NFVI Abstraction and Profiling

Version 2.0

25 March 2019

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

The main concept of NFV (Network Function Virtualization) is the ability to use general purpose compute hardware and platforms that run multiple VNFs (Virtualised Network Functions) and hence achieving the desired CapEx and OpEx savings. However, one of big challenges NFV is facing with VNF vendors is that vendors, while building or designing their virtualized services (whether it's VoLTE, EPC, or enterprise services like SD-WAN (Software Defined Wide Area Network)), must bring their own set of infrastructure requirements and custom design parameters. This attitude from vendors triggered the creation of various vendor/function specific silos which are incompatible with each other and have different operating models. In addition, this makes the onboarding and certification processes of VNFs (coming from different venrors) hard to automate and standardise.

Therefore, for a true cloud type deployment, a model, which relies on engagement with specific vendors and unique infrastructure, needs to be reversed in a way that there is a lot more consistency on infrastructure. Vendors need to bring their software to run into pre-defined environment with common capabilities. That common infrastructure, whether it is optimized for IT (Information Technology) workloads, NFV workloads, or even for AI (Artificial Intelligence) workloads, needs to be fully abstracted to VNFs so that it can be a standard offer.

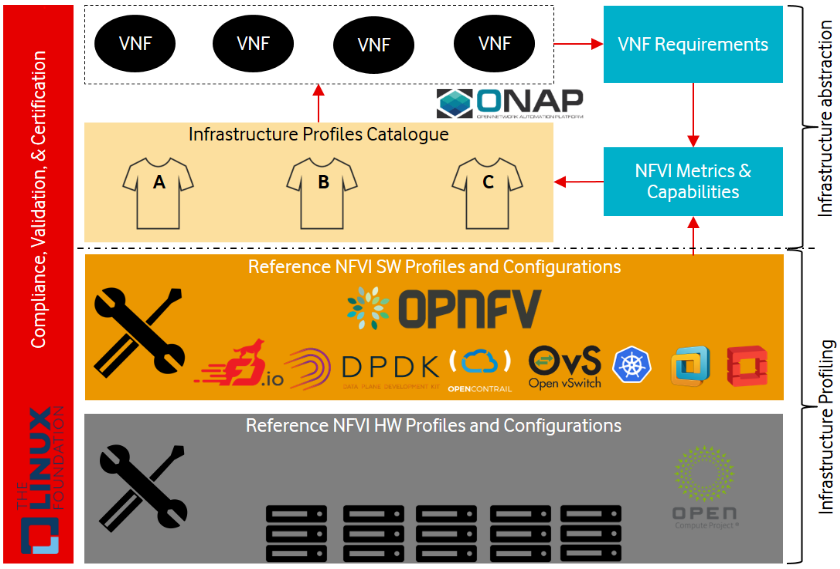
Additionally, to bring the most value to telco operators as well as vendors, agreeing on a standard set of infrastructure profiles for vendors to use for their VNFs is needed within the industry.

The benefits of this approach are:

- Configuration over customisation
    - By abstracting the infrastructure capabilities, operators are able to have common infrastructure platforms across all VNF vendors.
    - Maintaining a consistent infrastructure allows for higher levels of automation as there is less customisation.
    - Overall, this will reduce the total cost of ownership for operators
- Onboarding and certification
    - By defining abstracted infrastructure capabilities, and the metrics by which they are measured, the onboarding and certification process for both NFVI and VNFs can be standardised.
    - Supply chain, procurement and assurance teams can also then use these metrics to more accurately assess the most efficient / best value vendor for each scenario.
- Better utilization

- Mapping VNFs to flavors which are properly mapped to IaaS will bring better utilization, than current VNFs expressing variety of instance types as their needs on IaaS.

1.2 Scope


Compliance, Validation, & Certification
THE LINUX FOUNDATION
VNF
VNF
VNF
VNF
VNF Requirements
ONAP
Infrastructure Profiles Catalogue
A
B
C
NFVI Metrics & Capabilities
Infrastructure abstraction
Reference NFVI SW Profiles and Configurations
OPNFV
fd.io
DPDK
OPENCONTRAIL
OvS Open vSwitch
Reference NFVI HW Profiles and Configurations
OPEN Compute Project
Infrastructure Profiling

The scope of this document is illustrated in **Figure 1** below.

- **: Scope of work.**

This document specifies:

- NFVI Infrastructure abstraction
    - **NFVI metrics & capabilities:** A set of carrier grade metrics and capabilities of NFVI which VNFs require to perform telco grade network functions.
    - **Infrastructure profiles catalogue:** A catalogue of standard profiles needed in order to completely abstract the infrastructure from VNFs. With a limited and well defined profiles and well understood characteristics, VNF compatibility and performance predicatability can be achieved. The current focus is for VMs but the intention is to expand the definition to include Container profiles too.
- Reference software and hardware Infrastructure profiling
    - **Reference NFVI software profiles and configurations:** These reference software profiles and configurations should map efficiently to the infrastructure exposed profiles catalogue. The expectation is for Open Source communities (such as OPNFV) to maintain those reference profiles as the software technology evolves.
    - **Reference NFVI hardware profiles and configurations:** These reference hardware profiles and configurations should be suitable for the defined NFVI software profiles & configurations. The expectation is for Open Source communities (such as OPNFV) to maintain those reference profiles as the hardware technology evolves.

- Compliance and verification
  - **Certification programs:** Define the requirement for certification programs for both VNFs and NFVI.
  - **Test framework:** Provide test suites to allow compliance, certification, and verification of VNFs and NFVI against the defined set of profiles. Part of the framework is also developing a reference implementation of the defined profiles (with the defined configurations0 to be used as a reference for compliance, certification, and verification of NFVI and VNFs.

1.3 Abbreviations

Term	Description
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AZ	Availability Zone
BBU	Base Band Unit
BNG	Broadband Network Gateway
CapEx	Capital Expenditure
CCS	Convergent Charging System
CDN	Content Delivery Network
CGN	Carrier-grade Network Address Translation
CIR	Committed Information Rate
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSCF	Call Session Control Function
CSDB	Circuit Switch Data Base
CSGN	Cellular Serving Gateway Node
CMS	Content Management Systems
DNS	Domain Name System
DPDK	Data Plane Development Kit
DPI	Deep Packet Inspection
DRA	Diameter Routing Agent
ECMP	Equal-Cost Multi-Path
ENUM	Telephone Number Mapping
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
ETSI NFV-TST	ETSI - Network Functions Virtualisation - Test
ETSI	ETSI - Network Functions Virtualisation - Infrastructure

NFV-IFA	
FPGA	Field-Programmable Gate Array
FW	Firewall
GB	Gigabit
GPU	Graphics Processing Unit
Gi-LAN	The Gi-LAN is the segment of the network for which service providers deploy IP functions between the packet gateway and the Internet
GGSN	Gateway GPRS Support Node
GW	Gateway
HA	High Availability
HSS	Home Subscriber Server
HW	Hardware
IMS	IP Multimedia Subsystem
kpps	Kilo Packet Per Second
IT	Information Technology
I/O	Input/Output
IaaS	Infrastructure as a Service
IO	Input/Output
IOPS	Input/Output per Second
LB	Load Balancer
MB	Megabit
MGW	Media Gateway
MME	Mobility Management Entity
MRF	Media Resource Function
MSC-S	Mobile Switching Center System
MSP	Managed Service Providers
MSS	Mobile Soft Switch
MTBF	Mean Time Between Failure
mVAS	Mobile Value Added Services
NAT	Network Address Translation
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NGIN	Next Generation Intelligent Network
NVMe	Non-Volatile Memory Express
MPLSoUDP	MPLS over UDP
NPU	Network Processing Unit

NUMA	Non-Unified Memory Access
OCP	Open Compute Platform
ODM	Original Design Manufacturing
OOO	Open Stack on Open Stack
OpEx	Operating Expenditure
OPNFV	Open Platform for NFV
QoS	Quality of Services
P/S-GW	Packet/Service Gateway
PCRF	Policy and Charging Rules Function
PE	Provider Edge
PGW	PDN (Packet Data Network) Gateway
PIR	Peak Information Rate
RAM	Random Access Memory
RAN	Radio Access Network
RR	Route Reflector
S/G-GSN	Serving/Gateway GPRS Support Node
SBC	Session Border Controller
SDO	Standards Development Organization
SecGW	Security Gateway
SDM	Subscriber Data Management
SDN	Software Defined Networking
SD-WAN	Software Defined Wide Area Network
SEC-GW	Security Gateway
SFC	Service Function Changing
SGSN	Serving GPRS Support Node
SGW	Service Gateway
SIG	Standard Information Gathering
SLA	Service Level Agreement
SPO	Smart Pricing Options
SS7FW	SS7 (Signaling System 7) Firewall
STP	Signal Transfer Point
SW	Software
TAS	Telecommunication Application Server
TMF	TM Forum
vCPU	Virtual CPU (Central Processing Unit)
vNIC	Virtual NIC (Network Interface Card)

vRouter	Virtual Router
vSwitch	Virtual Switch
VIM	Virtual Infrastructure Manager
VNF	Virtualised Network Function
VNF-C	VNF Component (can be hosted on a VM, Container, etc)
VNFM	VNF Manager
VoLTE	Voice over LTE (Long-Term Evolution 4G Standard)
VXLAN	Virtual Extensible LAN (Local Area Network)
Web RTC	WebRTC is a free, open-source project that provides web browsers and mobile applications with real-time communication via simple application programming interfaces

1.4 References

Ref	Doc Number	Title

[1]	ETSI GS NFV TST-008	Network Functions Virtualisation (NFV) Release 3;
		Testing;
		NFVI Compute and Network Metrics Specification

[2]	ETSI GS NFV TST-009	Network Functions Virtualisation (NFV) Release 3;
		Testing;
		Specification of Networking Benchmarks and Measurement Methods for NFVI

[3]	ETSI GS NFV TST-012	Network Function Virtualisation (NFV);
		Testing;
		VIM & NFVI Control and Management Performance Evaluation

[4]	ETSI NFV IFA 002	Network Functions Visualisation (NFV);
		Acceleration Technologies;
		VNF Interfaces Specification

[5]	ETSI NFV IFA027	Network Functions Virtualisation (NFV) Release 2;
		Management and Orchestration;
		Performance Measurements Specification

2 VNF requirements

The NFV Infrastructure (NFVI) is the totality of all hardware and software components which build up the environment in which VNFs are deployed, managed and executed.

It is inevitable that different VNFs require different capabilities from the underlying infrastructure and therefore metrics that define those capabilities are needed.

