environment.

3.9.12.3 Orchestration flow for network slice deployment in two sites (Defence slice)

For the case of the slice for the Defence, the solution is based on autonomous edge, where the core network components are deployed in Edge and Central sites, with the requirement that if connectivity between the two sites is lost then the service will not be impacted.

This is a distributed slice in two sites, where different network solutions are used. In central site an SDN-based solution (Nuage) whereas in the Edge a simplified networking solution is used with a physical switch (Airframe Z9100).

In the Defence slice there are two types of VNFs. One is Ericsson 5G vEPC (NSA) and 3rd party VNFs (Metaswitch, Hermod). The deployment will use both Ericsson S-VNFM and G-VNFM.

The network slice deployment may be initiated from a user in the service orchestrator or in the BSS (OpenSlice). The steps for the service deployment are shown in Figure 3.136.

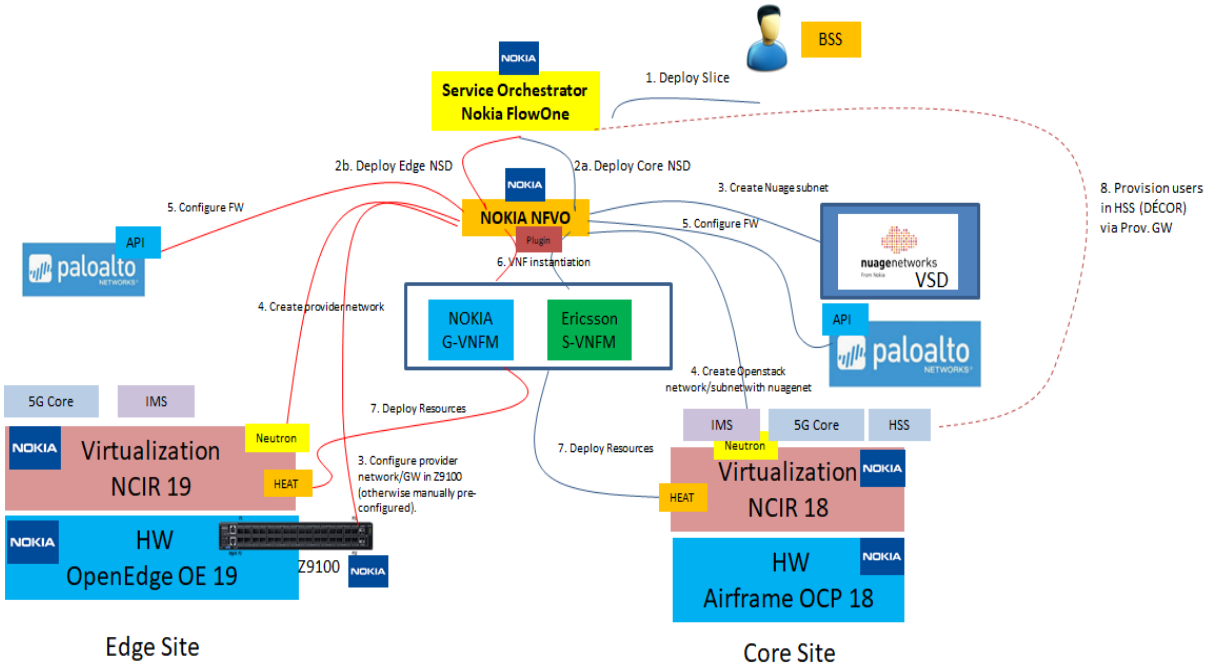


Figure 3.136 : Orchestration flow for network slice deployment in two sites (Defense Slice)

The steps are:

A user initiates the service from BSS

Service Orchestrator will trigger the creation and deployment of several network services in two sites, via NFVO (CBND)

NFVO will create first the needed external networks of the VNFs in Nuage (Central site) and also the networks in the physical switch (Edge site). This includes the networks for all the VNFs that will be deployed in this service (Ericsson and non-Ericsson VNFs)

The networks need to be created also in Openstack neutron, in both sites and under the right tenant.

NFVO will also tag the VNF IPs based on the policies that Telenor shared. After that step, the communication between the needed VNFs will be allowed and the rest will be blocked

NFVO will use the SOL003 interface to G-VNFM to deploy the non-Ericsson VNFs in both sites and also the customized plugin to Ericsson s-VNFM to deploy the Ericsson VNFs.

Both G-VNFM and S-VNFM will use the heat templates and deploy the resources in Openstack-based VIM (NCIR), in both sites. After that step the service is ready, the networks and static routes have been defined and also firewall allows the communication between the needed VNFs.

The last step is users to be provisioned for the slice. Service Orchestrator will automatically add the users in HSS via provisioning gateway and set the correct DECOR tag. Users will be able to register into the newly deployed service.

3.10 Satellite

Nodes with satellite back-haul are being implemented for the Norway facility. In the first phase the satellite will be used as backhaul for a fixed 5G RAN site that will be located in a military base close to Oslo. In a potential second phase, a nomadic 5G RAN may be placed on a maritime vessel (e.g. ferry or cruise ship) that is already using satellite and LTE communication services. Network Slicing will then be demonstrated over satellite with prioritization mapping to Slice ID in 5G. Edge sites will be deployed with the 5G RAN so that local breakout to low latency and high throughput applications can be realized.

All Edge Nodes are interconnected through the Telenor satellite fleet and Telenor teleport facility site located in Nittedal, Norway.

Configuration of a 5G RAN site with satellite backhaul:

- Standard VSAT terminal connecting via satellite to a Gateway with Internet backbone access
- Either shared access with DVB-S2 ACM outbound and A-TDMA inbound or SCPC both ways
- VSAT feeding local area network with various devices (5G RAN, WiFi, vessel operation)
- Perhaps access to multiple satellites for high capacity and/or reliability

3.11 Security

Palo Alto Networks Next Generation Firewall PA-5220 will be used for segmentation between security classes within the 5G-VINNI Norway facility site. Configuration and Management of Firewall policies will be conducted using the Panorama M200 management appliance as the EMS system for PA-5220, while the orchestration of policy object will be executed by Nokia CloudBand Orchestrator. The PA-5220 and Panorama M200 are implemented in two different physical boxes (i.e. not running on NFVI).

In order to achieve best practice level of security within the datacentre there will be 3 security classes for services and 1 for management:

- *Exposed*, which includes VNFs facing RAN, Internet and Other Networks
- *Non-Exposed*, which includes subscribers' database frontend VNFs
- *Secure*, which includes subscribers' database backend VNFs
- *Management*, including MANO, VNFMs, EMS and E2E Service Orchestrator

The PA-5220 Firewall will separate mentioned security classes and apply security policies for traffic passing between different security classes. As it is planned to have four different security classes and only one physical firewall is used for the deployment, the Virtual System feature of PANOS will be used. PANOS is the operating system of Palo Alto Networks Firewalls.

3.11.1 Virtual Systems Overview

Virtual systems are separate logical firewall instances within a single physical Palo Alto Networks firewall. Rather than using multiple firewalls, the Norway facility site can use a single firewall and enable virtual systems on them. Each virtual system (vsys) is an independent, separately-managed firewall with its traffic kept separate from the traffic of other virtual systems.

A virtual system consists of a set of physical and logical interfaces and sub-interfaces (including VLANs and virtual wires), virtual routers, and security zones. It is possible to choose the deployment mode(s) (any combination of virtual wire, Layer 2, or Layer 3) of each virtual system. Virtual systems segment any of the following:

- Administrative access
- The management of all policies (Security, NAT, QoS, Policy-based Forwarding, Decryption, Application Override, Authentication, and DoS protection)
- All objects (such as address objects, application groups and filters, dynamic block lists, security profiles, decryption profiles, custom objects, etc.)
- User-ID
- Certificate management
- Server profiles
- Logging, reporting, and visibility functions

3.11.2 Palo Alto Networks PA-5220 High Level Configuration

The following firewall configuration is used in the 5G-VINNI Norway facility site:

- PA-5220 Next Generation Firewall
- 8 x SFP+, 10 Gbps optical interfaces
- Threat Prevention, Wildfire, Global Protect and URL Filtering subscriptions
- Panorama M200 Appliance

Based on this, separation between security classes can be implemented based on available ports and 4 virtual systems.

The logical separation of virtual systems and relevant security classes separated by different virtual systems is illustrated in Figure 3.137.

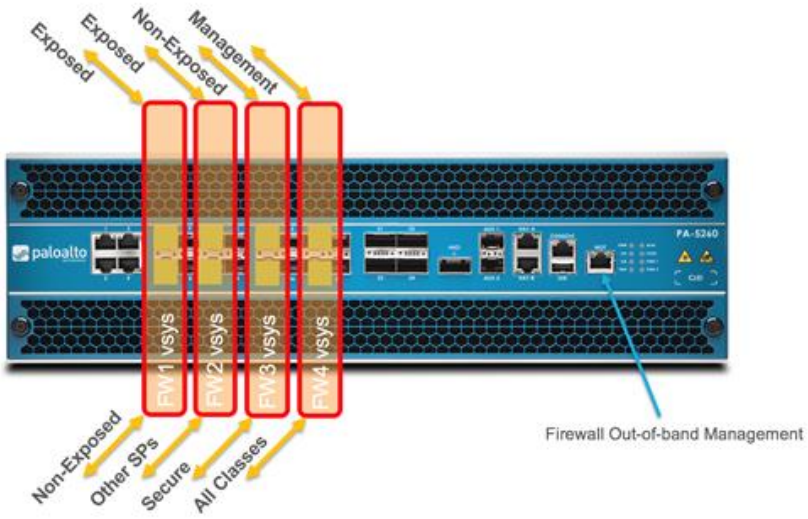


Figure 3.137 : Logical separation of virtual systems in the physical firewall for security classes

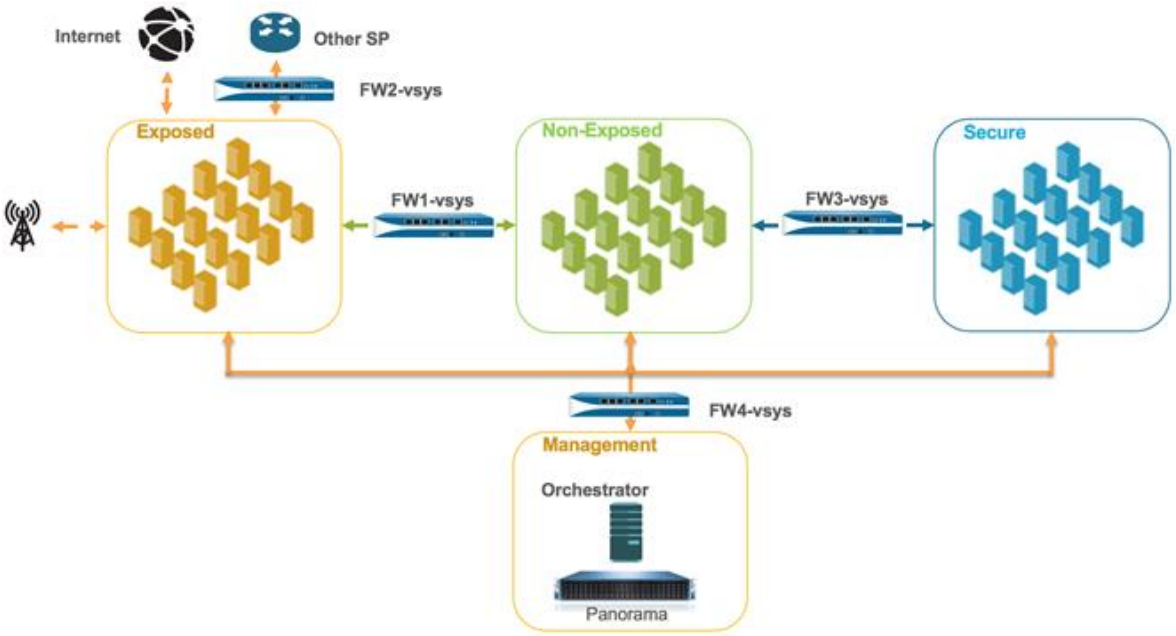


Figure 3.138 : Palo Alto Networks Firewalls management with Panorama M200 appliance

The network level representation of the implementation of the firewall with security zone class separation is illustrated in Figure 3.138.

The Panorama EMS system enables the administrator to configure, manage, and monitor the Palo Alto Networks firewalls with central oversight. The three main areas in which Panorama adds value are:

- Centralized configuration and deployment
- Aggregated logging with central oversight for analysis and reporting
- Distributed and role-based administration.

From Panorama standpoint different virtual systems of PA-5220 will be considered as separate logical firewalls and different set of policies will be applied to different virtual systems. However, certain configuration related to firewall management as a device cannot be separated between different virtual systems, e.g. firewall software, firewall dynamic updates. As a result, the logical separation will be implemented mainly targeting security policies and related security profiles.

3.11.3 Security Zones Implementation and VRF design

The implementation design of the security zones needs to consider the interconnection between the WBX switches and the firewall. In order to adapt for the different rules and policies, the one physical PA-5220 is split in 5 different and independent logical firewalls, whose traffic is distinguished respectively by the use of different VLANs. In the Release 0 architecture it is expected that Firewall 1 implement the policies between the Exposed and Non-Exposed classes, Firewall 3 between Non-Exposed and Secure. Finally firewall 4 is used to check the communication between the management class and the other 3 classes. On the other hand, for external traffic i.e., internet and traffic from other 5G-VINNI facility sites, firewall 2 and 5 are used respectively.

