Technical Report

TR-411

Definition of interfaces between CloudCO Functional Modules

Issue: 1
Issue Date: April 2021

Notice

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER’S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

Issue History

Issue Number	Approval Date	Release Date	Issue Editor	Changes
1	2 April 2021	2 April 2021	Tim Carey, Nokia	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor	Tim Carey	Nokia
Work Area Director(s)	George Dobrowski	Morris Creek Consulting
	Bruno Cornaglia	Vodafone
Project Stream Leader(s):	Yves Hertoghs	VMWare
	Ning Zong	Huawei Technologies Co Ltd

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This Technical Report provides the requirements and interface specification needed for the management and control of virtual or physical network functions in the context of the CloudCO framework.

More specifically, the requirements and interfaces specified in this Technical Report are applicable to CloudCO elements located higher in the SDN architecture, i.e., CloudCO Domain Orchestrator and the SDN Management and Control elements.

This provides technical enablers for automation of the Management, Control and User Plane network functions that are deployed in a CloudCO infrastructure and allow for:

- Zero-touch automation of services.
- Use of existing functionality contained within existing elements.
- Migration of functionality into the CloudCO virtualization infrastructure.
- Capabilities that ease the interoperability and on boarding of multi-vendor virtual or physical functions.

These technical enablers are key to meeting the Operator's business goals of providing better agility for the creation, activation, monitoring, assurance and optimization of services while continuing to reduce the Total Cost of Ownership of the Operator's network.

1 Purpose and Scope

1.1 Purpose

This Technical Report specifies the interfaces associated with the CloudCO framework's reference points in order to achieve implementable, multi-vendor and interoperable deployments of the CloudCO framework. Specifically this includes:

1) A generic overview of the CloudCO framework specified in TR-384 [2]
2) Functional level definitions for the interfaces between CloudCO components, i.e., a fast guideline for functionalities exposed on these interfaces
3) Implementation level description of these interfaces, i.e., protocols, data models/data structures for modeling these interfaces

The purpose of this Technical Report is to provide specifications on 2) and 3) above as applicable to the SDN Management and Control element and the CloudCO Domain Orchestrator described in TR-384 [2].

1.2 Scope

This Technical Report provides the definitions of interfaces between CloudCO functional modules with the following information:

1) General definitions of the interfaces
2) Description of the protocols supported by these interfaces
3) Description of the data models supported by these interfaces

Additionally, as supportive information to define these interfaces, the Appendix I provides a table that maps these CloudCO interfaces with the CloudCO AppNotes (status of Application Notes could be found here.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [18].

MUST	This word, or the term "REQUIRED", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term "RECOMMENDED", means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

2.2.1 Published References

Document	Title	Source	Year
[1] TR-370 Issue 2	Fixed Access Network Sharing – Architecture and Nodal Requirements	BBF	2019
[2] TR-384	Cloud Central Office Reference Architectural Framework	BBF	2018
[3] TR-386	Fixed Access Network Sharing - Access Network Sharing Interfaces	BBF	2019
[4] TR-413	SDN Management and Control Interfaces for CloudCO Network Functions	BBF	2018
[5] TR-436	Access & Home O&M Automation/Intelligence	BBF	2021
[6] TR-459	Control and User Plane Separation for a disaggregated BNG	BBF	2020
[7] ETSI GS NFV-INF 005	Network Functions Virtualisation (NFV); Infrastructure; Network Domain	ETSI ISG NFV	2014
[8] ETSI GS NFV-MAN 001	Network Functions Virtualisation (NFV); Management and Orchestration	ETSI ISG NFV	2014

[9] ETSI GS NFV-INF 005	Network Functions Virtualisation (NFV); Infrastructure; Network Domain	ETSI ISG NFV	2014
[10] ETSI GS NFV-IFA 005 V2.1.1	Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification	ETSI ISG NFV	2016
[11] ETSI GS NFV-IFA 006 V2.1.1	Network Functions Virtualisation (NFV); Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification	ETSI ISG NFV	2016
[12] ETSI GS NFV-IFA 007 V2.1.1	Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification	ETSI ISG NFV	2016
[13] ETSI GS NFV-IFA 008 V2.1.1	Network Functions Virtualisation (NFV); Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification	ETSI ISG NFV	2016