2.1 VNFs collateral (Sample)

The following is a list of VNFs that have been taken as samples and used to understand requirements and to drive the NFVI metrics definition.

- **Management and Control Plane:** EPC (MME, P/S-GW, S/G-GSN), IMS, SBC, PCRF, SDM, mVAS, DRA
- **User Plane and network:** RAN, BBU, MRF, BNG, CDN, PE, Switch, Router, RR, CPE
- **Security & testing:** FW, LB, DNS, AES, DPI, NAT/CGN, SecGW, Probe
- **Data Core:**
    - Packet Core: GGSN, SGW, PGW, SGSN, MME, CSGN.
    - Subscriber Management: HSS.
    - Policy & Traffic Management: PCRF, TMF
    - Optimizer: MSP.
- **Voice Core:**
    - IP Multimedia: CSCF, ENUM, TAS, SBC.
    - Database: CSDB
    - Circuit Switched: MSC-S(MSS), MGW.
    - Signalling: DRA, SGW, STP.
    - Messaging
    - Security
- **IP Core:** SEC-GW
- **SDO:**
    - Convergent Charging: CCS
    - Smart Pricing: SPO.
    - NGIN, Gi-LAN
    - SecureNet: Clean Pipe.
    - Network Security: SS7FW, CMS, SIG.
    - Others: Web RTC GW, Service integration GW
- **Fixed Access:**
    - BNG, CPE
- **Radio (Cloud RAN).**

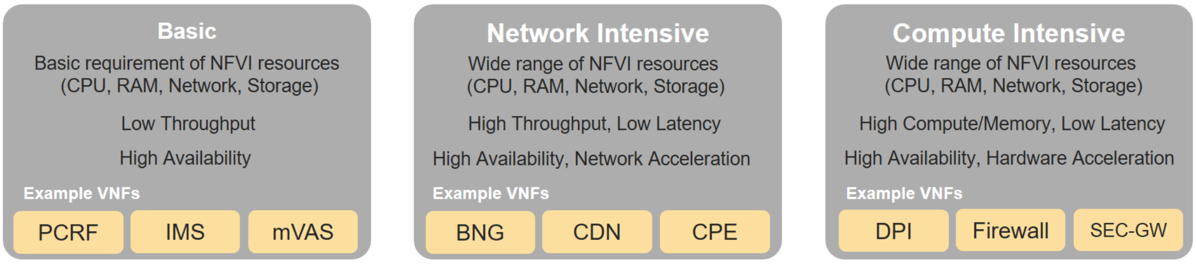
2.2 NFVI Profiles

By examining the list of VNFs provided in Section 2.1(VNFs collateral (Sample)) and understand their various requirments of NFVI capabilities and metrics, they can be categorised into the following categores.

- **Basic:** VNFs with VNF-Cs that perform basic compute operations.
- **Network intesnive**: VNFs with VNF-Cs that perform network intensive operations with high throuput and low latency requirements.
- **Compute Intensive**: VNFs with VNF-Cs that perform compute intensive operations with low latency requirements.

□ below shows proposed list of NFVI profiles to match those VNF categories.

Note: This is an initial set of proposed profiles and It is expected that more profiles will be added as more requirements are gathered and as technology enhances and matures.



Basic

Basic requirement of NFVI resources (CPU, RAM, Network, Storage)

Low Throughput

High Availability

Example VNFs

PCRF IMS mVAS

Network Intensive

Wide range of NFVI resources (CPU, RAM, Network, Storage)

High Throughput, Low Latency

High Availability, Network Acceleration

Example VNFs

BNG CDN CPE

Compute Intensive

Wide range of NFVI resources (CPU, RAM, Network, Storage)

High Compute/Memory, Low Latency

High Availability, Hardware Acceleration

Example VNFs

DPI Firewall SEC-GW

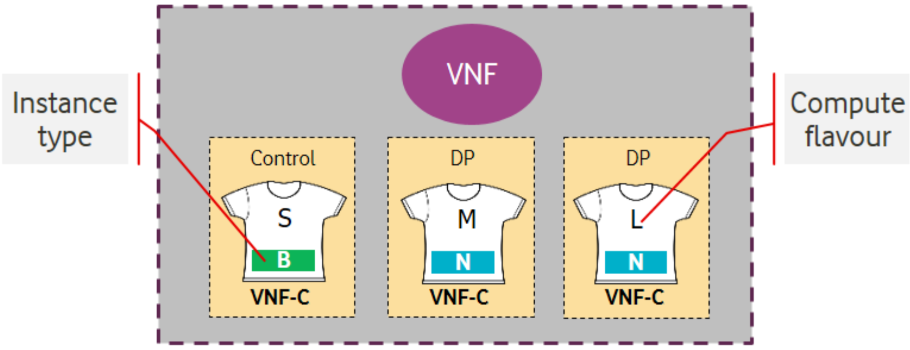
- **: Infrastructure profiles proposed based on VNFs categorisation.**

In the next chapter, Infrastructure profiles catalogue, those infrastructure profiles will be offered to VNFs in form of different instance types: B (Basic), N (Network intensive), and C (Compute intensive) respectively.

3 Infrastructure profiles catalogue

Infrastructure profiles are collection of capabilities, metrics, compute flavours, interface options, storage extensions, and acceleration capabilites that are offered by the infrastructure to VNFs. Infrastrcture profiles are offered to VNFs in form of instance types with their corresponding options and extensions.

The idea of the infrastructure profiles catalogue is to have a predefined set of instance types with a predefined set of compute flavours (sometimes refered to as T-shirt sizes) which VNF vendors use to to build their VNFs. Each VNF uses one or more of those compute flavours (with one or more of offered instance types) to build its overall functionality as illustrated in **Error! Reference source not found.**.



- **: VNFs built against standard instance types and compute flavours.**

3.1 Compute flavours

Compute flavors defines the compute, memory, storage capacity, and management network interface of an instance. The intent of this list is to be comprehensive and yet effective to cover both IT and NFV workloads.

.conf	vCPU	RAM	Local Disk	Mgmt interface
.tiny	1	512 MB	1 GB	1 Gbps
.small	1	2 GB	40 GB	1 Gbps
.medium	2	4 GB	40 GB	1 Gbps
.large	4	8 GB	80 GB	1 Gbps
.large2*	4	16 GB	80 GB	1 Gbps
.xlarge*	8	16 GB	160 GB	1 Gbps
.xlarge2*	8	32 GB	160 GB	1 Gbps
.xlarge3*	8	64 GB	160 GB	1 Gbps

Table 1: Compute flavours

* These compute flavours are intended to be used for transitional purposes and VNF vendors are expected to consume smaller flavours and adopt microservers designs for their VNFs.

3.1.1 Storage extensions

These are non ephemeral storage extensions that can be provided to VNFs for persistent data storage. More than one storage extension can be provided to a single VNF-C.

Add comment about CEPH distributed storage. (potentially create new profile for it).

.conf	Capacity	Read IO/s	Write IO/s	Read Throughput (MB/s)	Write Throughput (MB/s)
.bronze1	100GB	Up to 3K	Up to 15K	Up to 180	Up to 120
.bronze2	200GB	Up to 3K	Up to 15K	Up to 180	Up to 120
.bronze3	300GB	Up to 3K	Up to 15K	Up to 180	Up to 120
.silver1	100GB	Up to 60K	Up to 30K	Up to 1200	Up to 400
.silver2	200GB	Up to 60K	Up to 30K	Up to 1200	Up to 400
.silver3	300GB	Up to 60K	Up to 30K	Up to 1200	Up to 400
.gold1	100GB	Up to 680K	Up to 360K	Up to 2650	Up to 1400
.gold2	200GB	Up to 680K	Up to 360K	Up to 2650	Up to 1400
.gold3	300GB	Up to 680K	Up to 360K	Up to 2650	Up to 1400

Table 2: Storage extensions for compute flavours.

3.2 Instance types

3.2.1 B Instances (Basic)

This is the basic type of infrastructure profiles and is intended to be used for both IT workloads as well as NFV workloads. It has limited IO capabilities (up to 10Gbps Network interface) with a wide range of compute flavours. This instance type is intended to be available in any data centre within any Operator’s network.

B instance comes with various Interfaces options, Table below shows the various Interfaces options available for B instance type (Up to 6 interfaces are possible).

Virtual interface option*	Type	Description
1	virtio-net	1x 1Gbps network interface
1D	virtio-net	2x 1Gbps Network interface

1T*	virtio-net	3x 1Gbps Network interface
1Q, 1P, 1H*	virtio-net	4x 1Gbps, 5x 1Gbps, 6x 1Gbps
10	virtio-net	1x 10Gbps Network interface
10D	virtio-net	2x 10Gbps Network interface
10T*	virtio-net	3x 10Gbps Network interface
10Q, 10P, 10H*	virtio-net	4x 10Gbps, 5x 10Gbps, 6x 10Gbps

Table 3: Virtual NIC interfaces options for B instance type.

* These options are intended to be used for transitional purposes. VNFs are expected to use minimum number of interfaces and adopt microservers design principles.

3.2.2 N Instances (Network Intensive)

This instance type is intended to be used for those applications that has high network throughput requirements (up to 50Gbps). This instance type is more intended for VNFs and is expected to be available in regional (distributed) data centres and more towards the access networks.

N instance comes with various interfaces options, the Table below shows the various Interfaces options available for N instance types (Up to 6 interfaces are possible).

Virtual interface option	Type	Description
10	virtio-net	1x 10Gbps network interface
10D	virtio-net	2x 10Gbps Network interface
10T	virtio-net	3x 10Gbps Network interface
10Q, 10P, 10H*	virtio-net	4x 10Gbps, 5x 10Gbps, 6x 10Gbps
25	virtio-net	1x 25Gbps network interface
25D	virtio-net	2x 25Gbps Network interface
25T*	virtio-net	3x 25Gbps Network interface
25Q, 25P, 25H*	virtio-net	4x 25Gbps, 5x 1Gbps, 6x 1Gbps
40	virtio-net	1x 40Gbps Network interface
40D	virtio-net	2x 40Gbps Network interface
40T*	virtio-net	3x 40Gbps Network interface

40Q, 40P, 40H*	virtio-net	4x 40Gbps, 5x 40Gbps, 6x 40Gbps
50	virtio-net	1x 50Gbps Network interface
50D	virtio-net	2x 50Gbps Network interface
50T*	virtio-net	3x 50Gbps Network interface
50Q, 50P, 50H*	virtio-net	4x 50Gbps, 5x 50Gbps, 6x 50Gbps
100*	virtio-net	1x 100Gbps Network interface
100D*	virtio-net	2x 100Gbps Network interface
100T*	virtio-net	3x 100Gbps Network interface
100Q, 100P, 50H*	virtio-net	4x 100Gbps, 5x 100Gbps, 6x 100Gbps

Table 4: Virtual NIC interfaces options for N instance type.