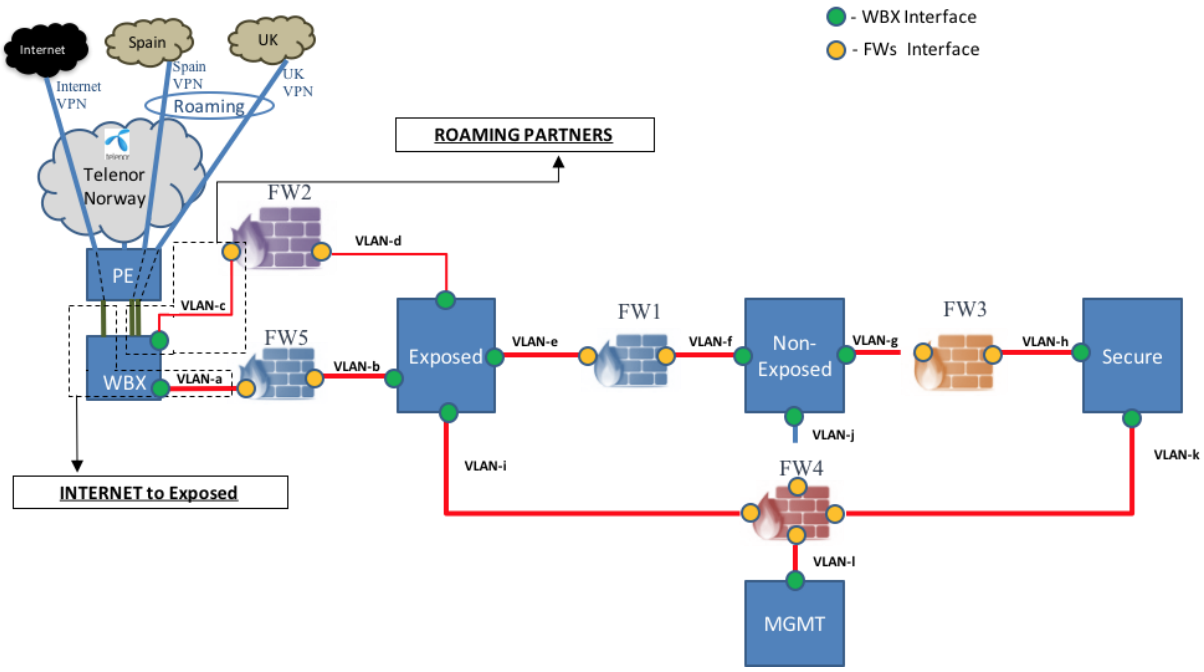


Figure 3.139 : Security Zones Implementation Design

The successful implementation of security zones policies depends on the VRF design. Figure 3.140 present the VRF in the framework on the security classes assigned, and the respective VNFs involved.

		INFRASTRUCTURE				MGMT					EXPOSED			NON-EXPOSED				SECURED	
		CBIS	VSD	PA EMS	VLAN	CBND	FlowOne	E/// VNFM	E/// EMS	VLAN	MME	SPGW	VLAN	PCRF	HSS-FE	EDA	VLAN	CUDB	VLAN
VRF	OAM-INFRA																		
	OAM	x	x	x		x	x	x	x	2112/ 2212 - FW4	e	e/x	2109/ 2209 FW4	e	e/x	e	2110/ 2210 FW4	e/x/e	2111/ 2211 FW4
	LDAP													e	e		2107/ 2207 FW3	e	2108/ 2208 - FW3
	DB-SYNC																	e	internal
	SIGNALING										e/e/e	e	2105/ 2205- FW1	e	e/e/e		2106/ 2206 - FW1		
	RAN										e/e	e/e							
	MEDIA										e	e/e/e/e	internal						
	INTERNET											e							

Figure 3.140 : VRF Design for Security Zones Implementation (e – eVIP, x – subnet).

3.12 Distributed IoT Data Fabric

The Cisco Edge and Fog Processing Module (EFM) will be used to collect telemetry from IoT devices, transform data, and take action on that data. For example, actions can generate alerts, create reports, or display dashboards. The data can also be used in other applications such as machine learning and Enterprise Resource Management.

3.12.1 EFM Concept

The Cisco EFM is a scalable software system that sits above the packet network. It is core to the Digital Platform for IoT and delivers data to applications. EFM is a high performance, scalable distributed computing system for IoT where computing can be performed anywhere where it is needed, including the Edge, Fog, data centre, or cloud.

EFM is based upon the Distributed Services Architecture (DSA), an open source platform and development environment for IoT devices and micro-services. DSA presumes data heterogeneity so all telemetry must be normalized into a common format; This abstracts the applications from the specific communication protocol of the devices. DSA also presumes distributed micro-services, allowing the deployment of applications anywhere they are needed.

3.12.2 EFM Components

Each EFM component is a node. Nodes in EFM have data, expose actions, have a profile, and can have children. Following brief description of EFM components:

NodeAPI

The nodeAPI is the common communication method for all nodes and facilitates all messaging between entities in a standardized manner. The nodeAPI implements *websockets* for transport.

Message Broker

The broker is a core component to the EFM system. The broker acts as a message router for incoming and outgoing streams. The links that are connected to the broker act as originators of the data streams. All communication between nodes is performed via the message broker, which is based on a publish-subscribe bidirectional message exchange. Connections between brokers form a graph, which provides introspection capabilities, allowing for a client or application to traverse the entire graph and discover all nodes and capabilities.

DSLinks

The link is a domain-specific function that is exposed to the EFM network. The link implements the nodeAPI and enables the micro-services (implementing specific IoT protocols for instance).

DataFlow Engine

This streaming engine provides event-driven data transformation and logic execution capabilities. It is used to build simple to complex algorithms that clean data, build tables, transform, perform mathematical and string functions, and easily export using the built-in functions.

The DataFlow Editor is used to create dataflows. It provides a powerful graphical development environment that not only allows for the management of a dataflow, but also for a block-by-block output examination for troubleshooting and experimentation.

Parstream Database Historian

Purpose-built database to handle the massive volumes and high velocity of data as well as analytics at the edge, fog and data center nodes.

3.12.3 Architecture

To form a scalable and distributed stream processing network, the architecture allows brokers to connect to other brokers. This allows for deployment of brokers, links, and micro-services anywhere in the system. The DSLinks are connected to the IoT objects and act as originators of the data streams.

Figure 3.141 presents an architecture example.

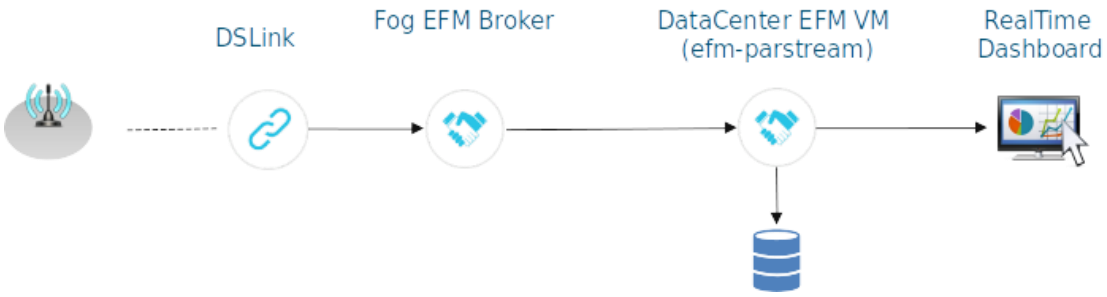


Figure 3.141 : Architecture Example: Message Broker, DSLink and Partsream

3.12.4 Deployment

In 5G-VINNI, EFM will be deployed on VMs that can be orchestrated as VNFs:

- VMs running EFM central broker (Storing the data, managing and monitoring the system).
- VMs running Edge broker (The first broker communicating with IoT objects)

The following resources are required for the EFM:

- VMs running EFM central broker: 2vCPU, 4G RAM, 20GB, Centos
- VMs running Edge broker: 1vCPU, 1G RAM, 10GB, Centos

3.13 Test Equipment

The testing tools will be described further in 5G-VINNI WP4 Deliverable 4.1. All testing tools will run on the NFVI except the massive traffic generator. The Norway facility site will host a set of testing tools that are centralized and used for all the main facility sites in 5G-VINNI. In addition to the centralized tools across all facility sites there will be tools for testing and visibility that will be deployed locally in each main facility site.

The connectivity design is being established and will be reported in a later deliverable.

3.14 User Equipment

Below is a list of other mobile 5G devices that have been used:

- Huawei Mate 20X (NSA, sub6)
- Huawei Mate 30X (NSA, SA, sub6)
- Huawei P40 (NSA, SA, sub6)
- Huawei 5G CPE (NSA, SA, sub6)
- Huawei mmWave CPE (NSA, mmWave)
- Motorola 5G plus (NSA, sub6)
- Sony XQ-AT51 (NSA, sub6)
- Askey mmWave CPE (NSA, mmWave).

Mobile 5G devices from the following suppliers did not connect since they do not allow use of the network code (24212) in the 5G-VINNI Norway facility site:

- Samsung
- Apply

3.14.1 WNC Pocket Router

The WNC pocket router can be seen in Figure 3.142 with specifications given in Figure 3.143.

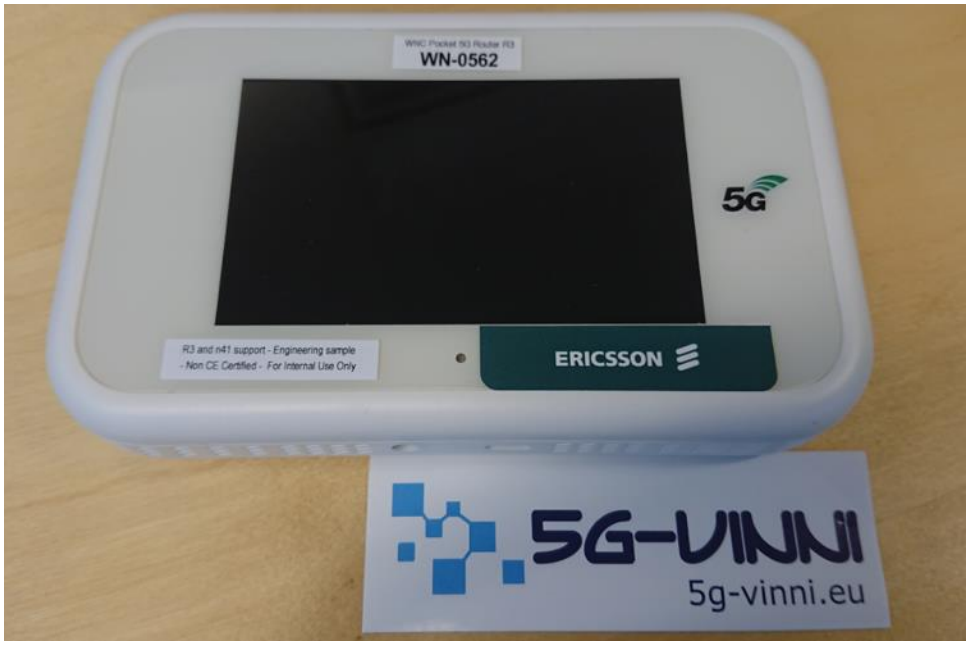


Figure 3.142 : WNC Pocket Router (5G UE) picture

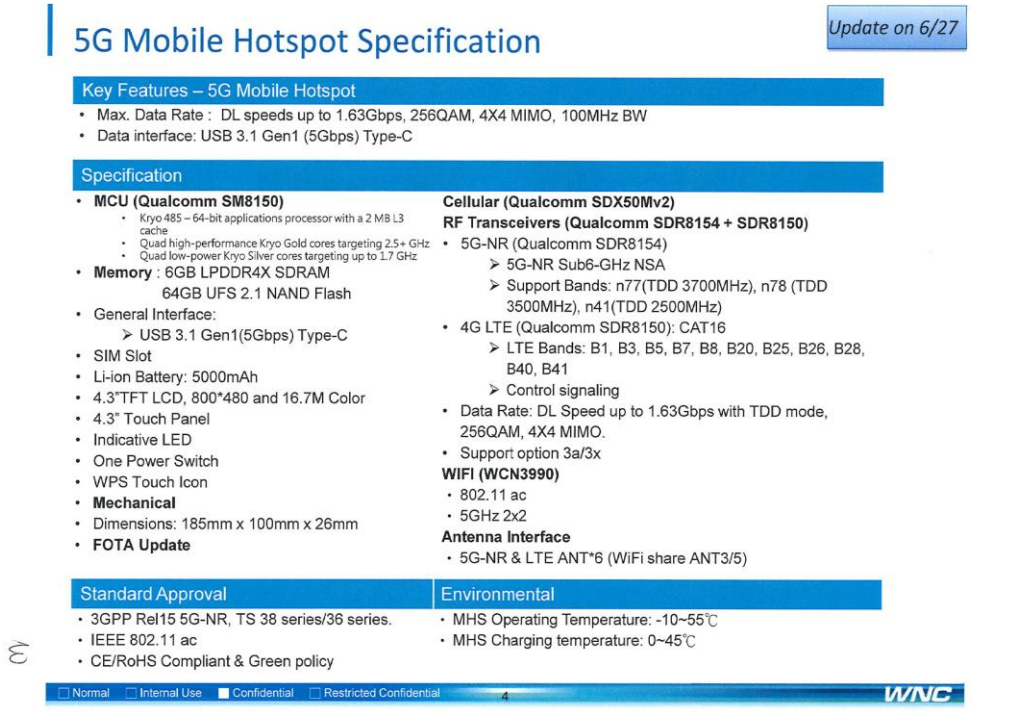


Figure 3.143 : WNC Pocket Router (5G UE) specication

3.14.2 Huawei CPE

Huawei 5G CPE v1.0 is the one available for testing at Release 0. Huawei 5G CPE Pro will be available during the Release 0 period and onwards.

3.14.2.1 Huawei 5G CPE v1.0

Figure 3.144 : Huawei 5G CPE Pro v1.0

Based on Balong 5G01-chipset, Air Interface Protocol 5G NSA/SA radio access modes are supported. NSA access is used by default. It takes about 5 minutes to connect the CPE to the SA network for the first time.

The CPE on the 3.5 GHz band supports the following: 5G C-Band CPE Product Description

- 4 – 4:1/8:2/7:3 downlink-to-uplink subframe configuration
- A PS data rate of up to 1000 Mbit/s in the downlink and 100 Mbit/s in the uplink in the best-case scenario in the NSA networking – A PS data rate of up to 855 Mbit/s in the downlink and 100 Mbit/s in the uplink in the best-case scenario in the SA networking.

Table 3.29 : Huawei 5G CPE v1.0 specifications

Item	Description
Protocol compliance	● WAN: 5G NR (3GPP Release 15) ● LAN: IEEE 802.3/802.3u ● WLAN: IEEE 802.11b/g/n, IEEE 802.11ac
Operating frequency band	● 5G NR: 3400 – 3800 MHz ● LTE: Band 1/3/4/7/38/39/40 ● WLAN: 2400 – 2483.5 MHz; 5250 – 5825 MHz **NOTE** Different areas support different frequency bands. In proprietary extension scenarios where only tests can be performed, band 4/40 can be used as the NSA access anchor of n78 and band 4/38/39 can be used as the NSA access anchor of n77.
Working bandwidth of the WAN port	NR 2T4R: 100/80/40 MHz (TDD) NR 2T2R: 100/80 MHz (TDD) LTE 1T2R: 5/10/15/20 MHz (FDD), 10/15/20 MHz (TDD)
Memory capacity	2 GB NAND Flash, 4 GB DDR4 SDRAM

3.14.2.2 Huawei 5G CPE Pro

Figure 3.145 : Huawei 5G CPE Pro

Dimensions

- 99 mm x 107 mm x 215 mm

Weight

- About 700 g (excluding the power adapter)

  * Product size, product weight, and related specifications are theoretical values only. Actual measurements between individual products may vary. All specifications are subject to the actual product.

Wireless

- Transmission Standard: 802.11ax/ac/a/n 4 x 4 & 802.11b/g/n 2 x 2, MIMO
- Wireless Transmission Rate: DBDC, 5100 Mbps
- Wireless Frequency Band: 2.4 GHz & 5 GHz, dual-band auto-selection
- Antenna Type: Dual-band Wi-Fi antenna with six signal amplifiers

Hardware

- CPU: Balong 5000 multi-mode chipset
- Network Port: One Wan / Lan GE port, one Lan GE port, one TEL port, one SIM card slot (Nano-SIM)
- Key: Reset / Power / H, support HiLink device one-button pairing, compatible with WPS
- Led Indicator: 5G / 4G / Wi-Fi
- External Antenna: Two 5G antenna extension ports, allowing users to purchase antennas

Software Functions

- APP: HUAWEI SmartHome App
- HUAWEI HiLink Smart Home: Support HiLink device password-free access, modify Wi-Fi name / password auto sync
- More Functions: Mobile network (5G / 4G) access, Ethernet access, 5GHz preferred, SMS service, firewall, PIN protection, MAC address filtering, Wi-Fi encryption authentication, VPN tunnel / VPN penetration, IP penetration, IPv6 and IPv6 / IPv4 dual stack, multi-APN, WeBUI, administrator maintenance, HOTA, etc

Attributes

- Power : <24 W
- AC/DC Power Supply: AC: 100 V - 240 V 50 Hz / 60 Hz, DC: 12V / 2A
- Temperature: Operating temperature: 0 °C ~ 40 °C, storage temperature: -20 °C ~ +70 °C

- Humidity: 5% ~ 95% (non-condensing)

Packing list

- HUAWEI 5G CPE Pro: 1 (standard configuration)
- Power Adapter: 1 (standard configuration)
- Quick Start: 1 (standard configuration)
- Ethernet Cable: 1 (standard configuration)
- Warranty Card: 1 (optional)
- External Antenna: 2 (optional)

3.15 Facility-site configuration (LLD)

The LLD contains detailed configuration related information like IP addresses, routing information, configuration parameters etc. The LLD will not be covered in this HLD document

4 Facility-site slices, services and applications

4.1 NSA ICT-19 Slices

There are two NSA slices Slice #1 supporting the eMBB use case and Slice #2 supporting the mMTC use case as shown in Figure 4.1, where it can be seen how the VNFs are deployed and shared between the two with slices. VNFs are redundant by themselves, there is no need to have spare VNFs. For more details about VNF please see section 3.3.

Both slices provide data connectivity to external PDNs with defined QCI and QoS. In default configuration maximum throughput (MBR UL and MBR DL) is provisioned in UDR subscriber profile and PCRF accepts such CCR coming from PGW that contains the maximum speed. It is possible to configure speed restriction on PCRF based on uses case needs.

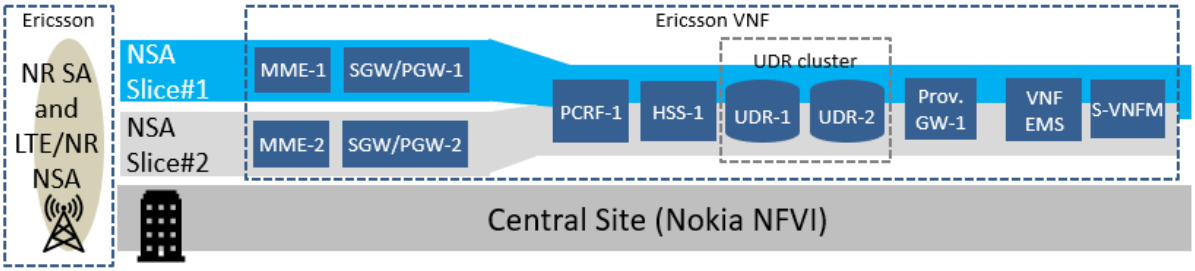


Figure 4.1 : NSA ICT-19 Slices

5G EPC consists of the same network functions as in LTE network but with additional functionalities to support 5G use cases and connectivity options.

Figure 4.2 show the implemented interfaces.

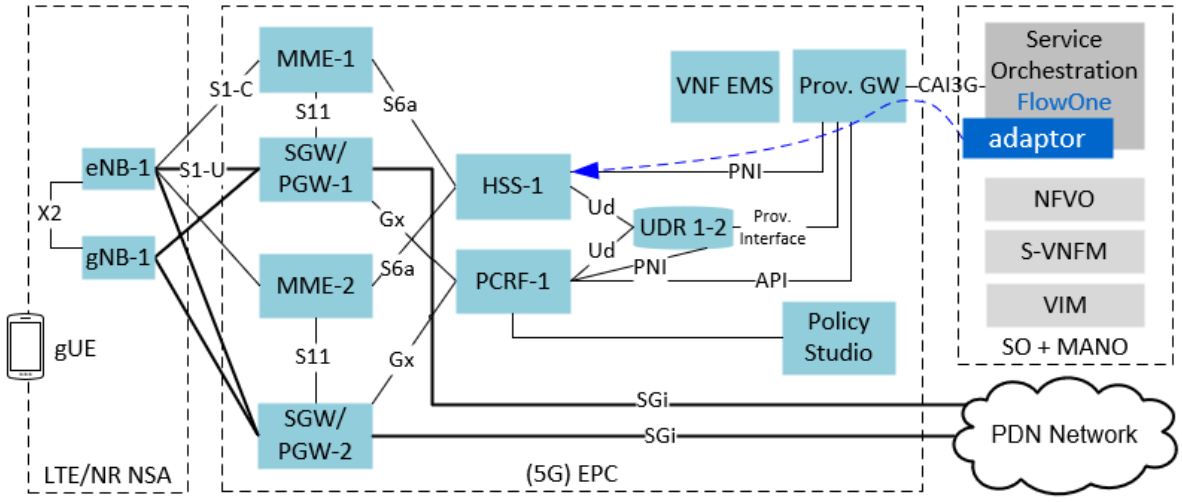


Figure 4.2 : NSA ICT-19 Topology

4.1.1 Provisioning

For provisioning a total of three profiles are created per slice. The profiles differ according to QCI and maximum allowed speeds. The subscription data is held in UDR which is common for both slices.

Three profiles in each slice are shown in the tables in Figure 4.3. Slice 1 profiles are on the left and slice 2 profiles are on the right.

	"gold"	"silver"	"bronze"
Name	s1-gold	s1-silver	s1-bronze
Usage type	10	10	10
QCI	6	7	8
Maximum DL	Uncapped	500Mbps	50Mbps
Maximum UL	Uncapped	500Mbps	50Mbps

	"gold"	"silver"	"bronze"
Name	s2-gold	s2-silver	s2-bronze
Usage type	20	20	20
QCI	6	7	8
Maximum DL	Uncapped	500Mbps	50Mbps
Maximum UL	Uncapped	500Mbps	50Mbps

Figure 4.3 : Provisioning profiles

The profiles can be updated at any time and will automatically trigger a reattach procedure for the subscriber in order to apply the new values to the data session.

In order to differentiate between different slices, all profiles have a UE Usage type parameter. The parameter is used for DECOR and differs between slices. With this parameter the user can easily be assigned to i.e. slice 1 by using UE usage type 10.

4.2 SA ICT-19 Slices

Two SA slices are implemented as illustrated in Figure 4.4. SA slices as seen from the overall facility solution are shown in Figure 2.1. At the time of writing, both sliced are designed with equivalent functionality and can provide the same type of service.

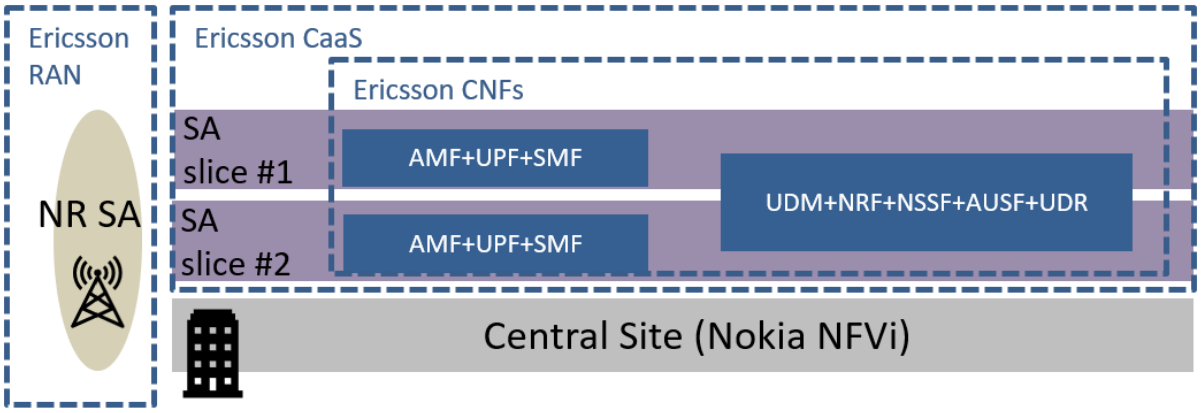


Figure 4.4 : SA ICT-19 Slices

More information on SA core network design and included functions can be found in Section 3.4.

4.3 Military Service and Slice Implementation

(note that *Military* and *Defense* are used interchangeably throughout this section, and that *Military Slice* and *Defense Slice* means the same.)

4.3.1 Service Description

The Services required by the Military mobile users can be categorized into two primary mobile services:

- *Military Service*: is an isolated network exclusively for Military users. Access to internet should by default be rejected, but it should be possible to allow access to and from some trusted domains. Basic communication services shall be supported, which may include (but not limited to) data, voice, messaging and video. Communication between Military users in this slice and with Military applications should use end-to-end encryption due to exchange of classified information.
- *Commercial Service*: is a service giving access to the commercial 5G network including traditional services not limited to data, voice and SMS.

Military users shall be able to select which service to use; the *Military Service* or the *Commercial Service* depending on the scenario.

In addition to the basic communication services mentioned above (data, voice, messaging and video) there are value added services for the *Military Service* that can be required for some or all of the Military users as listed below:

- Push-To-Talk (PTT), which might be realized using Mission Critical PTT (MCPTT) standard or alternatively an Over-The-Top (OTT) PTT service supporting end-to-end encryption.
- Fixed Mobile Convergence (FMC), involving communication between Military users connected across the mobile and fixed Military network.
- Prioritized Quality-of-Service (QoS) for Military users.
- Autonomous Edge Cloud, i.e. if connectivity between an edge cloud and central cloud is lost the edge should be able to serve all Military users connected to that edge.
- Satellite backhaul for redundancy in case the fiber or microwave backhaul connection is lost, might be required for certain locations only.
- Coverage-on-Demand, i.e. if a device wants connectivity in an area not covered by the commercial network it should be able to use alternative connectivity, e.g. satellite.
- Many-to-many communication between a group of Military users, which require deployment of 3rd party VNFs for discovery and user group management.
- 5G RAN as sensor, e.g. to detect jamming or to detect drones using mmWave.
- Drone control.

4.3.2 Service Requirements

In this section, we describe some of the important requirements for the Military. However, this list does not cover all requirements which is use case dependent where privacy concerns may exist, and hence it goes beyond the scope of this paper.

4.3.2.1 Isolation

Isolation can be defined as the property that services in a slice may operate without any direct or indirect influence from activities in other slices, and unsolicited influence of the infrastructure providers. This requirement is a must for a military use case. In order to achieve Isolation two different approaches must be considered.