* These options are intended to be used for transitional purposes. VNFs are expected to use minimum number of interfaces and adopt microservers design principles.

3.2.2.1 Network Acceleration Extensions

N instance types can come with Network Acceleration extensions to assist VNFs offloading some of their network intensive operations to hardware. The list below is preliminary and is expected to grow as more network acceleration resources are developed and standardized. Those interfaces are aligned with ETSI NFV IFA 002 [4].

.acc conf	Interface type	description
.il-ipsec	virtio-ipsec*	In-line IPSec acceleration
.la-crypto	virtio-crypto	Look-Aside encryption/decryption engine

Table 5: Acceleration extensions for N instance type.

*Note: Need to work with relevant open source communities to create missing interfaces.

3.2.3 C Instances (Compute Intensive)

This instance type is intended to be used for those applications that has high compute requirements and can take advantage of acceleration technologies such as GPU, FPGA, etc. This instance type is intended to be available in local data centers and more towards the Edge of the network.

H instance comes with various Interfaces options, the table below shows the various interfaces options available for C instance type (Up to 6 interfaces are possible).

Virtual interface option	Type	Description
10	virtio-net	1x 10Gbps network interface
10D	virtio-net	2x 10Gbps Network interface
10T	virtio-net	3x 10Gbps Network interface
10Q, 10P, 10H*	virtio-net	4x 10Gbps, 5x 10Gbps, 6x 10Gbps
25	virtio-net	1x 25Gbps network interface
25D	virtio-net	2x 25Gbps Network interface
25T*	virtio-net	3x 25Gbps Network interface
25Q, 25P, 25H*	virtio-net	4x 25Gbps, 5x 1Gbps, 6x 1Gbps
40	virtio-net	1x 40Gbps Network interface
40D	virtio-net	2x 40Gbps Network interface
40T*	virtio-net	3x 40Gbps Network interface
40Q, 40P, 40H*	virtio-net	4x 40Gbps, 5x 40Gbps, 6x 40Gbps
50	virtio-net	1x 50Gbps Network interface
50D	virtio-net	2x 50Gbps Network interface
50T*	virtio-net	3x 50Gbps Network interface
50Q, 50P, 50H*	virtio-net	4x 50Gbps, 5x 50Gbps, 6x 50Gbps

Table 6: Virtual NIC interfaces options for C instance type.

* These options are intended to be used for transitional purposes. VNFs are expected to use minimum number of interfaces and adopt microservers design principles.

3.2.3.1 Compute acceleration extensions

C instance types can come with compute acceleration extensions to assist VNF/applications offloading some of their compute intensive operations to hardware. The list below is preliminary and is expected to grow as more compute acceleration resources are developed and standardized.

.acc conf	Interface type	description
.la-trans	virtio-trans*	Look-Aside transcoding
.la-programmable	virtio-programmable*	Look-Aside programmable

		acceleration.

Table 7: Acceleration extensions for C instance type.

*Note: Need to work with relevant open source communities to create missing interfaces.

3.3 Catalogue

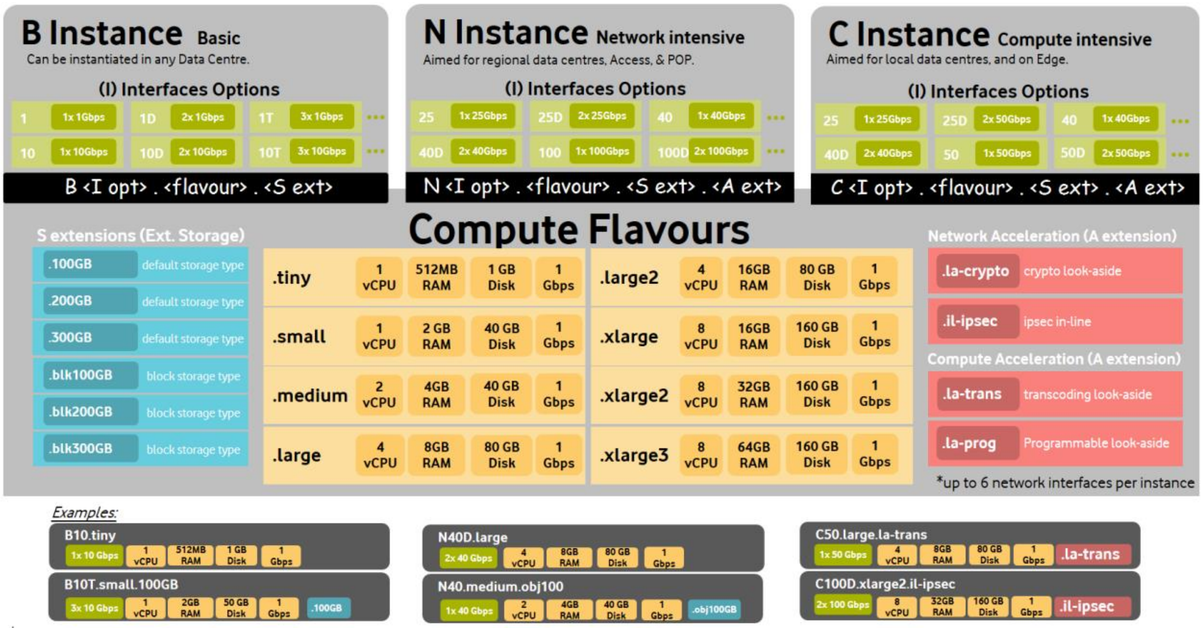
3.3.1 Naming convention

An entry in the infrastructure profile catalogue can be referenced using the following naming convention.

```
B/N/C <I opt> . <flavour> . <S ext> . <A ext>
```

Whereas:

- **B/N/C:** specifies the instance type (Basic, Network Intensive, and Compute Intensive)
- **<I opt>:** specifies the interface option of the instant.
- **<flavour>:** specifies the compute flavour.
- **<S ext>:** specifies an optional storage extension.
- **<A ext>:** specifies an optional acceleration extension for either N or H instance types.


B Instance Basic
Can be instantiated in any Data Centre.
(I) Interfaces Options
1 1x 1Gbps
1D 2x 1Gbps
1T 3x 1Gbps
10 1x 10Gbps
10D 2x 10Gbps
10T 3x 10Gbps
B <I opt> . <flavour> . <S ext>
N Instance Network intensive
Aimed for regional data centres, Access, & POP.
(I) Interfaces Options
25 1x 25Gbps
25D 2x 25Gbps
40 1x 40Gbps
40D 2x 40Gbps
100 1x 100Gbps
100D 2x 100Gbps
N <I opt> . <flavour> . <S ext> . <A ext>
C Instance Compute intensive
Aimed for local data centres, and on Edge.
(I) Interfaces Options
25 1x 25Gbps
25D 2x 50Gbps
40 1x 40Gbps
40D 2x 40Gbps
50 1x 50Gbps
50D 2x 50Gbps
C <I opt> . <flavour> . <S ext> . <A ext>
Compute Flavours
S extensions (Ext. Storage)
.100GB default storage type
.200GB default storage type
.300GB default storage type
.blk100GB block storage type
.blk200GB block storage type
.blk300GB block storage type
.tiny 1 vCPU 512MB RAM 1 GB Disk 1 Gbps
.small 1 vCPU 2 GB RAM 40 GB Disk 1 Gbps
.medium 2 vCPU 4GB RAM 40 GB Disk 1 Gbps
.large 4 vCPU 8GB RAM 80 GB Disk 1 Gbps
.large2 4 vCPU 16GB RAM 80 GB Disk 1 Gbps
.xlarge 8 vCPU 16GB RAM 160 GB Disk 1 Gbps
.xlarge2 8 vCPU 32GB RAM 160 GB Disk 1 Gbps
.xlarge3 8 vCPU 64GB RAM 160 GB Disk 1 Gbps
Network Acceleration (A extension)
.la-crypto crypto look-aside
.il-ipsec ipsec in-line
Compute Acceleration (A extension)
.la-trans transcoding look-aside
.la-prog Programmable look-aside
*up to 6 network interfaces per instance
Examples:
B10.tiny 1x 10 Gbps 1 vCPU 512MB RAM 1 GB Disk 1 Gbps
B10T.small.100GB 3x 10 Gbps 1 vCPU 2GB RAM 50 GB Disk 1 Gbps .100GB
N40D.large 2x 40 Gbps 4 vCPU 8GB RAM 80 GB Disk 1 Gbps
N40.medium.obj100 1x 40 Gbps 2 vCPU 4GB RAM 40 GB Disk 1 Gbps .obj100GB
C50.large.la-trans 1x 50 Gbps 4 vCPU 8GB RAM 80 GB Disk 1 Gbps .la-trans
C100D.xlarge2.il-ipsec 2x 100 Gbps 8 vCPU 32GB RAM 160 GB Disk 1 Gbps .il-ipsec

- **: Infrastructure profiles catalogue.**

3.3.2 Explicit NFVI capabilities

This section covers a list of explict NFVI capabilities and metrics that defines an NFVI. These capabilities and metrics are well known to VNFs as they provide capabilities which VNFs rely on.

Note: It is expected that NFVI capabilities and metrics will evolve with time as more capabilities are added as technology enhances and matures.

3.3.2.1 Explicit resource capabilities

Error! Reference source not found. below shows resource capabilities of NFVI. Those indicate resources offered to VNFs by NFVI.

Ref	NFVI capability	Unit	Definition/Notes
e.nfvi.res.cap.001	#vCPU cores	number	Min, Max number of vCPU cores that can be assigned to a single VNF-C
e.nfvi.res.cap.002	Amount of RAM (MB)	MB	Min, Max memory in MB that can be assigned to a single VNF-C by NFVI.
e.nfvi.res.cap.003	Total amount of instance (ephemeral) storage (GB)	GB	Min, Max storage in GB that can be assigned to a single VNF-C by NFVI.
e.nfvi.res.cap.004	# vNICs	number	Max number of vNIC interfaces that can be assigned to a single VNF-C by NFVI.
e.nfvi.res.cap.005	Total amount of external (persistent) storage (GB)	GB	Min, Max storage in GB that can be attached / mounted to VNF-C by NFVI.
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
e.nfvi.res.cap.001	As per selected <flavour>	As per selected <flavour>	As per selected <flavour>
e.nfvi.res.cap.002	As per selected <flavour>	As per selected <flavour>	As per selected <flavour>
e.nfvi.res.cap.003	As per selected <flavour>	As per selected <flavour>	As per selected <flavour>
e.nfvi.res.cap.004	As per selected <I Opt>	As per selected <I Opt>	As per selected <I Opt>
e.nfvi.res.cap.005	As per selected <S Ext>	As per selected <S Ext>	As per selected <S Ext>

Table 8: Explicit resource capabilities of NFVI.

3.3.2.2 Explicit performance optimisation capabilities

Error! Reference source not found. below shows possible performance optimisation capabilities that can be provided by NFVI. These indicate capabilities exposed to VNFs. Those capabilities need to be consumed by VNFs in a standard way.

Ref	NFVI capability	Unit	Definition/Notes
e.nfvi.per.cap.001	CPU pinning support	**Yes/No**	Determining if NFVI support CPU pinning
e.nfvi.per.cap.002	NUMA support	**Yes/No**	Determining if NFVI support NUMA awareness
e.nfvi.per.cap.003	IPSec Acceleration	**Yes/No**	IPSec Acceleration
e.nfvi.per.cap.004	Crypto Acceleration	**Yes/No**	Crypto Acceleration
e.nfvi.per.cap.005	Transcoding Acceleration	**Yes/No**	Transcoding Acceleration
e.nfvi.per.cap.006	Programmable	**Yes/No**	Programmable Acceleration

	Acceleration		
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
e.nfvi.per.cap.001	No	Yes	Yes
e.nfvi.per.cap.002	No	Yes	No
e.nfvi.per.cap.003	No	Yes (if offered)	No
e.nfvi.per.cap.004	No	Yes (if offered)	No
e.nfvi.per.cap.005	No	No	Yes (if offered)
e.nfvi.per.cap.006	No	No	Yes (if offered)

Table 9: Explicit performance optimisation capabilities of NFVI.

3.3.2.3 Expliict monitoring capabilities

Table 10 below shows possible monitoring capabilities available by NFVI for VNFs.

Ref	NFVI capability	Unit	Definition/Notes
e.nfvi.mon.cap.001	Monitoring of L2-7 data	**Yes/No**	Ability for VNF-C to monitor their own L2-L7 data.
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
e.nfvi.mon.cap.001	No	Yes	No

Table 10: Explicit monitoring capabilities of NFVI.

3.3.3 Explicit NFVI metrics

3.3.3.1 Expliict performance metrics

Table 11 below shows performance metrics of NFVI. The intent of those metircs is to be well known to VNFs. These metrics are aligned with ETSI GS NFV TST-009 [2].

Ref	NFVI capability	Unit	Definition/Notes
e.nfvi.per.met.001	Network Throughput	**bps**	Max thougput per vNIC assigned to VNF-C @256 Bytes.
e.nfvi.per.met.002	Network Latency	**ms**	Range (min, max) on each vNIC assigned to VNF-C. ETSI NFV-TST 009[2].
e.nfvi.per.met.003	External (persistent) storage IO	**Iops**	Range (min, max) per VNF-C
e.nfvi.per.met.004	External (persistent) storage throughput	**MB/s**	Range (min, max) per VNF-C
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
e.nfvi.per.met.001	Up to speed of <I Opt>	Up to speed of <I Opt>	Up to speed of <I Opt>
e.nfvi.per.met.002	<30ms	<0.5	<5
e.nfvi.per.met.003	As per selected <S Ext>	As per selected <S Ext>	As per selected <S Ext>
e.nfvi.per.met.004	As per selected <S Ext>	As per selected <S Ext>	As per selected <S Ext>

Table 11: Explicit performance metrics of NFVI.

3.4 Implicit NFVI capabilities and metrics

This section covers a list of implicit NFVI capabilities and metrics that defines the interior of NFVI. These capabilities and metrics determines how NFVI behaves internally. They are hidden from VNFs (i.e. VNFs may not know about them) but they will have a big impact on the overall performance and capabilities of a given NFVI solution.

Note: It is expected that implicit NFVI capabilities and metrics will evolve with time as more capabilities are added as technology enhances and matures.

3.4.1 Implicit NFVI capabilities

3.4.1.1 Implicit resource capabilities

Table 12 below shows resource capabilities of NFVI. These include capabilities offered to VNFs and resources consumed internally by NFVI.

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.res.cap.001	Number of vCPU cores consumed by NFVI software in a single compute nodes.	% (of total available)	This indicates the number of vCPU cores consumed (wasted) by NFVI components (including host OS) in a compute node.
i.nfvi.res.cap.002	Amount of memory consumed by NFVI software in a single compute nodes.	% (of total available)	This indicates the amount of memory consumed (wasted) by NFVI components (including host OS) in a compute node.
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.res.cap.001	5-10%	10-20%	15-25%
i.nfvi.res.cap.002	5-10%	10-20%	15-25%

Table 12: Implicit resource capabilities of NFVI.

3.4.1.2 Implicit SLA capabilities

Table 13 below shows SLA (Service Level Agreement) capabilities available by NFVI. These include capabilities required by VNFs as well as internal capabilities to NFVI. These capabilities will be determined by the standard instance type used by VNF-C (Please see Section 3)

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.sla.cap.001	CPU overbooking	**1:N**	
i.nfvi.sla.cap.002	vNIC QoS	**Yes/No**	QoS enablement
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.sla.cap.001	1:4	1:1	1:1
i.nfvi.sla.cap.002	No	Yes	Yes

Table 13: Implicit SLA capabilities of NFVI.

3.4.1.3 Implicit performance optimisation capabilities

Table 14 below shows possible performance optimisation capabilities that can be provided by NFVI. These include capabilities exposed to VNFs as well as internal capabilities to NFVI. These capabilities will be determined by the standard instance type used by VNF-C (VNF Component) (Please see Section 3)

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.per.cap.001	Huge page support	**Yes/No**	Determining if NFVI support huge pages.
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.per.cap.001	No	Yes	No

Table 14: Implicit performance optimisation capabilities of NFVI.

3.4.1.4 Implicit monitoring capabilities

Table 15 below shows possible monitoring capabilities available by NFVI. The availability of these capabilities will be determined by the instance type used by VNFs. (See Section 3).

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.mon.cap.001	Host CPU usage		Per Compute node. It needs to Maps to ETSI NFV-TST 008[1] clause 6, processor usage metric (NFVI exposed to VIM) and ETSI NFV-IFA 027 Mean Virtual CPU usage and Peak Virtual CPU usage (VIM exposed to VNFM).
i.nfvi.mon.cap.002	Virtual compute resource CPU usage		
i.nfvi.mon.cap.003	Host CPU utilization		Per Compute node. It needs to map to ETSI NFV-IFA 027 Mean Virtual CPU usage and Peak Virtual CPU usage (VIM, exposed to VNFM).
i.nfvi.mon.cap.004	Virtual compute resource CPU utilization		
i.nfvi.mon.cap.005	Monitoring of external storage IOPS	**Yes/No**	
i.nfvi.mon.cap.006	Monitoring of external storage throughput	**Yes/No**	
i.nfvi.mon.cap.007	Monitoring of external storage capacity	**Yes/No**	
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.mon.cap.001	Yes	Yes	Yes
i.nfvi.mon.cap.002	Yes	Yes	Yes
i.nfvi.mon.cap.003	Yes	Yes	Yes
i.nfvi.mon.cap.004	Yes	Yes	Yes
i.nfvi.mon.cap.005	Yes	No	Yes
i.nfvi.mon.cap.006	Yes	No	Yes
i.nfvi.mon.cap.007	Yes	No	Yes

Table 15: Implicit monitoring capabilities of NFVI.

3.4.1.5 Implicit security capabilities

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.sec.cap.001	VNF-C<->VNF-C memory isolation	**Yes/No**	Are VNF-C memories isolated from each other by hardware support?
i.nfvi.sec.cap.002	VNF-C -> Host	**Yes/No**	Can VNF-C access host memory?
i.nfvi.sec.cap.003	Host -> VNF-C	**Yes/No**	Can Host access VNF-C memory?
i.nfvi.sec.cap.004	External storage at-rest encryption	**Yes/No**	Is external storage encrypted at-rest?
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.sec.cap.001	Yes	Yes	Yes
i.nfvi.sec.cap.002	No	No	No
i.nfvi.sec.cap.003	Yes	No	No
i.nfvi.sec.cap.004	Yes	Yes	Yes

Table 16: Implicit security capabilities of NFVI.

3.4.2 Implicit NFVI metrics

3.4.2.1 Implicit resources management metrics

Table 17 below shows resource management metrics of NFVI as aligned with ETSI GS NFV TST-012 [3]. Some of these metrics are related to what VNFs sees from the infrastructure and some of them are internal to NFVI.

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.rmt.met.001	Time to create VNF-C for a given VNF	**Maxvms**	To support scaling operations
i.nfvi.rmt.met.002	Time to delete VNF-C of a given VNF	**Max ms**	To support scaling operations
i.nfvi.rmt.met.003	Time to start VNF-C of a given VNF	**Max ms**	
i.nfvi.rmt.met.004	Time to stop VNF-C of a given VNF	**Max ms**	
i.nfvi.rmt.met.005	Time to pause VNF-C of a given VNF	**Max ms**	
i.nfvi.rmt.met.006	Time to create internal virtual network	**Max ms**	
i.nfvi.rmt.met.007	Time to delete internal virtual network	**Max ms**	
i.nfvi.rmt.met.008	Time to update internal virtual network	**Max ms**	
i.nfvi.rmt.met.009	Time to create external virtual network	**Max ms**	
i.nfvi.rmt.met.010	Time to delete external virtual network	**Max ms**	
i.nfvi.rmt.met.011	Time to update external	**Max ms**	

	virtual network		
i.nfvi.rmt.met.012	Time to create vSwitch	**Max ms**	
i.nfvi.rmt.met.013	Time to create vRouter	**Max ms**	
i.nfvi.rmt.met.014	Time to create external storage ready for use by VNF	**Max ms**	
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.rmt.met.001			
i.nfvi.rmt.met.002			
i.nfvi.rmt.met.003			
i.nfvi.rmt.met.004			
i.nfvi.rmt.met.005			
i.nfvi.rmt.met.006			
i.nfvi.rmt.met.007			
i.nfvi.rmt.met.008			
i.nfvi.rmt.met.009			
i.nfvi.rmt.met.010			
i.nfvi.rmt.met.011			
i.nfvi.rmt.met.012			
i.nfvi.rmt.met.013			
i.nfvi.rmt.met.014			

Table 17: Implicit resource management metrics of NFVI.