The first approach is isolation at the resource level. Each network domain (RAN, Transport and Core) has particular mechanisms to isolate its resources. In the RAN, different subcarriers or separated radio resource blocks can be used. In the transport, different lambdas at the optical fibre or different logical MPLS paths can be used. In the core, different datacenters, availability zones, computational hosts, VMs or dockers provide different kind of isolation.

The second approach is isolation at the management level. First, the management tools allow the coordination of the isolated resources within and across the different network domains in order to enable unified and harmonized service across them. Second, the multitenancy concept that allows that only the resources that are allocated to a given slice can be managed In isolation without interfering with other slices.

4.3.2.2 Security

As Military transfer classified information over the network security is of high importance. For this, some attack vectors in general mobile networks should be removed such as complete isolation from the Internet, no external SS7 links, and no international roaming partnerships. Regarding roaming, one exception might be if the Military wants to use multiple mobile networks for improved coverage and reliability.

End-to-end encryption is an important security requirement for the military, i.e. the data should be encrypted from mobile device to mobile device. The user plane traffic is encrypted on a hop-by-hop basis on the path from the user device to the gNB node and to the mobile core nodes in both NSA and SA mode, i.e. user plane traffic is decrypted when received at the node and encrypted again when transmitted from the node. End-to-end encryption can be realized using Secure Real-time Transport Protocol (SRTP) or alternatively at the application layer using an application that implements end-to-end encryption for e.g. voice, video, messages and data.

In addition to security in the RAN, transport and mobile core domains, security must also be ensured in the telco cloud domain. Hence, the VNFs and applications in the *Military slice* shall be completely isolated from other VNFs and applications running in the cloud. Such isolation must be ensured on all the compute, storage and network layers.

4.3.2.3 High Availability

Military is classified as critical communication and thus high availability is important. Uptime in any given area should be 99,999%. Mechanisms should be considered to assure high availability at base station (e.g., redundant BBU), at backhaul (satellite as backhaul for fibre, autonomous edge), core network (high redundancy scheme, autonomous edges).

Robustness against jamming is important for the Military, since jamming techniques are used in situations (e.g., war) to hinder the Military from communicating. The robustness against jamming with the use of massive-MIMO and beamforming should be investigated further.

4.3.3 Service Implementation

Two slices are used to deliver the services required by the Military; the *Military slice* and the *Commercial slice*. In the following, we describe the implementation of the *Military slice*, which is based on the 5G URLLC slice type presented in the general slice design of the Norway Facility. The reason is that it uses separated CP and UP for SGW/PGW, which enables the implementation of efficient edge-central site designs. It also enables implementation of low latency services with application functions deployed in the Edge.

The *Military slice* implementation is illustrated in Figure 4.5.

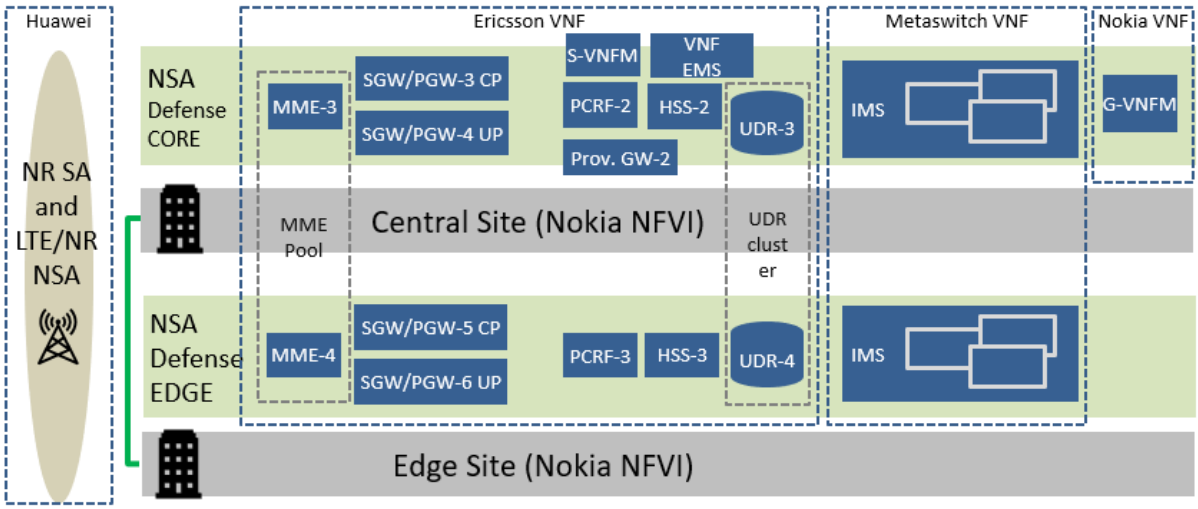


Figure 4.5 : NSA Edge Slice

All the VNFs are dedicated for the *Military slice* to maintain full isolation from the other slices, whereas for the *eMBB* and *mMTC* slices (see slice #1 and #2 in both Figure 2.1 and Figure 4.1) there are some VNFs that are shared (i.e., PCRF, HSS and UDR). In the *eMBB* and *mMTC* slices the MME and SGW/PGW are dedicated due to the need for different functionality and configuration for the service

types (e.g. LTE-M and NB-IOT for the *mMTC* slice). The VNFs in the *Military slice* are deployed on a shared NFVI in this deployment, but might also be physically separated if physical isolation is a requirement, which can be using physical separation within the same datacenter or using separate datacenters.

The Military slice is deployed across a central and edge site. To support the deployment of Autonomous Edge. It can be seen that all the main 5G EPC and IMS functions are deployed in both the central and edge sites, which is because the Edge shall be able to be autonomous. When an edge site is autonomous it will be able to operate as a full mobile network in the area covered by the edge even if the connectivity to the central site is down or if the central site is down.

An Autonomous Edge can be deployed at a single base station co-located with the BaseBand Unit (BBU) and the CSR (referred to as "Access Edge"), or in a regional location co-located with the PE router in the transport network (referred to as "Regional Edge") to provide services to a larger geographical area.

The detailed implementation of the NSA EPC and IMS including the VNF topology and communication interfaces across the Central and Edge sites is illustrated in Figure 4.6.

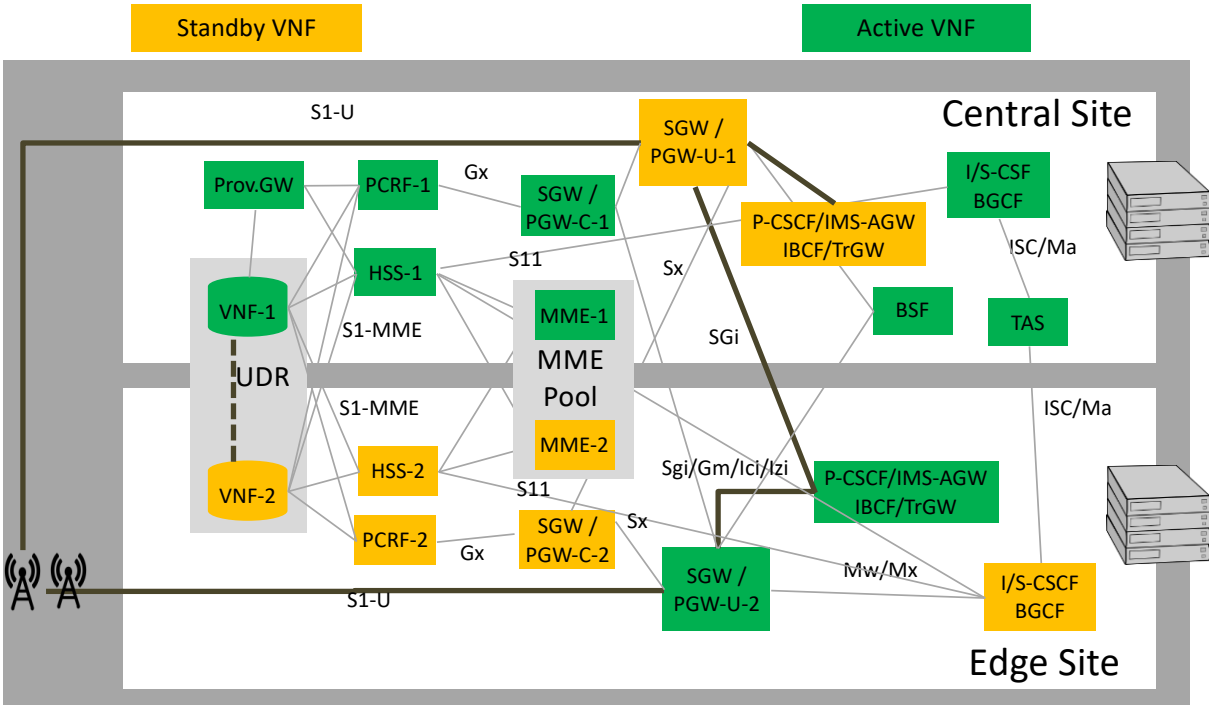


Figure 4.6 : NSA Edge VNF Topology

In normal operation where the link between central and edge sites are operational the VNFs that are green will be active and those that are orange will be standby. In the case of a link failure (e.g. fibre cut) to the edge site or failure of the central site, the edge site will become autonomous in which all the VNFs in the edge site will become active.

Control and User Plane Separation (CUPS) architecture is used where the SGW/PGW UP is active in the edge, whereas the other VNFs are inactive in normal operation. The reason for active SGW/PGW UP is to enable local breakout to time critical applications such as drone control or real-time analytics or to save transport network bandwidth using applications such as Content Delivery Network (CDN).

The gNB uses load sharing used to select the MME to be used. In this case the MME-1 (central) is configured with 100% load and MME-2 (edge) with 0% load. When MME-1 fails or connectivity to it is lost, the gNB will send the traffic to MME-2. Traffic will automatically recover to MME-1 when it is up or connectivity to it is established again.

4.3.3.1 Provisioning

Related to provisioning, military slices will inherit similar provisioning model as NSA slices. Four main profiles will be created. Profiles are s3-gold, s3-silver and s3-bronze. Fourth profile is s3-ims which specifically enables the use of IMS based VoLTE functionality via additional APN. Maximum speeds and QCI values are as provided in below table. UE Usage Type (UUE) for Defence slice is 30.

	"gold"	"silver"	"bronze"	VoLTE
Name	s3-gold	s3-silver	s3-bronze	s3-ims
QCI	6	7	8	5
Maximum DL	Uncapped	500Mbps	50Mbps	1Gbps
Maximum UL	Uncapped	500Mbps	50Mbps	1Gbps

Figure 4.7 : Provisioning profiles

For purposes of testing OTT applications gold profile shall be used as it provides highest rates and highest non-GBR QCI thus prioritizing the traffic. Since the OTT applications that will be implemented do not support Rx interface, in future, special policies and packet inspection design can be considered to create dedicated bearers with highest GBR QCI.

For purposes of DECOR all military users will be using specific UE Usage Type so all military traffic is separated and routed towards Military slice.

4.3.4 Military Applications and Services

The Military want to integrate and onboard a set of applications in the Military slice:

- HERMOD service
- OTT Push-to-Talk
- OTT Voice (in case end-to-end encryption with IMS Voice does not work)
- OTT Video
- Firewall-as-a-Service
- Gunshot Detection System (GDS)
- Drone Control and Drone Video Streaming

The plan is to use the G-VNFM to orchestrate the third party applications for the Military. Initial integration is done by installing the applications in VMs on OpenStack/VIM directly. Container based applications setup containers and Kubernetes if needed in the VMs.

4.3.4.1 HERMOD service

HERMOD is a service used by the Military to allow certain clients to connect to the network, discover other UEs and enable direct communication with them. The Ericsson PGW can be configured to allow UE-to-UE communication between certain IP address ranges within the same APN. This is accomplished by defining a UE-to-UE unblocked range, under which one or more IP address ranges are configured. Communication is only allowed between UE devices using IP addresses from the configured IP address ranges in a single UE-to-UE unblocked range. It is possible for the same IP address range to be configured in more than one UE-to-UE unblocked range.