3.4.2.2 Implicit performance Metrics

Table 18 below shows performance metrics of NFVI. Some of these metrics are related to what VNFs sees from the infrastructure and some of them are internal to NFVI. These metrics are aligned with ETSI GS NFV TST-009 [2].

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.per.met.001	Network I/O East/West	**Mpps @256Bytes**	VNF-C to VNF-C within same platform. Do we need to expose it to VNF?
i.nfvi.per.met.002	Simultaneous active flows	**max #**	
i.nfvi.per.met.003	New flows per second	**flows/s**	
i.nfvi.per.met.004	Network Latency	**ms**	ETSI NFV-TST 009[2].
i.nfvi.per.met.005	ephemeral storage IO	**iops**	Range (min, max)
i.nfvi.per.met.006	ephemeral storage throughput	**MB/s**	Range (min, max) per VNF-C
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.per.met.001	3-5	15 - 30	3-5
i.nfvi.per.met.002	Up to 200K	Up to 1M	Up to 200K
i.nfvi.per.met.003			

i.nfvi.per.met.004	<10ms	<0.5ms	<5ms
i.nfvi.per.met.005	280K-680K	280K-680K	280K-680K
i.nfvi.per.met.006	1000 – 2650	1000 – 2650	1000 – 2650

Table 18: Implicit performance metrics exposed to VNFs by NFVI.

3.4.2.3 Implicit SLA metrics

Table 19 below shows SLA metrics of NFVI. Expected values of these metrics are determined by the standard instance type used by VNF-C (Please see Section 3)

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.sla.met.001	vNIC CIR	**bbs**	Committed Information Rate per vNIC
i.nfvi.sla.met.002	vNIC PIR	**bbs**	Peak Information Rate per vNIC
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.sla.met.001	NA	As per vNIC option	NA
i.nfvi.sla.met.002	NA	As per vNIC option	NA

Table 19: Implicit SLA metrics of NFVI.

3.4.2.4 Implicit scalability metrics

Table 20 below shows scalability of NFVI. These metrics are aligned with ETSI GS NFV TST-012 [3]

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.scl.met.001	Time to scale out VNF	**Max ms**	Excluding initial VNF deployment.
i.nfvi.scl.met.002	Time to scale in VNF	**Max ms**	
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.scl.met.001			
i.nfvi.scl.met.002			

Table 20: Implicit scalability metrics of NFVI.

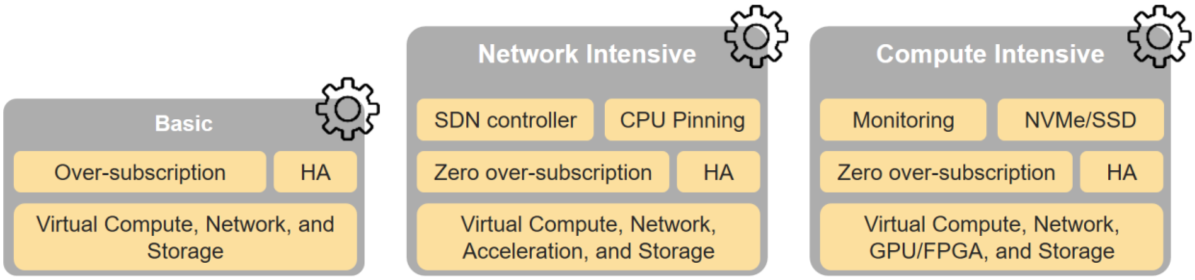
3.4.2.5 Implicit availability/reliability metrics

Ref	NFVI capability	Unit	Definition/Notes
i.nfvi.arl.met.001	Availability	**%**	
i.nfvi.arl.met.002	MTBF single node	**days**	Mean Time between Failure for single node
i.nfvi.arl.met.003	MTBF AZ	**days**	Mean Time between Failure for an AZ
i.nfvi.arl.met.004	Recovery time	**seconds**	
Mapping to instance types			
Ref	**B Instance**	**N instance**	**C instance**
i.nfvi.arl.met.001			
i.nfvi.arl.met.002			
i.nfvi.arl.met.003			

i.nfvi.arl.met.004			

4 Reference NFVI SW profiles and configurations

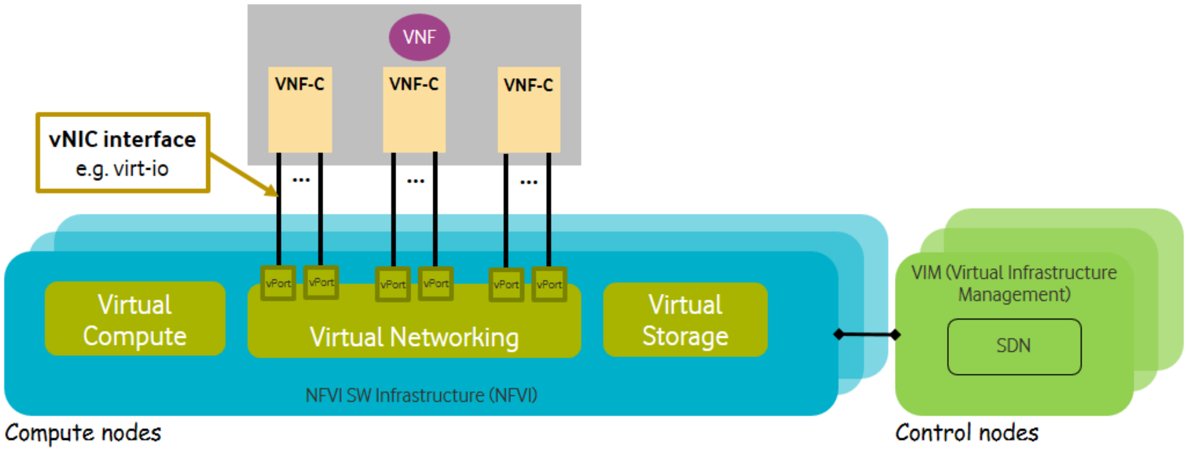
Depending on the requirements of VNFs and the capabilities expected from the infrastructure, this area is defining the right infrastructure configuration that is needed for each profile.



- **: Reference NFVI software profiles.**

4.1 Basic NFVI reference SW profile and configuration

This NFVI SW Profile and configuration will be suitable for **B instance** type (Please see Section 3). □ below shows the reference architecture of the NFVI solution.



- **: Reference NFVI software profile and configuration for B instance.**

4.1.1 Virtual Compute

Reference	Feature	Configuration	Mandatory	Description
nfvi.com.cfg.001	VM Flavours	All flavours listed in Table 1	Yes	Supported VM Flavours needs to be the same as those listed in the compute flavours catalogue.
nfvi.com.cfg.002	Hyperthreading	Enabled	Yes	Hyperthreading needs to be enabled and allowed.
nfvi.com.cfg.003				

Table 21: Virtual Compute Configuration for B instance.

4.1.2 Virtual Storage

Reference	Feature	Configuration	Mandatory	Description
nfvi.stg.cfg.001	Storage Flavours	All flavours listed in Table 2	Yes	Supported Storage Flavours needs to be the same as those listed in the catalogue.
nfvi.stg.cfg.002				
nfvi.stg.cfg.003				

Table 22: Virtual Storage Configuration for B instance.

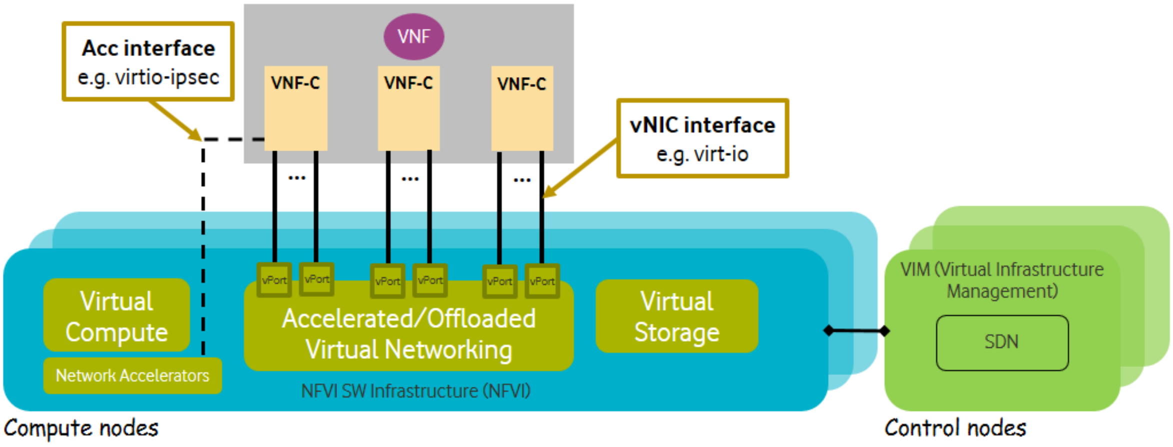
4.1.3 Virtual Networking and SDN

Reference	Feature	Configuration	Mandatory	Description
nfvi.net.cfg.001	vNIC Interface	Virtio1.1		vNIC interface needs to be virtio1.1.
nfvi.net.cfg.002	Overlay protocol	VXLAN, MPLSoUDP, GENEVE, other		The overlay network encapsulation protocol needs to enable ECMP in the underlay to take advantage of the scale-out features of the network fabric.
nfvi.net.cfg.003	SFC support	-		
nfvi.net.cfg.004	Traffic patterns symmetry			Traffic patterns should be optimal, in terms of packet flow. North-south traffic shall not be concentrated in specific elements in the architecture, making those critical choke-points, unless strictly necessary (i.e. when NAT 1:many is required).
nfvi.net.cfg.005	Horizontal scaling			The VNF cluster must be able to scale horizontally and to leverage technologies such as ECMP to enable scale-outs/scale-ins, privileging Active-Active HA models, even though this may require some level of application re-design to cope with the need of sharing state between VNF instances.

Table 23: Virtual Networking and SDN Configuration for B instance.

4.2 Network intensive NFVI reference SW profile and configuration

This NFVI SW Profile and configuration will be suitable for both **B and N instance** types (Please see Section 3)



- **: Reference NFVI software profile and configuration for N instance.**

4.2.1 Virtual Compute

Reference	Feature	Configuration	Mandatory	Description
nfvi.com.cfg.001	VM Flavours	All flavours listed in Table 1	Yes	Supported VM Flavours needs to be the same as those listed in the compute flavours catalogue.
nfvi.com.cfg.002	Hyperthreading	Enabled	Yes	Hyperthreading needs to be enabled and allowed.
nfvi.com.cfg.003				

Table 24: Virtual Compute Configuration for N instance.

4.2.2 Virtual Storage

Reference	Feature	Configuration	Mandatory	Description
nfvi.stg.cfg.001	Storage Flavours	All flavours listed in Table 2	Yes	Supported Storage Flavours needs to be the same as those listed in the catalogue.
nfvi.stg.cfg.002				

Table 25: Virtual Storage Configuration for N instance.

4.2.3 Virtual Networking and SDN

Reference	Feature	Configurations	Mandatory	Description
nfvi.net.cfg.001	vNIC Interface	Virtio1.1		vNIC interface needs to be virtio1.1.

nfvi.net.cfg.002	Overlay protocol	VXLAN, MPLSoUDP, GENEVE, other		The overlay network encapsulation protocol needs to enable ECMP in the underlay to take advantage of the scale-out features of the network fabric.
nfvi.net.cfg.003	SFC support	-		
nfvi.net.cfg.004	Traffic patterns symmetry			Traffic patterns should be optimal, in terms of packet flow. North-south traffic shall not be concentrated in specific elements in the architecture, making those critical choke-points, unless strictly necessary (i.e. when NAT 1:many is required).
nfvi.net.cfg.005	Horizontal scaling			The VNF cluster must be able to scale horizontally and to leverage technologies such as ECMP to enable scale-outs/scale-ins, privileging Active-Active HA models, even though this may require some level of application re-design to cope with the need of sharing state between VNF instances.
nfvi.net.cfg.006	vRouter/vSwitch			The vRouter/vSwitch elements must be optimised/accelerated and/or HW offloadable.

Table 26 : Virtual Networking and SDN configuration for N instance.

4.2.4 Virtual Acceleration

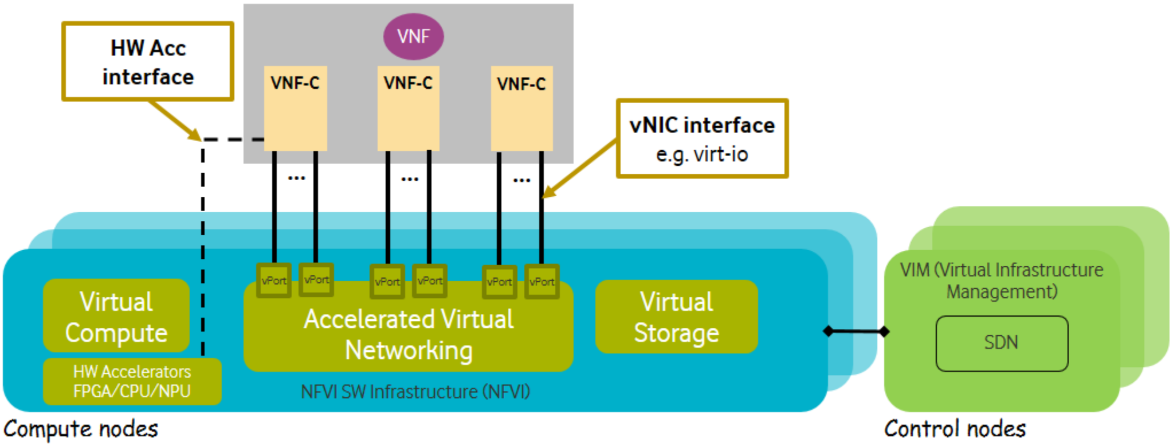
Reference	Feature	Configuration	Mandatory	Description
nfvi.acc.cfg.001	Crypto Acceleration	Supported	No	

nfvi.acc.cfg.002	Crypto Acceleration Interface	VDPA/virtio-ipsec	Yes	To be decided what interface it needs to support.
nfvi.acc.cfg.003				

Table 27: Virtual Acceleration configuration for N instance.

4.3 Compute intensive NFVI reference SW profile and configuration

This NFVI SW profile and configuration will be suitable for **C instance** type (Please see Section 3)


HW Acc interface
VNF
VNF-C
VNF-C
VNF-C
vNIC interface
e.g. virt-io
vPort
Virtual Compute
HW Accelerators FPGA/CPU/NPU
Accelerated Virtual Networking
Virtual Storage
NFVI SW Infrastructure (NFVI)
VIM (Virtual Infrastructure Management)
SDN
Compute nodes
Control nodes

- **: Reference NFVI software profile and configuration for C instance.**

4.3.1 Virtual Compute

Reference	Feature	Configuration	Mandatory	Description
nfvi.com.cfg.001	VM Flavours	All flavours listed in Table 1	Yes	Supported VM Flavours needs to be the same as those listed in the compute flavours catalogue.
nfvi.com.cfg.002	Hyperthreading	Enabled	Yes	Hyperthreading needs to be enabled and allowed.
nfvi.com.cfg.003				

Table 28: Virtual Compute Configuration for C instance.

4.3.2 Virtual Storage

Reference	Feature	Configuration	Mandatory	Description
nfvi.stg.cfg.001	Storage Flavours	All flavours listed in Table 2	Yes	Supported Storage Flavours needs to be the same as those listed in the catalogue.

nfvi.stg.cfg.002				
nfvi.stg.cfg.003				

Table 29: Virtual Storage Configuration for C instance.

4.3.3 Virtual Networking and SDN

Reference	Feature	Options	Mandatory	Description
nfvi.net.cfg.001	vNIC Interface	Virtio1.1		vNIC interface needs to be virtio1.1.
nfvi.net.cfg.002	Overlay protocol	VXLAN, MPLSoUDP, GENEVE, other		The overlay network encapsulation protocol needs to enable ECMP in the underlay to take advantage of the scale-out features of the network fabric.
nfvi.net.cfg.003	SFC support	-		
nfvi.net.cfg.004	Traffic patterns symmetry			Traffic patterns should be optimal, in terms of packet flow. North-south traffic shall not be concentrated in specific elements in the architecture, making those critical choke-points, unless strictly necessary (i.e. when NAT 1:many is required).
nfvi.net.cfg.005	Horizontal scaling			The VNF cluster must be able to scale horizontally and to leverage technologies such as ECMP to enable scale-outs/scale-ins, privileging Active-Active HA models, even though this may require some level of application re-design to cope with the need of sharing state between VNF instances.
nfvi.net.cfg.006	vRouter/vSwitch			The vRouter/vSwitch elements must be optimised/accelerated and/or HW offloadable

Table 30: Virtual Networking and SDN Configuration for C instance.

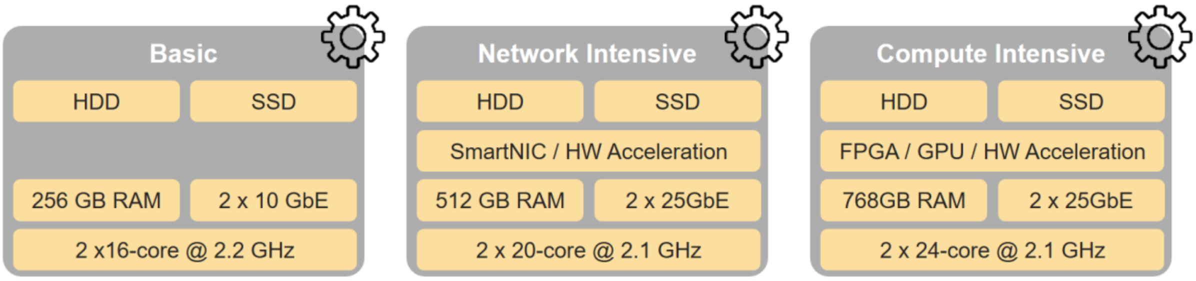
4.3.4 Virtual Acceleration

Reference	Feature	Configuration	Mandatory	Description
nfvi.acc.cfg.001				
nfvi.acc.cfg.002				
nfvi.acc.cfg.003				

Table 31: Virtual Acceleration Configuration for C instance.

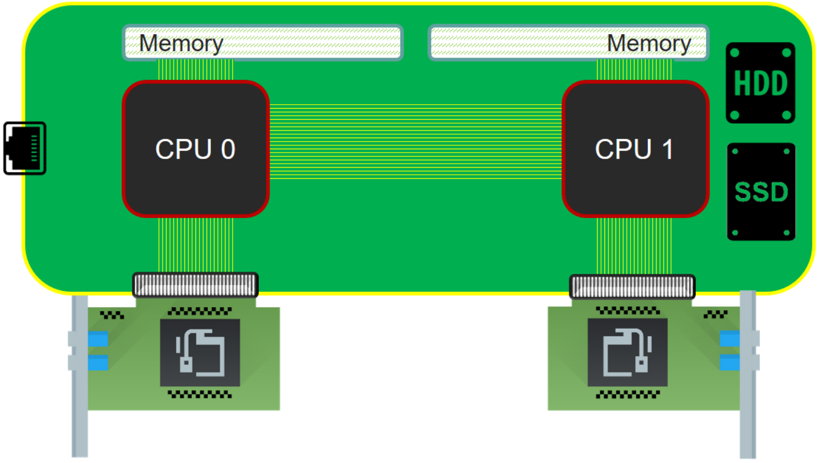
5 Reference NFVI HW profiles and configurations

This chapter defined various hardware configuratioins that are suitable for the defined profiles.



- **: Reference NFVI hardware profiles.**

5.1 Basic NFVI reference HW profile and configuration



- **: Reference NFVI hardware configuration for B instance.**

5.1.1 CPU Configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.cpu.cfg.001	Number of CPU Sockets	2		This determines the number of CPU sockets exist within each platform.
nfvi.hw.cpu.cfg.002	Number of Cores per CPU	14-16		This determines the number of cores needed per each CPU.
nfvi.hw.cpu.cfg.003	Clock Speed	>= 2.2		This determines the Clock speed of CPU.

Table 32: Hardware CPU configuration for B instance.

5.1.2 PCI Configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.pci.cfg.001	PCIe Slots	>= 2		Number of PCIe slots available in the platform
nfvi.hw.pci.cfg.002	PCIe Speed	>= Gen3		PCIe slots in the platform has to support at least Gen 3.
nfvi.hw.pci.cfg.003	PCIe Lanes	>= 8		PCIe slots in the platform has to have at least 8 lanes each.

Table 33: Hardware PCI configuration for B instance.

5.1.3 Security Configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.sec.cfg.001	TPM	Yes		Platform must have Trusted Platform Module.