Assumptions considered for HERMOD service:

1. IMSI range dedicated to HERMOD UEs will be provisioned with HERMOD APN (i.e hermod.5gvinni.no) in UDR (User Database)
2. DNS1 and DNS2 are virtualized DNS applications dedicated only to HERMOD project
3. DNS1 and DNS2 IPs will be restricted only to HERMOD APN and configured on PGW
4. HERMOD client (~ Android app) needs to be installed on UE, client needs to know HERMOD AF FQDN
5. HERMOD AF FQDN + HERMOD AF IPs needs to be configured in both DNS

6. UE to UE communication needs to be allowed on PGW

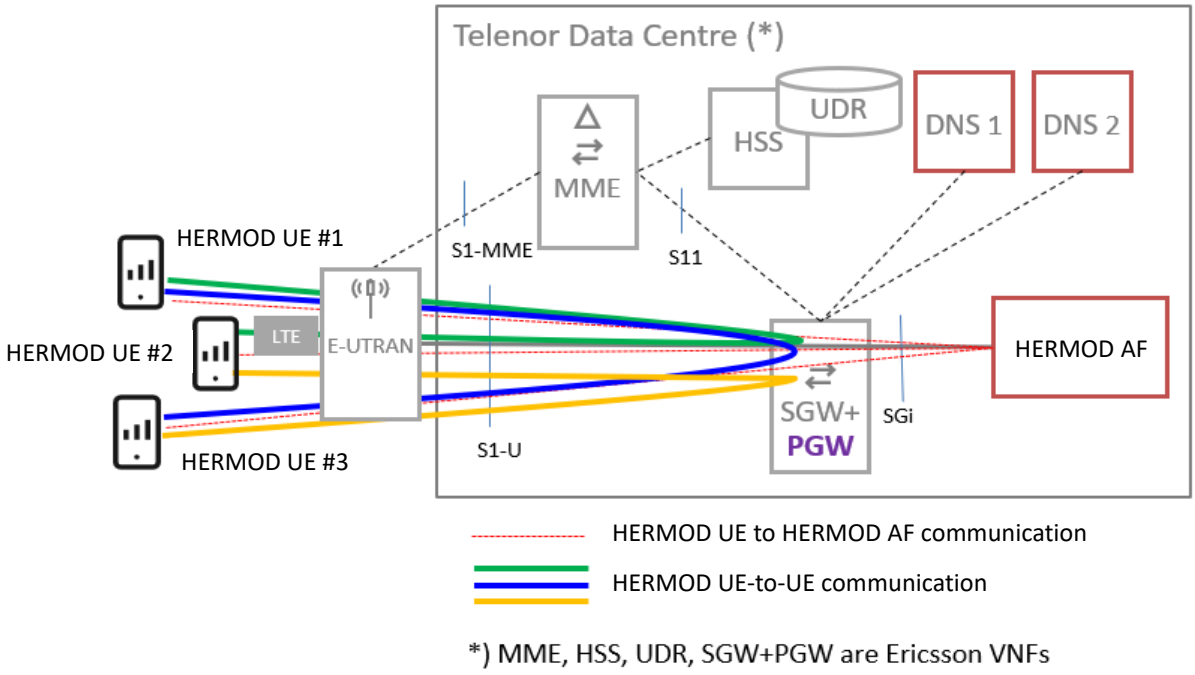


Figure 4.8 : HERMOD service

Figure 4.8 shows following service activation steps:

1. Switch HERMOD UE On
2. HERMOD UE initiate LTE session setup
    a. Default LTE bearer is created based on APN preconfigured in UE
    b. IPv4 and/or IPv4v6 addresses provided by PGW to UE during session setup
        i. UE IP address (IP range is preconfigured on PGW)
        ii. DNS IP1, DNS IP2 (preconfigured on PGW)
3. HERMOD client shall send DNS Query (Server-Name: HERMOD AF FQDN)
4. DNS response (with HERMOD AF IPv4 address list)
5. HERMOD client registers in HERMOD AF
6. HERMOD client retrieves list of all HERMOD clients (IP + ID) from HERMOD AF

HERMOD UE/clients can reach each other directly without contacting HERMOD AF (UE-to-UE communication)

Hermod VNF design

Hermod VNF will consist of a Hermod application function VM (HERMOD AF) and two redundant DNS VMs per site.

The VMs function is as follows:

- The HERMOD AF VM will contain the base OS and SW for the Hermod application.
- The DNS VMs will consist of base OS with DNS service configured. The entries in DNS will point to the local HERMOD VM with higher priority and other site with lower priority. Both DNS will be available and will be working as active-active loadshare.

Figure 4.9 show the proposed VNF architecture and interfaces.

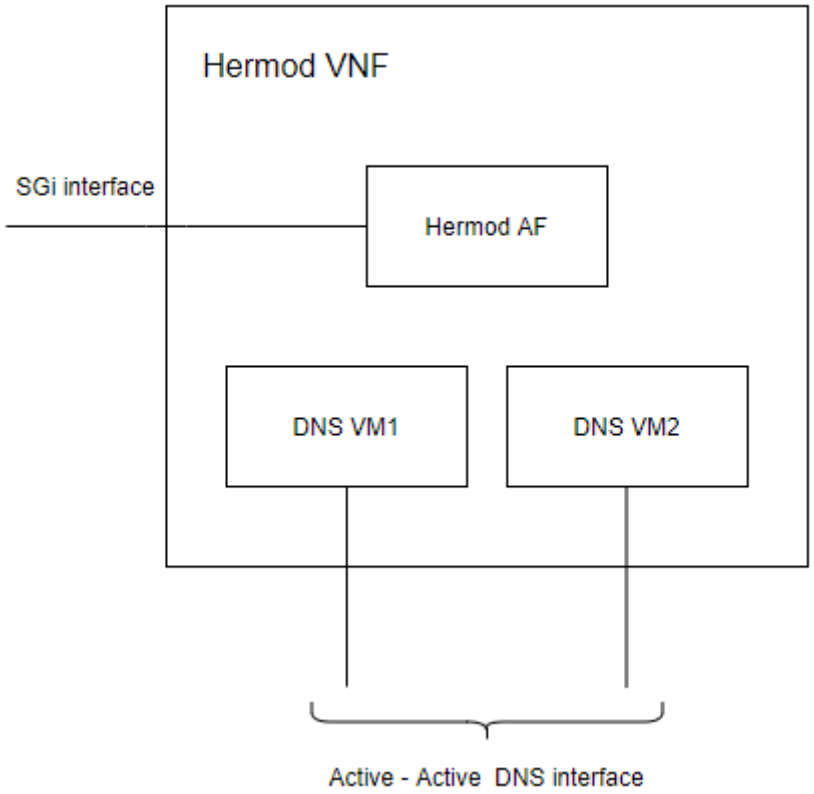


Figure 4.9 : HERMOD VNF

4.3.4.2 OTT Push-To-Talk (PTT)

The Over-The-Top (OTT) Push-To-Talk (PTT) application called Tactical Voice Service (TVS) provided by Thales is implemented in a VM in OpenStack. A dedicated OpenStack tenant is created for the TVS VM. The TVS is initially implemented in the Central site and will later be implemented in the Autonomous Edge site to become autonomous. The PTT service has not yet got specific QCI calls, but this is planned for later.

It has been successfully tested that the TVS clients register in the TVS server (Figure 4.10) and are able to communicate with each other using PTT.

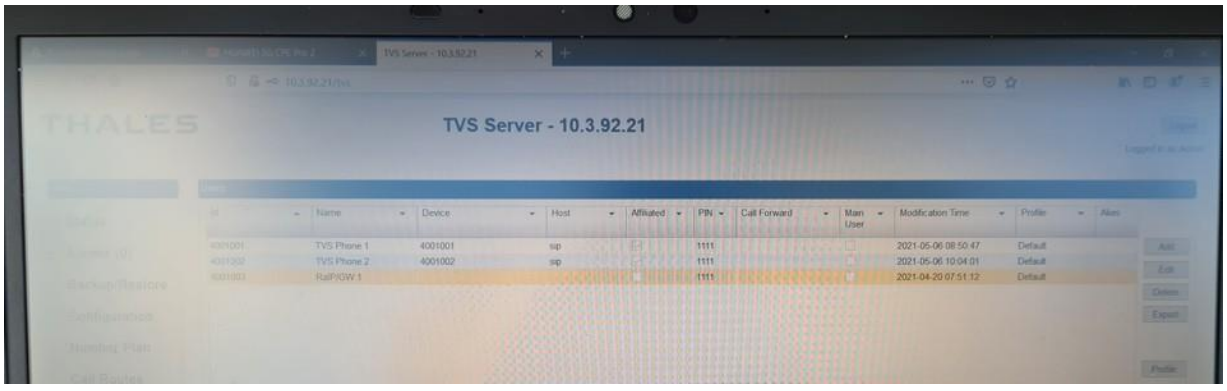


Figure 4.10 : Tactical Voice System (TVS) server view with registered devices.

4.3.4.3 OTT Voice

The OTT Voice service will be implemented in case SRTP is not supported for VoLTE/VoNR. The reason for considering this is that SRTP is not much used in commercial networks and there are few UEs that support SRTP at the time of writing.

4.3.4.4 OTT Video

The OTT Video service is in the planning. End-to-end encryption is important for the video service.

4.3.4.5 Firewall-as-a-Service (FWaaS)

To assure proper traffic isolation for the Military Slice a separate Palo Alto Networks Next Generation firewall will be implemented on the Gi/N6 interface. All mobile users from the Military Slice will connect to internet via that firewall. Figure 4.11 represents different network slices and FW-6 is dedicated FW for the Defence Slice.

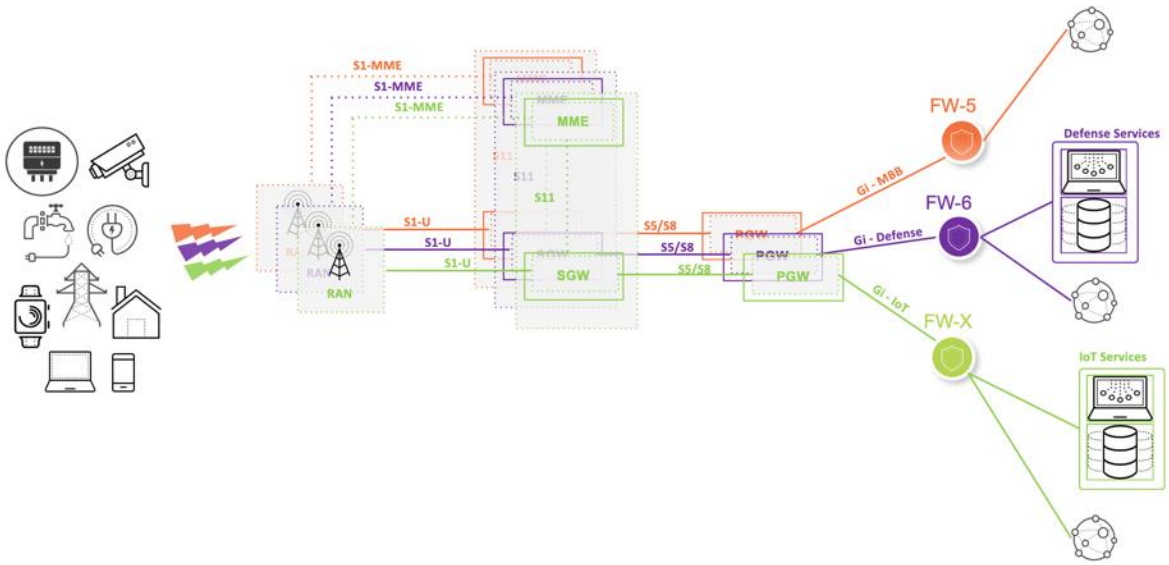


Figure 4.11 : Firewall for Military Slice

FW-6 have several functions:

- Provide CGNAT function for mobile devices connecting to internet
- Protect PGW and mobile users from external attacks
- Provide Next Generation Firewall functions for mobile users such as Applications whitelisting, IPS, Antivirus, Command and Control prevention, DNS Security, Antispyware, URL Filtering, Sandboxing, etc.

The Military organization will have the possibility to control security policies, allowed applications and respective firewall functions configuration of FW-6 according to their own security and compliance rules and regulations. It is also possible to feed own Indicators of compromise (lists of malicious IPs, Domains, URLs) via External Dynamic Lists to assure best possible security of mobile users. Military users will be able to connect to the system via Remote VPN connection and have access granted for configuring agreed set of functions on FW-6.

Hence, we can call this setup: Firewall-as-a-Service (FWaaS).

4.3.4.1 Gunshot Detection System (GDS)

GDS is implemented in a VM on OpenStack / VIM in the Central site. GDS is container based and runs on Kubernetes running in the VM. VM has two interfaces, one for management and one for data traffic. GDS will later also be onboarded into the Autonomous Edge.

A set of normal mobile handsets acting as GDS clients registers with the GDS server. GDS clients use DNS for service discovery of the GDS server (the same DNS servers as for the HERMOD described in section 4.3.4.1). The GDS clients detect audio and analyse the audio using machine learning to determine if it is a gunshot. The GDS clients report gunshots and other relevant data to the GDS server that is then able to estimate the location of the gunshot and what type of gun is used. The high level GDS system implementation using 5G is illustrated in Figure 4.12.

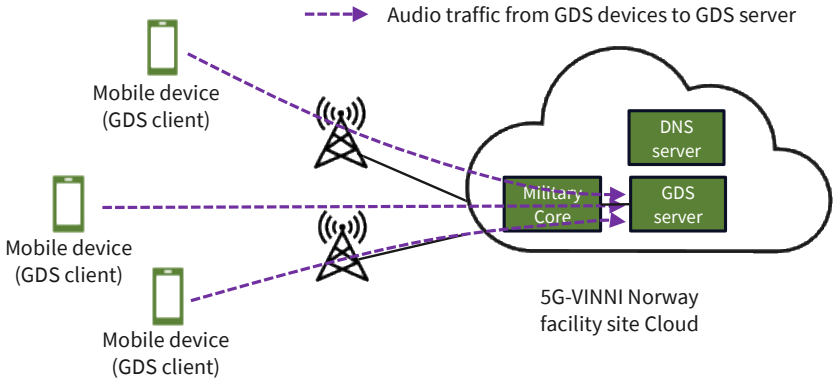


Figure 4.12 : GDS implementation in 5G-VINNI

It can be seen how a set of mobile devices acting as GDS clients are located on the map in Figure 4.13 and that these detect gunshot and estimate its location in Figure 4.14.