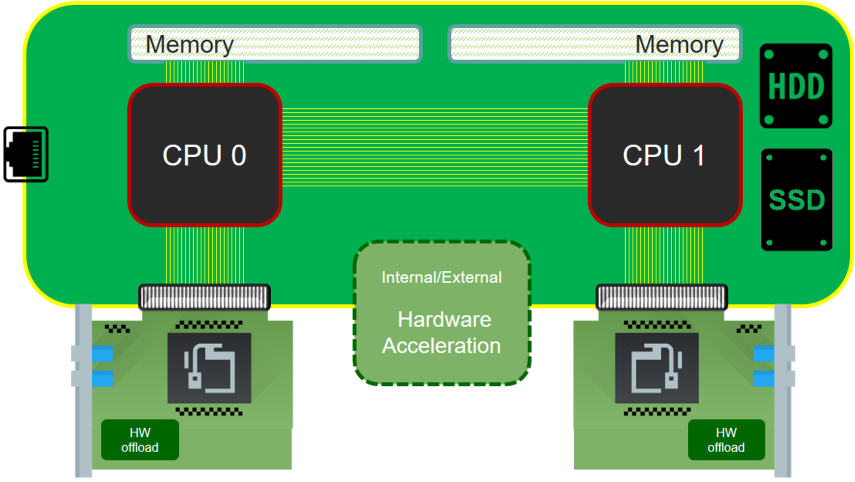
Table 34: Hardware Security configuration for B instance.

5.1.4 Storage Configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.stg.cfg.001	Local Storage	HDD/SSD	No	This determines local storage configurations.

Table 35: Hardware Storage configuration for B instance.

5.2 Network Intensive NFVI reference HW profile and configuration



- **: Reference NFVI hardware configuration for N instance.**

5.2.1 CPU configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.cfg.001	Number of CPU Sockets	2		This determines the number of CPU sockets exist within each platform.
nfvi.hw.cfg.002	Number of Cores per CPU	20-24		This determines the number of cores needed per each CPU.
nfvi.hw.cfg.003	Clock Speed	>= 2.1		This determines the Clock speed of CPU.

Table 36: Hardware CPU configuration for N instance.

5.2.2 PCI configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.pci.cfg.001	PCIe Slots	>= 3		Number of PCIe slots available in the platform
nfvi.hw.pci.cfg.002	PCIe Speed	>= Gen3		PCIe slots in the platform has to support at least Gen 3.
nfvi.hw.pci.cfg.003	PCIe Lanes	>= 16		PCIe slots in the platform has to have at least 16 lanes each.

Table 37: Hardware PCI configuration for N instance.

5.2.3 Security configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.sec.cfg.001	TPM	Yes		Platform must have Trusted Platform Module.

Table 38: Hardware security configuration for N instance.

5.2.4 Storage configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.stg.cfg.001	Local Storage	HDD/SSD		This determines local storage configurations.

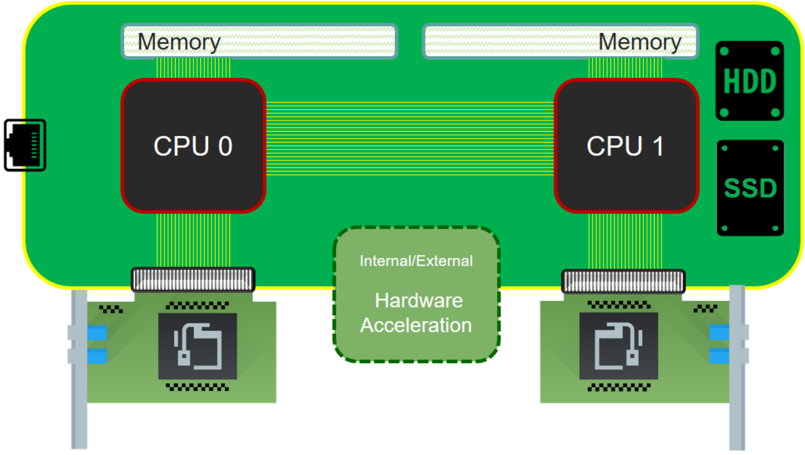
Table 39: Hardware storage configuration for N instance.

5.2.5 Hardware Acceleration configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.acc.cfg.002	Hardwae Acceleration	IPSec, Crypto		
nfvi.hw.acc.cfg.003	SmartNIC	vSwitch Offload		A SmartNIC that is used to offload vSwitch functionality to hardware.

Table 40: Hardware Acceleration configuration for N instance.

5.3 Compute Intensive NFVI reference HW Profile and configuration



- **: Reference NFVI hardware configuration for C instance.**

5.3.1 CPU configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.cpu.cfg.001	Number of CPU Sockets	2		This determines the number of CPU sockets exist within each platform.
nfvi.hw.cpu.cfg.002	Number of Cores per CPU	22-24		This determines the number of cores needed per each CPU.
nfvi.hw.cpu.cfg.003	Clock Speed	>= 2.1		This determines the Clock speed of CPU.

Table 41: Hardware CPU configuration for C instance.

5.3.2 PCIe configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.pci.cfg.001	PCIe Slots	>= 2		Number of PCIe slots available in the platform
nfvi.hw.pci.cfg.002	PCIe Speed	>= Gen3		PCIe slots in the platform has to support at least Gen 3.
nfvi.hw.pci.cfg.003	PCIe Lanes	>= 16		PCIe slots in the platform has to have at least 16 lanes each.

Table 42: Hardware PCI configuration for C instance.

5.3.3 Security configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.sec.cfg.007	TPM	Yes		Platform must have Trusted Platform Module.

Table 43: Hardware security configuration for C instance.

5.3.4 Storage configurations

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.stg.cfg.001	Local Storage	HDD/SSD	No	This determines local storage configurations.

Table 44: Hardware storage configuration for C instance.

5.3.5 Hardware Acceleration configuration

Reference	Feature	Configuration	Mandatory	Description
nfvi.hw.acc.cfg.002	Hardwae Acceleration	IPSec, Crypto		

Table 45: Hardware Acceleration configuration for C instance.

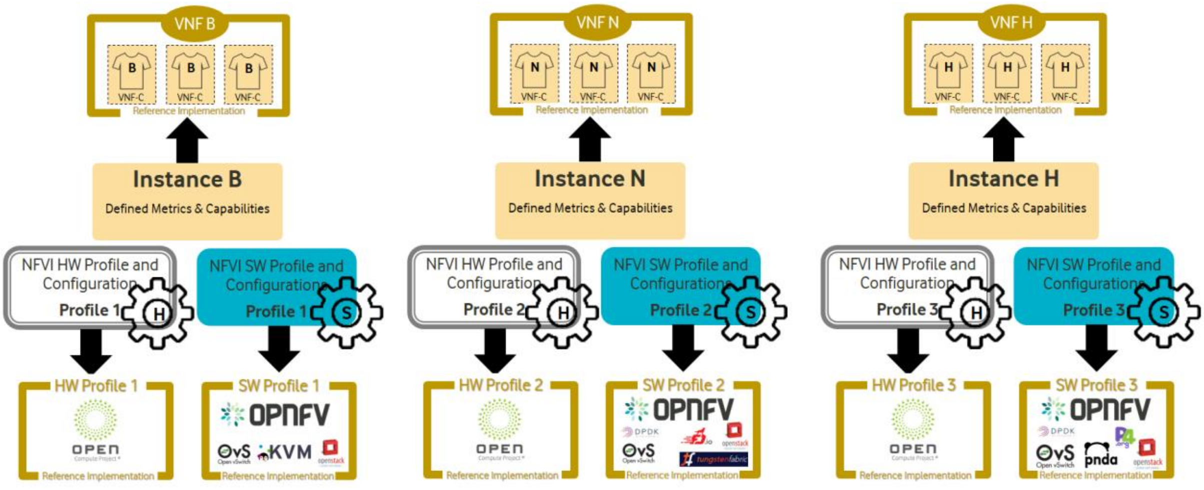
6 Compliance, Verification, and Certification

6.1 NFVI Profiles reference implementations.

For compliance, verification, and certification, of NFVI solutions provided for a given NFVI Profile, it is required to have a reference implementation of each profile so it can be used for compliance, validation, and certification.

Those reference implementations need to reflect on their corresponding profiles and deliver all metrics and capabilities promised. They need to use open source components. □ below shows the various reference implementations required for each profile, they are:

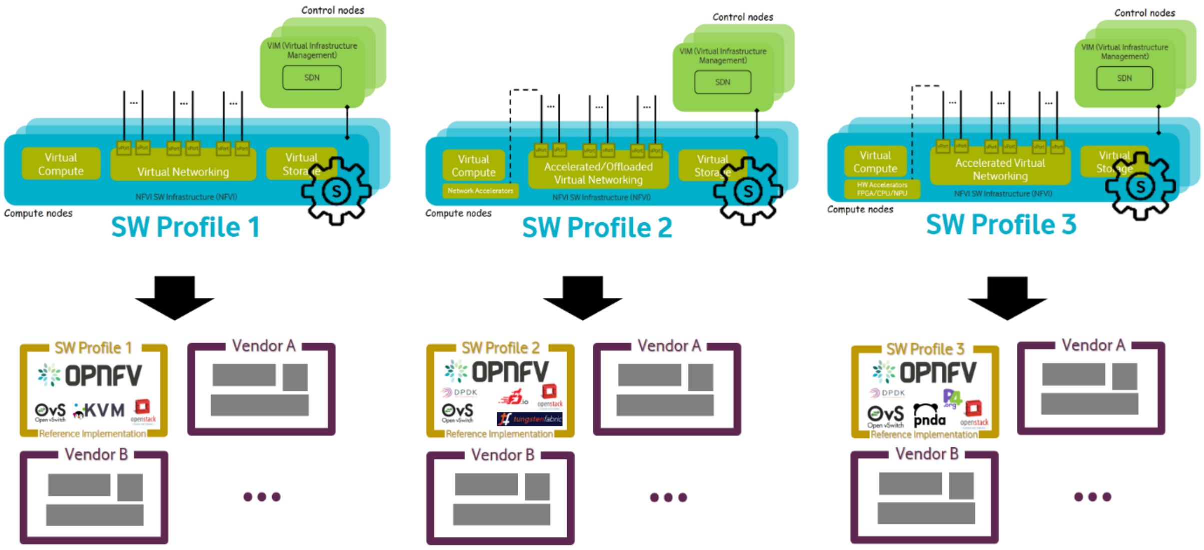
- NFVI SW Reference implementation.
- NFVI HW Reference implementation.
- VNF reference implementation.