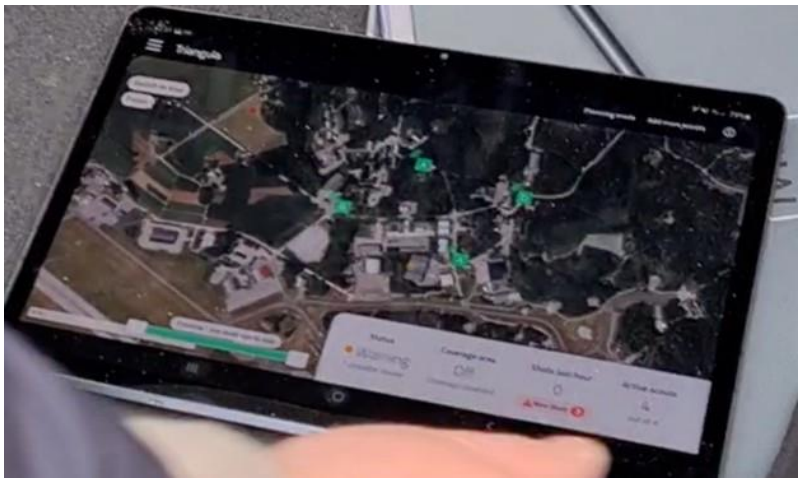


Figure 4.13 : Mobile Devices detecting audio of gunshots and reporting to GDS server

Figure 4.14 : GDS system detecting gunshots in a location

4.3.4.2 Drone Control and Drone Video Streaming

The drone control and drone video streaming architecture is illustrated in Figure 4.15.

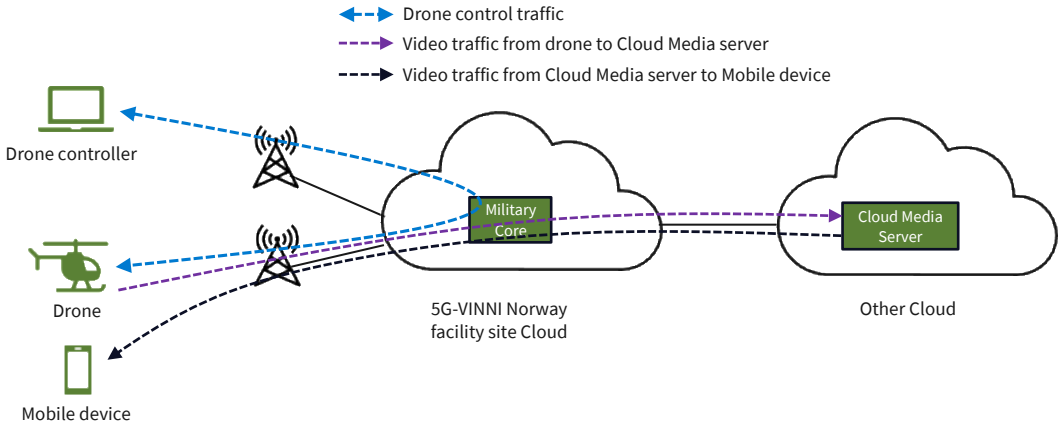


Figure 4.15 : Drone Control and Drone Video streaming in the 5G-VINNI Norway facility site.

Drone control is realised by connecting a drone controller to 5G that controls the drone also connected to 5G. To realize this communication UE-to-UE communication was enabled for the specific devices (drone controller, drone) in the Defence slice.

Drone video streaming is realized by streaming video from the drone over the 5G network to a Cloud Media Server running in a Cloud nearby. The cloud Media Server uses WebRTC and stream video to devices connected to 5G or any other network in any administrative domain (e.g. 4G, WiFi).

The drone used during testing is pictured in Figure 4.16 and the video streamed from the drone to the Cloud Media Server and back to the Mobile device is pictured in Figure 4.17.

Figure 4.16 : Picture of Drone being controlled.

Figure 4.17 : Video streamed from Drone under test to Cloud Media Server and to Mobile Device.

4.4 Services and Slices for ICT-19 project 5G-HEART

The ICT-19 project 5G-HEART will use the 5G-VINNI Norway facility site to implemented use cases for aquaculture (fish farming) and eHealth. The service design is ongoing and the implementation will be reported in an updated version of this report. High level use case description and initial design considerations are given below.

4.4.1 Fish Farming service

The End-to-End architecture of the solution for the use case of fish farming video analytics with Edge Cloud on premise is illustrated in Figure 4.18. The cameras in the fish farming cages record video of the fishes, which then are transmitted to Analytics Applications for analytics purposes. Extreme bandwidth requirements are put on the link between the cameras transmitting multiple video streams of high resolution towards the Fish Analytics application. Very often this link has to be wireless, where 5G providing high capacity is a good solution. However, in order to support the optimal video resolution for optimal analytics results, the wireless interface might require mmWave with extreme bandwidths up to GHz.

In order to avoid the challenge of extreme capacity on the wireless interface the analytics applications might be deployed locally in an Edge Cloud at the fish farm as illustrated Figure 4.1. After analytics processing in the Edge Cloud, the results will be available locally at the fish farm so that immediate action can be taken with minimal latency. Furthermore, only the analytics results have to be transmitted to a central location such as for processing in a Business Intelligence tool.

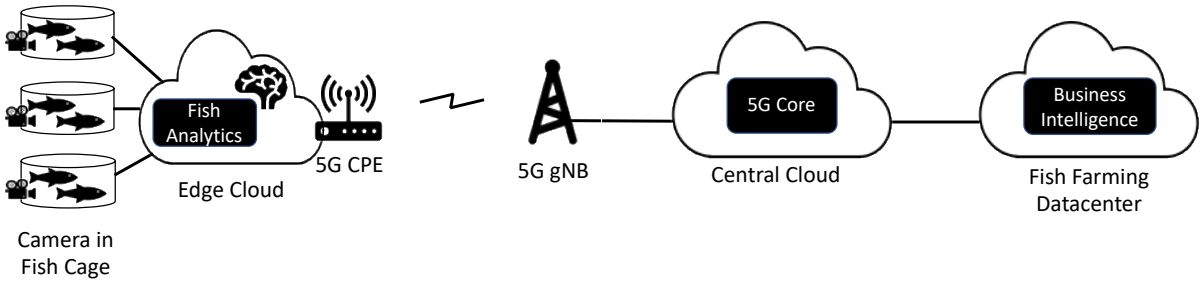


Figure 4.18 : End-to-End Solution for Fish Farming with Edge Cloud on premise

This use case is served by eMBB NSA slices presented in Section 4.2.

Both 3.6GHz and 26GHz gNBs are deployed at the fish farming site and there will also be tests to transmit all the video feeds over the radio interface.

There will be just one common availability zone for the analytics. There will be two types of VMs, one using GPU and one without.

For video analysis there is a request for GPU cards. Tesla T4 GPU has been used in 2 out of 5 servers where the VMs requiring GPU will be deployed. Openstack can deploy the VM in the specific server by using the correct flavour (property pci_passthrough:allias is set to T4_Tesla:1).

The detailed design of the Edge Cloud implementation for Fish Farming is described in Section 3.8.

4.4.2 eHealth services

Three eHealth services are planned for implementation;

- Pillcam, which is a capsule with a camera that detects colon cancer.
- Vital sign patches that enable continuous monitoring of ambulatory patients, anytime and anywhere
- Remote Ultrasound

The implementation of the *remote ultrasound use case* in the context of network slicing will be done in several phases. The first phase is just for initial testing and to prove basic operability as it is illustrated in Figure 4.19 below. For this, all devices in the patient-side are connected to a common local switch, which uses the 5G-CPE router as gateway for the connection to the 5G antenna. From the antenna, the packets go to the core via the transport network. The core in this phase is the NSA1 eMMB slice. The packets are processed in the core, the users data-plane are routed from the core S/PGW to the remote-expert side. The remote expert side has a similar setting. All the devices are connected to a common local switch that uses the 5G-CPE router as gateway. A specific APN is configured for the remote ultrasound and direct UE-to-UE communication is enabled for a joystick that controls the robotic ultrasound arm as well as for transmitting the video and ultrasound image between the UEs. In summary, Figure 4.19 presents the communication from/to patient-side to/from expert-side using eMBB.

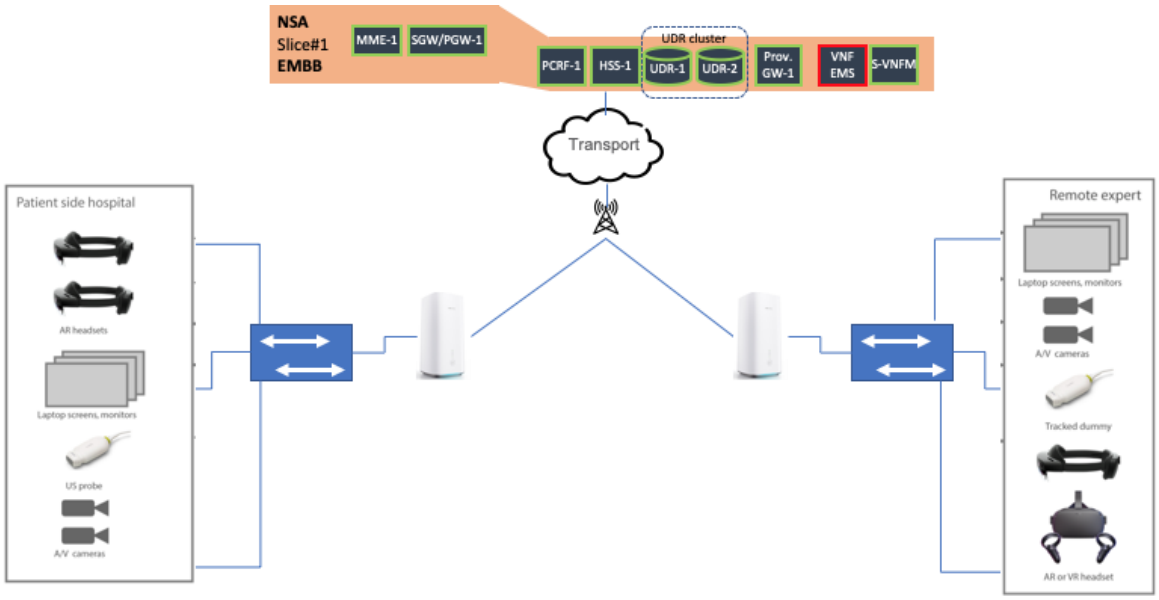


Figure 4.19 : Remote Ultrasound connectivity test diagram

The improvement of the connectivity for the remote ultrasound use case will be developed in Phase 2 and 3. After testing basic operability in Phase 1, Phase 2 and 3 will focus on tuning the network setting in order to fulfil the requirements of this use case. For this, there are two main differences in comparison to Phase 1.

The first one is the finer tuning of the QoS Class Identifier (QCI) in the RAN part, which will allow to set the RAN according to the corresponding requirements. Those values are presented in the 3GPP TS 23.501 specification, table 5.7.4-1.

The second one includes the use of EDGE in order to have the shortest delay possible. This setting enable the user data packets to be treated locally without need to travel to central site. This is enabled at the same time by the NSA Slice 3 used in Phase 2, since its S/PGW setting is split in the control and user plane part as illustrated in Figure 4.20.

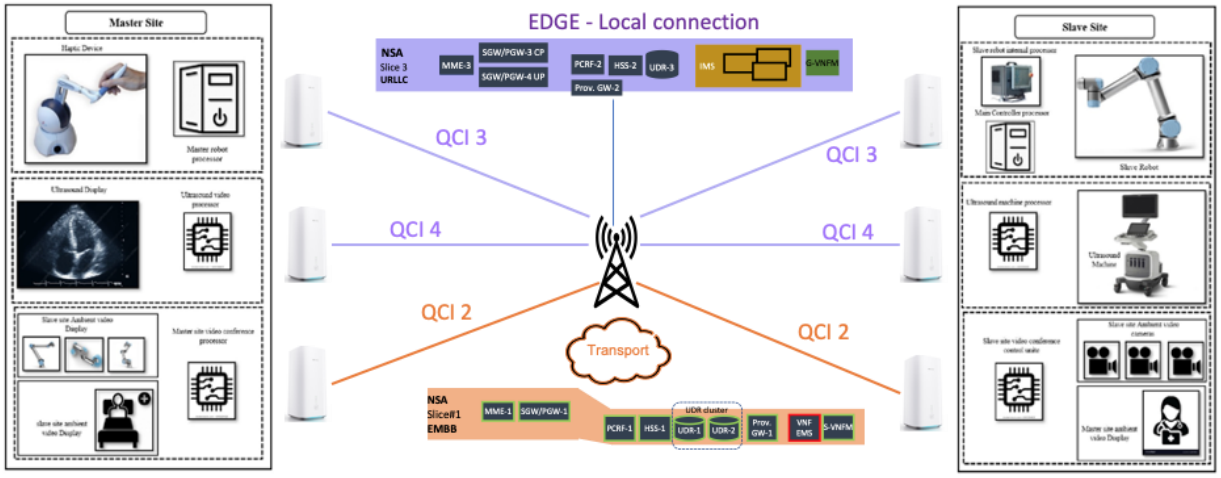


Figure 4.20 : Remote Ultrasound Phase 2 and Phase 3

4.5 Services and Slices for ICT-19 project 5G-SOLUTIONS

The ICT-19 project 5G-SOLUTIONS will use the 5G-VINNI Norway facility site to implemented use cases for smart port, smart city and factory of the future. The implementation and testing is ongoing for the Smart Port and Factory of the Future use cases.

The smart port use case is implemented at Herøya industrial park with Yara. Two Ericsson BBUs are installed each serving two sectors all using the 3.6GHz band. This use case is using the 5G SA eMBB slice. Hence, no LTE anchor band is needed.

The factory of the future use cases is implemented at Gøshaugen (Trondheim) with NTNU. Five 5G indoor radio nodes (Ericsson DOTs) are deployed in the factory building, where two of them are using the 3.6GHz band and three of them are using the 3.4GHz band. The 5G SA eMBB slices will be used.

5G-SOLUTIONS project has onboarded their own BSS tool called CDSO in the central site. The CDSO communicates with OpenSlice and if needed the E2E Orchestrator (FlowOne).

5G-SOLUTIONS uses the TaaS service to do measurements. A visibility tool managed by 5G-SOLUTIONS collects measurement from TaaS and potentially later monitoring data.

4.6 Services and Slices for a Hospital

A 5G network was implemented for a hospital that requested a shared 5G radio system for:

- a private 5G service for employees and medical devices. The private 5G service is only available for employees and medical devices inside the hospital premises.
- a public 5G service for patients and visitors in the hospital. The public 5G services is available both in the hospital premises and outside the hospital premises for any users including employees.

The network architecture and traffic flow are illustrated in Figure 4.21.

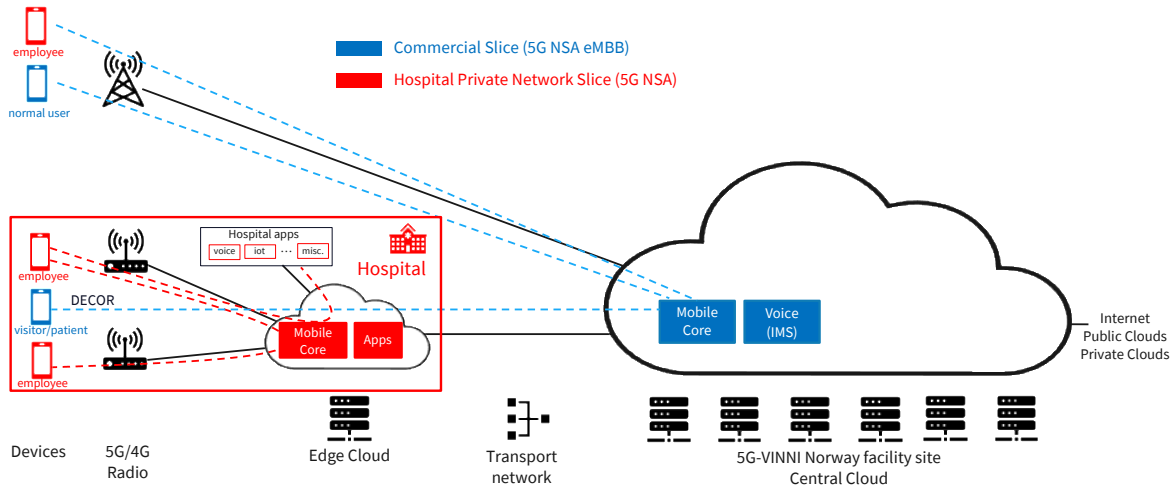


Figure 4.21 : Hospital 5G network with private and public 5G service

The 5G radio access network was implemented using indoor radio system from Ericsson with 5G (3.6GHz) and also 4G (2.1GHz) to provide NSA 5G. The radio access network was managed by 5G-VINNI Norway facility site. Two pair of radio nodes (5G and 4G) were installed for testing:

- One pair of 5G and 4G indoor radio nodes was installed inside the hospital
- One pair of 5G and 4G indoor radios was installed to emulate the outdoor public radio network.

The public 5G service was delivered using the eMBB NSA slice in 5G-VINNI Norway facility site to which all radio access network nodes connected. Site-to-site VPN is setup between the PaloAlto firewall in the Edge to the PaloAlto firewall in the central site to enable access to the central core.

The private 5G service was delivered using another 5G NSA core installed in an Edge cloud in the hospital premises to which only the indoor radio access nodes in the hospital connected.

DECOR was used as the mechanism for sharing the radio nodes between private and public networks. Employee subscribers were provisioned in both the private network HSS and the public network HSS, while the other subscribers (e.g. patients, visitors) were provisioned in the public HSS only.

Ericsson Indoor radio nodes (DOTs) that were installed can be seen in Figure 4.22, where the one to the left is 5G and the one to the right is 4G. The central site and core network used for the public network service is the same as described in Section 3 and the eMBB NSA slice described in Section 4.2. The rack with equipment installed in the hospital premises is depicted in Figure 4.23, where from top can be seen the rectifier for the BBUs, Ericsson BBUs, Ericsson Indoor Radio Units (IRUs), a Cisco switch, PaloAlto firewall and a Microsoft Azure Stack Edge (ASE).

Figure 4.22 : Ericsson Indoor radio DOTs, 5G (right) and 4G (left).

Figure 4.23 : Rack and equipment installed in the hospital premises.

5 Dimensioning and Bill of Material (BOM)

5.1 User Equipment

The following UEs was available for testing initially:

- 4 x WNC pocket router for Ericsson with specification based on Qualcomm X50.
- 5 x Huawei 5G CPE.

5.2 Transport Network

5.2.1 Provider Edge (PE)

The commercial transport network in Telenor Norway will be used. An existing PE router will be used to connect to the WBX switches in the datacenter acting as the datacenter gateway.

Two new Juniper MX480 mpc7 cards are installed in the PE (100G capacity).

Two new fibres will be installed between the PE and WBX (100G capacity).

5.2.2 RAN sites

For each RAN site we will install a new Cell Siter Router (CSR).

- Ericsson R6675 will be used on RAN sites where Ericsson gNBs is deployed.
- Huawei ATN910-F will be used on RAN sites where Huawei gNB is deployed.

5.3 MANO and NFVI

5.3.1 Core site

Totally there are 21 Servers that will be used as below:

- 6 Compute Nodes
- 3 Compute nodes and Controllers
- 9 Compute and storage nodes
- 3 servers for Nuage components (not part of the cloud)

The maximum number of available vCPUs are approximately 1250, but in the reality, it will be less. This depends on different factors such as anti-affinity rules, single NUMA resource allocation requirements, VNF onboarding order and so on.

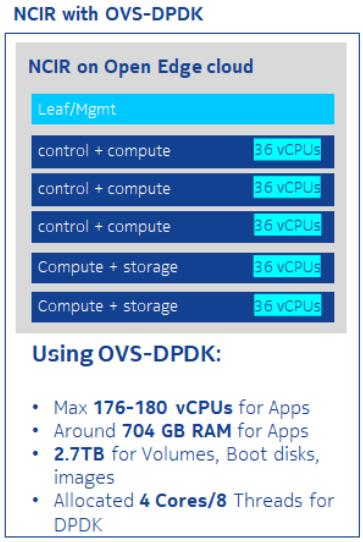
The BOM for NFVI is given in Table 5.1 (note that additional three servers are deployed for Release 1, which numbers are not included in the table reflecting the initial deployment).

Table 5.1 : BoM for Central NFVI

Import	Import	Import	Import
Product ID	Product Description	Customer Material Number	Qty
	AirFrame	CONFIGURATION	
NDCHW0020	AT_70790445485_OR_RC1	CONFIGURATION	1
NDCHWA2037	AF OR rack frame 42OU White		1
NDCHWA2205	AF OR Transportation Crate 42OU rack		1
NDCHWA2017	AF 12kW power shelf for AO-RACK42U-B		2
NDCHWA2206	AF OR Compute rack Integration work		1
NDCHWA1149	AF RJ45 Cat5e variable length		52
NDCHWA2019	AF PDU3-phase 12.5kW International		2
NDCHWA2022	AF 2.5kW PSU for AO-PS12KW-B power shelf		12
NDCHWA1148	AF 25GbE Break DAC variable length		48
NDCHWA1261	AF OR switch 5404BT 48x 10GBase-T		1
NDCHWA2051	AF power cable C13-C14 3m AC		6
NDCHWA2025	AF Rack Management Control for PS12KW-B		2
NDCHWA2043	AF Cable Manager 1U with air block		1
NDCHWA2118	AF OR v2 three bay shelf 2U EMI shield		7
NDCHWA2115	AF OR Server L6 Barebone 2U Single		21
NDCHWA1520	AF 6138 Intel processor 20c 2.0GHz 125W		42
NDCHWA1069	AF RDIMM DDR4 32GB 2666		252
NDCHWA1053	AF OCP Mezz 25Gb dual port		21
NDCHWA1054	AF PCIe card 25Gb dual port		21
NDCHWA1346	AF SSD 3.84TB SATA 1dwpd 2.5 inch		18
NDCHWA1395	AF M.2 2280 480GB SATA 1dwpd		21
NDCHWA1165	AF QSFP to SFP+ Adapter		4
NDCHWA1021	AF SFP Transceiver 1000Base-T RJ45		4
NDCHWA2042	AF OR Blank panel 2 OU		9
NDCHWA1351	AF Disk SSD480G 3dwpd 2.5 inch		12
NDCHWA2039	AF OR rack door set for RACK42U-W		2
NDCHWA2038	AF OR rack side panel set for RACK42U-W		1
NDCSSW0000	AirFrame NDCS eSW e-media	CONFIGURATION	1
ORSW18101	OR18 Server eSW e-media		1
ORSW18201	OR18 Switch eSW e-media		1
ORSW18301	OR18 RMC eSW e-media		1
NADCMSW018	AirFrame Data Center Manager 18 NOLS		1
NADCMSW0001	AF Data Center Manager TL SRS		24
NADCMSW0003	AF Data Center Manager TL CLTU		24
NCIRSW0000	AirFrame NCIR SW e-media	CONFIGURATION	1
NCIRSW0018	NCIR 18 SW E-Media		1
NCIRSWVIM0101	Nokia NCIR SW VIM Implementation TL SRS		21
NADCM0LK	AirFrame NADCM SW LK	CONFIGURATION	1
NADCMSW0004LK	AF Data Center Manager CLK		24

5.3.2 Edge site

Below is the maximum capacity that the NFVI can handle together with VNFs requirements. The NFVI Edge setup has been built just to accommodate the current needs for Metaswitch IMS and Ericsson 5G Core. If there is requirement for more resources in the future then expansion will be needed (more servers and a new chassis).



	vCPUs	Memory (GB)	Storage(Volumes, Boot disks, Images)
Ericsson	120	552	1524 GB
Metaswitch	24	66	925 GB
Total	144	618	2.39TB

Storage Solution:

- CEPH as software defined storage
- Replication factor of 2
- Net storage is approximately 2.7 TB
- This is for Cinder volumes, Boot disks and Images
- Images should be stored in raw format due to CEPH limitation

*Resilience and anti-affinity rules haven't been considered yet, but there are extra resources for this

Figure 5.1 : Cloud infrastructure dimensioning

5.4 5G RAN and Core

Table 5.2 provides the summary for Ericsson 5G EPC resource requirements.

Table 5.2 : 5G EPC resource requirements

Ericsson 5G EPC with CUPS dimensioning					
VNF	#	Number of VMs	Number of vCPU	Memory [GB]	Disk [GB]
MME	3	18	84	900	972
SGW-PGW	3	24	144	624	2.880
SGW-PGW UP	1	4	16	88	160
HSS-FE	2	8	16	96	800
PCRF-FE (SAPC-FE)	2	8	16	64	160
UDR (CUDB)	4	24	48	144	1.280
Provisioning (EDA)	1	3	24	90	495
5G EPC Total		**89**	**348**	**2.006**	**6.747**
Nokia compute node capacity			**80**	**384**	x
Nokia storage node capacity			x	x	**3840**
Number of nodes			5	6	2
Compute nodes for 5G EPC				6	
Storage nodes for 5G EPC				2	

5.4.1 eNB

Table 5.3 provides the summary for Ericsson LTE nodes resource requirements for 2 sites.

Table 5.3 : Ericsson LTE nodes resource requirements

Node type	Total number of nodes	Total number of sectors	Baseband type	Total number of Basebands	Radio Type	Total number of Radios
eNodeB	2	6	BB 6630	2	Radio 4415	6

Table 5.4 provides the summary for Huawei LTE nodes resource requirements for 2 sites.

Table 5.4 : Huawei LTE nodes resource requirements

Node type	Total number of nodes	Total number of sectors	Baseband type	Total number of Basebands	Radio Type	Total number of Radios
eNodeB	2	4	BBU5900	2	RRU5904	4

5.4.2 gNB

Table 5.5 provides the summary for Ericsson 5G nodes resource requirements for 2 sites.

Table 5.5 : Ericsson 5G nodes resource requirements

Node type	Total number of nodes	Total number of sectors	Baseband type	Total number of Basebands	Radio Type	Total number of Radios
gNodeB	2	6	BB 6630	2	AIR 6488	6

Table 5.6 provides the summary for Huawei 5G nodes resource requirements for 2 sites.

Table 5.6 : Huawei 5G nodes resource requirements

Node type	Total number of nodes	Total number of sectors	Baseband type	Total number of Basebands	Radio Type	Total number of Radios
gNodeB	2	4	BBU5900	2	AAU5613/AAU5213	8

5.4.3 MME

Table 5.7 : MME Resource requirements

VNF Name	VM Type	VMs per type	vCPU per VM	RAM [GB] per VM	Storage [GB] per VM
vSGSN-MME	FSB	2	4	10	160
	NCB	2	4	10	1
	GPB w vLC	2	6	40	1

Table 5.8 : MME Anti-affinity rules

VM	VM	VM	Availability zone
FSB-1	NCB-1	GPB-1	1
FSB-2	NCB-2	GPB-2	2

5.4.4 SGW/PGW

Table 5.9 : SGW/PGW Resource requirements

VNF Name	VM Type	VMs per type	vCPU per VM	RAM [GB] per VM	Storage (GB) per VM
vSGW-PGW (CP+UP)	vRP	2	2	4	80
	vSFO CP	4	8	30	160
	vSFO UP	2	6	40	80
vSGW-PGW Control Plane	vRP	2	2	4	80
	vSFO CP	4	8	30	160
	vSFO UP	2	6	40	80
vSGW-PGW User Plane	vRP	2	2	4	40
	vSFO UP	2	6	40	40

Table 5.10 : PGW/SGW Anti-affinity rules

VNF	VM	VM	VM	VM	Availability zone
vSGW-PGW (CP+UP)	vRP-1	vSFO UP-1	vSFO CP-1	vSFO CP-2	1
	vRP-2	vSFO UP-2	vSFO CP-3	vSFO CP-4	2
vSGW-PGW Control Plane	vRP-1	vSFO UP-1	vSFO CP-1	vSFO CP-2	1
	vRP-2	vSFO UP-2	vSFO CP-3	vSFO CP-4	2
vSGW-PGW User Plane	vRP-1	vSFO UP-1	1		
	vRP-2	vSFO UP-2	2		

5.4.5 PCRF

Table 5.11 : PCRF Resource requirements

VNF Name	VM Type	VMs per type	vCPU per VM	RAM [GB] per VM	Storage [GB] per VM
PCRF-FE	SC	2	2	6	40
	TP	2	2	10	40

Note 1: Only frontend part of PCRF will deployed, subscriber database (SRP) will be part of UDR VNF.