- **: Reference NFVI profiles implementation**

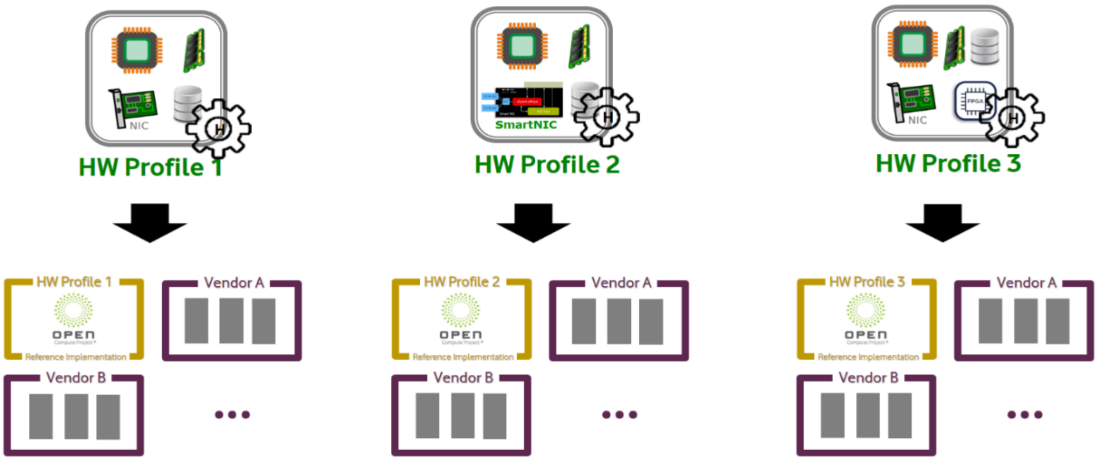
6.2 Vendor supplied NFVI solutions.

Infrastructure Abstraction and Profiling allows NFVI SW vendors to provide solutions that are suitable for a given profile (as demonstrated in □). Having NFVI solutions tailored towards a given profile makes it easier to verify, certify and test that solution against that profile using the reference implementation of the profile mentioned previously.



- **: Vendor supplied NFVI SW solutions.**

Similarly, Infrastructure Abstraction and Profiling allows NFVI HW vendors to provide solutions that are suitable for a given profile (as demonstrated in □). Having NFVI hardware solutions tailored towards a given profile makes it easier to verify, certify and test that hardware solution against that profile using the reference implementation of the profile mentioned previously.



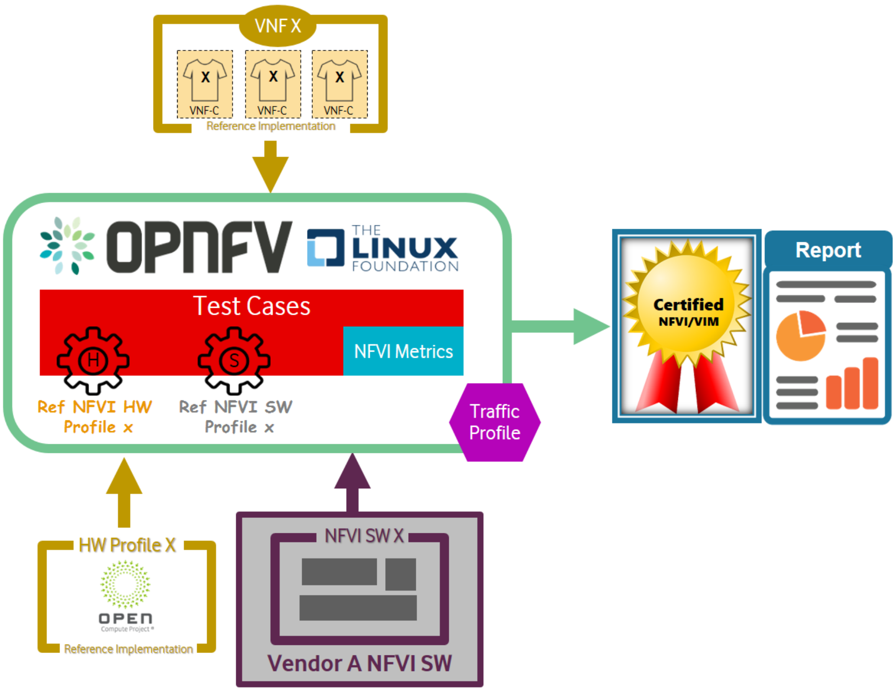
- **: Vendor supplied NFVI HW solutions.**

6.3 NFVI Compliance, Verification and Certification

Infrastructure abstraction and profiling makes it easier for a given NFVI SW solutions to be validated, certified and tested against the profile it is intended for.

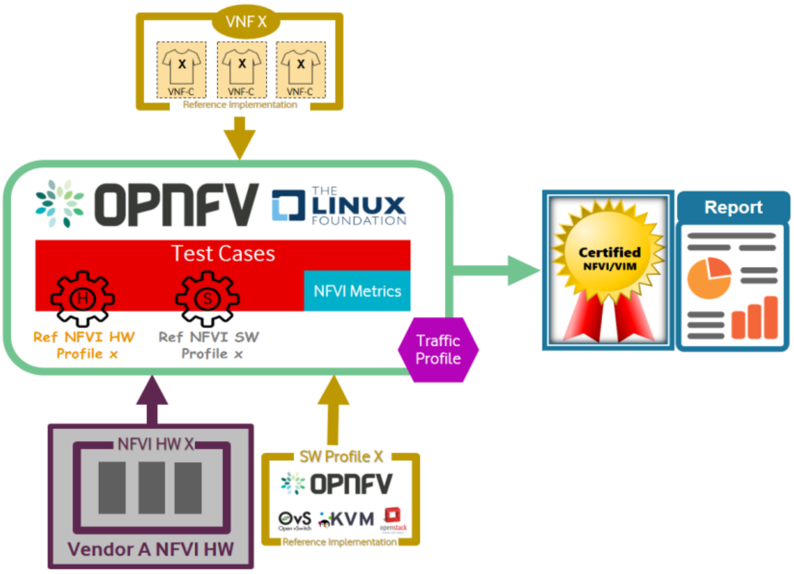
Having a deterministic NFVI metrics and capabilities expected for a given profile, allows NFVI SW solutions to be characterised, validated, and verified against those metrics and capabilities, and therefore report the results in a standard format. This will allow operators to understand in depth the details and the differentiation a given solution can provide against other options.

 below demonstrates how a given NFVI SW solution can be validated and certified against a given profile by using a reference HW implementation and a reference NFVI implementation.



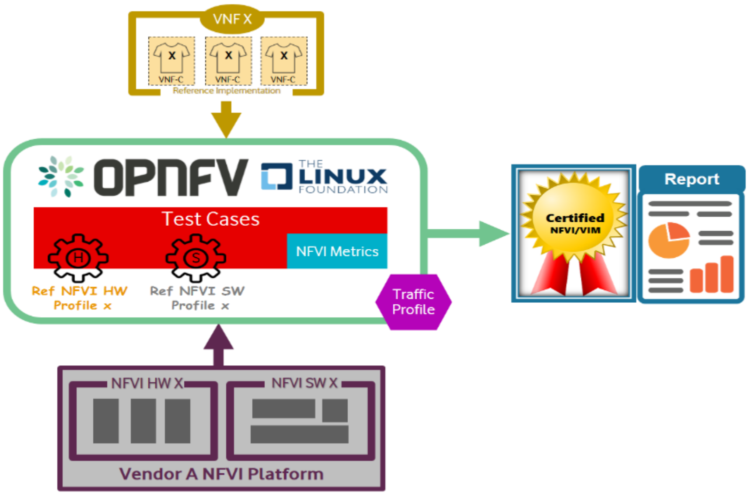
- **: Certifying Vendor NFVI SW solutions.**

Similarly, to characterise, validate, and certify NFVI HW solution against a given profile, both NFVI SW reference implementation and a VNF reference implementation are needed as demonstrated as in below.



- **: Certifying NFVI HW solutions.**

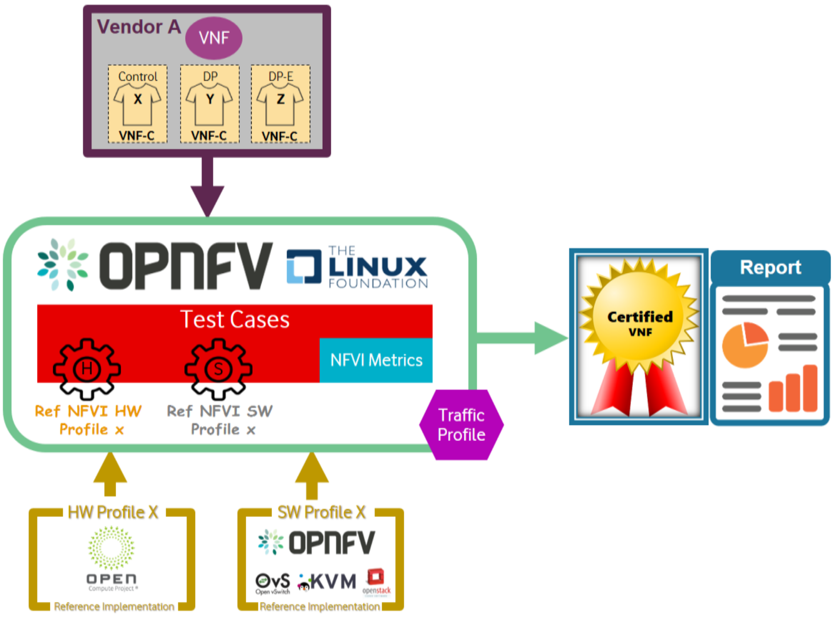
Finally, NFVI vendors can characterise, validate, and certify an entire NFVI platform (both SW & HW) against a given profile by using a VNF reference implementation as shown in □ below.



- : **Certifying vendor supplied NFVI (SW/HW) solutions**

6.4 VNF Compliance, Validation, and Certification

Standardising on Infrastructure profiles allows VNFs to be characterised, validated, and certified against a given profile by using reference NFVI implementations as demonstrated in □ below. Where VNFs are using multiple profiles (different VNF-C written against different profiles), multiple Reference NFVI implementations should be used.



- : **Certifying vendor supplied VNFs.**

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0		New PRD Baseline	GSMA TG	Rabi Abdel (Vodafone), Jamil Chawki (Orange)
2.0	25/03/2019	CR1002 is incorporated	Future Networks Programme	Rabi Abdel (Vodafone), Jamil Chawki (Orange)

Other information

Type	Description
Document Owner	GSMA Future Network Programme
Editor / Company	Rabi Abdel (Vodafone), Jamil Chawki (Orange)

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

7 Your comments or suggestions & questions