Note 2: Optional VM VR will not be deployed.

Note 3: Ericsson product name for PCRF is SAPC

Table 5.12 : PCRF Anti-affinity rules

VM	VM	Availability zone
SC-1	TP-1	1
SC-2	TP-2	2

5.4.6 HSS and & Subscriber Database

HSS Frontend

Table 5.13 : HSS Resource requirements

VNF Name	VM Type	VMs per type	vCPU per VM	RAM [GB] per VM	Storage [GB] per VM
HSS-FE	SC	2	2	12	200
	PL	2	2	12	0

Table 5.14 : HSS Anti-affinity rules

VM	VM	Availability zone
SC-1	PL-1	1
SC-2	PL-2	2

5.4.7 Subscriber Database (CUDB)

Table 5.15 : Subscriber Database (CUDB) Resource requirements

VNF Name	VM Type	VMs per type	vCPU per VM	RAM [GB] per VM	Storage [GB] per VM
Subscriber Database	SC	4	2	6	40
	PL	2	2	6	80

Table 5.16 : Subscriber Database (CUDB) Anti-affinity rules

VM	VM	VM	Availability zone
PL-1	PL-3	SC-1	1
PL-4	PL-6	SC-2	2

5.4.8 Provisioning System

Table 5.17 : Provisioning system Resource requirements

VNF Name	VM Type	VMs per type	vCPU per VM	RAM [GB] per VM	Storage [GB] per VM	Ephemeral storage [GB]
Provisioning	VN	3	8	30	165	1

Table 5.18 : Provisioning system Anti-affinity rules

VM	Availability zone
Node-1	1
Node-2	2
Node-3	3

5.4.9 EMS

Table 5.19 : EMS Resource requirements

VNF Name	VMs types	VMs per site	Total vCPU	Total RAM [GB]	Total eph Storage [GB]	Total [GB] persistent volumes
vENM	95	167	405	992	2020	794

Anti-affinity rules will not be applied in order to save NFVI HW resources.

5.4.10 5G SA Core (5GC)

Table 5.20 : 5GC Resource requirements

Type	Number of VMs	CPUs	RAM (GB)	Local/Ephemeral storage (GB)	Cinder storage (GB)
CaaS Director VM	2	2	4	0	210
CaaS Master VM	2	2	4	0	30
CaaS Worker VM	8	24	48	0	100
Simulator VM	1	4	10	40	0
CNFs	N/A	N/A	N/A	N/A	At least 720
Total	**13**	**204**	**410**	**40**	**At least 2000**

Note: The resources need to be spread over at least 4 compute nodes to facilitate anti-affinity. It is planned that 4 compute nodes will be dedicated for deployment of the 5G SA core, to allow appropriate scheduling of the relatively large Worker VMs.

5.5 IMS Dimensioning

5.5.1 IMS in Central site (with Active Edge scenario)

Table 5.21 : IMS dimensioning for Central site (with Active Edge scenario)

VM	Spec	Topology	VMs	HT-vCPUs	RAM (MB)	Boot Storage (GB)	Volume storage (GB)
DCM	Prod	1+1 pool	2	1	1024	20	0
MVS	Lab	1 instance	1	1	8192	35	265
SAS	Lab	1 instance	1	1	4096	60	0
SIMON	Lab	1 instance	1	4	8192	20	100
MDM	Lab	2+1 pool	3	1	4096	40	0

VM	Spec	Topology	VMs	HT-vCPUs	RAM (MB)	Boot Storage (GB)	Volume storage (GB)
CFS	Lab	1 HA pair	2	1	4096	30	170
MRS	Lab	1+1 pool	2	1	4096	100	0
MVD	Lab	1 HA pair	2	1	8192	30	70
EAS	Lab	1 instance	1	1	4096	70	230
AMS	Lab	1+1 pool	2	1	4096	100	0
Clearwater DGN	Lab	2 instances	2	1	2048	20	0
Clearwater SPN	Lab	2 instances	2	1	2048	20	0
Clearwater SCN	Lab	2+1 pool	3	1	4096	20	0
Rhino MMT	Small	2+1 pool	3	4	16384	30	0
Rhino MAG	Small	2+1 pool	3	4	16384	30	0
Rhino ShCM	Single	1+1 pool	1	4	8192	30	0
Radisys MRF	Medium	1 instance	1	10	8192	40	0
Total			**32**	**65**	**215040**	**1255**	**1075**

5.5.2 IMS in Central site (with Inactive Edge scenario)

Table 5.22 : IMS dimensioning for Central site (with Inactive Edge scenario)

VM	Spec	Topology	VMs	HT-vCPUs	RAM (MB)	Boot Storage (GB)	Volume storage (GB)
DCM	Prod	1+1 pool	2	1	1024	20	0
MVS	Lab	1 instance	1	1	8192	35	265
SAS	Lab	1 instance	1	1	4096	60	0
SIMON	Lab	1 instance	1	4	8192	20	100
MDM	Lab	2+1 pool	3	1	4096	40	0
CFS	Lab	1 HA pair	2	1	4096	30	170
MRS	Lab	1+1 pool	2	1	4096	100	0
MVD	Lab	1 HA pair	2	1	8192	30	70
EAS	Lab	1 instance	1	1	4096	70	230
AMS	Lab	1+1 pool	2	1	4096	100	0
Perimeta ISC	Medium	1 HA pair	2	8	16384	60	0
Clearwater DGN	Lab	2 instances	2	1	2048	20	0

VM	Spec	Topology	VMs	HT-vCPUs	RAM (MB)	Boot Storage (GB)	Volume storage (GB)
Clearwater SPN	Lab	2 instances	2	1	2048	20	0
Clearwater SCN	Lab	2+1 pool	3	1	4096	20	0
Rhino MMT	Small	2+1 pool	3	4	16384	30	0
Rhino MAG	Small	2+1 pool	3	4	16384	30	0
Rhino ShCM	Single	1+1 pool	1	4	8192	30	0
Radisys MRF	Medium	1 instance	1	10	8192	40	0
Total			**34**	**81**	**247808**	**1375**	**1075**

5.5.3 IMS in Edge

Table 5.23 : IMS dimensioning for Edge site

VM	Spec	Topology	VMs	HT-vCPUs	RAM (MB)	Boot Storage (GB)	Volume storage (GB)
DCM	Prod	1+1 pool	2	1	1024	20	0
SAS	Lab	1 instance	1	1	4096	60	0
MDM	Lab	2+1 pool	3	1	4096	40	0
Perimeta ISC	Medium	1 HA pair	2	8	16384	60	0
Clearwater DGN	Lab	2 instances	2	1	2048	20	0
Clearwater SPN	Lab	2 instances	2	1	2048	20	0
Clearwater SCN	Lab	2+1 pool	3	1	4096	20	0
Total			**15**	**29**	**71680**	**480**	**0**

5.6 Test Equipment

The resource requirements for the testing tools that will be instantiated on the NFVI in the Norway facility site are listed in Table 5.24. The testing tools will be described further in 5G-VINNI WP4 deliverable 4.1. The Norway facility site will host a set of testing tools that are centralized and used for all the main facility sites in 5G-VINNI, which can be identified in the “Location” row as Norway. In addition to the centralized tools across all facility sites there will be tools for testing and visibility that will be deployed locally in each main facility site, which can be identified in the “Location” column as local.

Table 5.24 : Testing tools and resource requirements on NFVI

Product	Category	# Units	Cores	RAM	Disk	Network	Other requirements	Location
CloudLens Manager	Visibility		2	8GB	4GB			Norway
CloudLens Cloud Sensor Management Platform	Visibility		4	4GB	10GB			Norway
vTap	Visibility	?	1-2	1GB	2-4GB		RAM for TaaS with KVM integrated with OVS	local
Fabric Controller	Visibility	?	2	2GB	10GB		Potentially one per slice. Verify if it supports virtual PBs	Norway
BreakingPoint Controller	Testing	1	10	16GB	150GB		CentOS 6.6	local
BreakingPoint vBlade	Testing	4	4	8GB	14GB	10G	CentOS 7	local
IxLoad vChassis	Testing	1	2	4GB	8GB			local
IxLoad Load Module	Testing	4	2	4GB	2GB	10G		local
Testing Web service	Testing	1	4	8GB	50GB			Norway
Hawkeye web service	Testing	1						Norway
Executor core/API	Testing	1	1-2	4GB	4GB			Norway
Executor spawn	Testing	1-2	2	4GB	4GB		Container	local
License servers		2	1	1GB	2GB			Norway
NEMO Xynergy	Analytics	1	10	32GB	1.1T		Disk space depending on use of third parties' BigData	Norway
Cloudera	Analytics	1	40-100					local

6 Cross-Facility-sites end-to-end design

The cross-facility site end-to-end design is described in D2.1 overall document.

There are at least two things to design, (i) the interconnection between facility sites and (ii) the orchestration of services cross facility sites. For (ii), this is described in the D2.1 overall document. For (i), the plan is to start using SD-WAN over regular internet and later move to dedicated lines.

The Norway facility site is interconnected with the UK facility site using site-to-site VPN over the Internet. Interworking has not yet been implemented.

7 API

7.1 Orchestration API

Figure 4.2 depicts an integration view of FlowOne APIs.

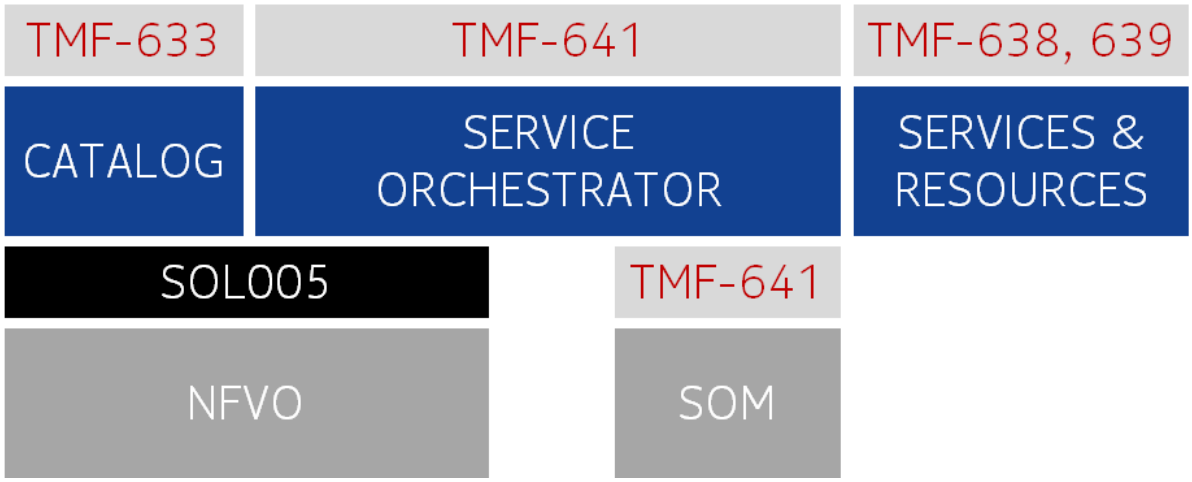


Figure 7.1 : Typical integration architecture of an E2E Orchestrator

In Figure 7.1, SOL005, TMF-633, TMF-641 and TMF-638 & TMF-639 boxes refer to interfaces. The module that appears below a given interface is the provider, while the module that appears above is the consumer of that particular interface. Both SOM (Service Order Management) and NFVO could be of another VINNI facility.

7.2 ENM API

The Ericsson Network Manager has a number of external interfaces / API available for external systems over the northbound interface. There is a number of different NBI/API available for Fault Management (FM), Configuration Management (CM), Performance Management (PM) and Security Management (SM).

The different NBI/API is listed below:

- ENM Fault Management Northbound Interface (FM NBI)
- ENM Bulk CM Interface (Import/Export NBI using 3GPP XML File Format over REST)
- ENM Configuration Management Events NBI
- ENM CM File Interface (Import/Export NBI using Ericsson Dynamic File Format over REST)
- ENM CM Bulk Import REST Northbound Interface
- ENM Configuration Management Task Northbound Interface (CM Task NBI)
- ENM Performance Management NBI
- ENM Uplink Spectrum File Collection NBI
- ENM Software, Hardware and License Inventory Export NBI
- ENM Identity and Access Management NBI
- ENM Single Sign-On NBI (SSO NBI)
- ENM External Identity Provider (LDAP) NBI
- VNF Lifecycle Manager (VNF-LCM) NBI
- ENM Scripting Support
- ENM Analytic Session Records Northbound Interface (ASR) NBI
- ENM Single Session Quota Constraint NBI

Detailed descriptions of each NBI/API are described in the ENM product description.