[14] ETSI GS NFV-IFA 010 V3.2.1	Network Functions Virtualisation (NFV) Release 3;
	Management and Orchestration;
	Functional requirements specification
		ETSI ISG NFV	2019

[15] ETSI GS NFV-IFA 013 V3.4.1	Network Functions Virtualisation (NFV); Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification	ETSI ISG NFV	2020
[16] ETSI NFV-SOL 005 V2.7.1	Network Functions Virtualisation (NFV); Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point	ETSI ISG NFV	2020
[17] ETSI ZSM 002	Zero-touch network and Service Management (ZSM); Reference Architecture	ETSI ISG ZSM	2019
[18] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[19] RFC 5277	NETCONF Event Notifications	IETF	2008
[20] RFC 6020	YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF)	IETF	2010
[21] RFC 7950	The YANG 1.1 Data Modeling Language	IETF	2016
[22] RFC 8040	RESTCONF Protocol	IETF	2017
[23] RFC 8345	A YANG Data Model for Network Topologies	IETF	2018
[24] RFC 8772	The China Mobile, Huawei, and ZTE Broadband Network Gateway (BNG) Simple Control and User Plane Separation Protocol (S-CUSP)	IETF	2020
[25] TMF633	Service Catalog API User Guide	TMF	2021
[26] TMF638	Service Inventory API User Guide	TMF	2020
[27] TMF639	Resource Inventory API User Guide	TMF	2020
[28] TMF641	Service Ordering API User Guide	TMF	2020
[29] TMF645	Service Qualification API User Guide	TMF	2020
[30] TMF653	Service Test Management API User Guide	TMF	2020

2.2.2 Draft References

The reference documents listed in this section are applicable to this Technical Report but are currently under development within the respective body and are expected to be released in the future. Users of this Technical Report are advised to consult the source body for current status of the referenced documents or their successors.

Document	Title	Source	Year
[31] WT-413 Issue 2	SDN Management and Control Interfaces for CloudCO Network Functions	BBF	TBD

[32]	WT-454	YANG Modules for Network Map & Equipment Inventory	BBF	TBD

2.3 Definitions

The following terminology is used throughout this Technical Report.

CPE Customer Premises Equipment.

RESTCONF IETF HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastore concepts defined in the NETCONF.

VNF VNF is used to refer to a network function that is virtualized. In this Technical Report a VNF can be a virtualized function that resides within a virtual environment or in a containerized environment (CNF).

YANG A data modeling language using in the management of network resources.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

API	Application Programming Interface
AppNote	Application Note
BSS	Business Support System
BW	Bandwidth
CloudCO	Cloud Central Office
CNF	Container Network Function
CO	Central Office
CP	Control Plane
CRUD-N	Create, Retrieve, Update, Delete - Notify
DC	Data Center
DS	Downstream
E2E	End to End
ETSI	European Telecommunications Standards Institute
EUD	End-user Device
HVAC	Heating, Ventilation and Air Conditioning
HTTP	HyperText Transfer Protocol
InP	Infrastructure Provider
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
Lx	Layer x (x=1,2,3)
MANO	Management and Orchestration
MCO	Management and Control Orchestration
MP	Management Plane
MSBN	Multi Service Broadband Network
NETCONF	Network Configuration Protocol
NNI	Network to Network Interface
NFVI	Network Functions Virtualization Infrastructure
NFVO	Network Functions Virtualization Orchestrator

NS	Network Sharing
OAM	Operations, Administration and Management
OSS	Operational Support System
PDU	Protocol Data Unit
REST	Representational State Transfer
RFS	Resource Facing Service
SA	Service Assurance
SLA	Service Level Agreement
SDN	Software Defined Network
SDN M&C	SDN Management and Control
TR	Technical Report
UNI	User to Network Interface
UP	User Plane
US	Upstream
vAN	Virtual Access Node
VIM	Virtualization Infrastructure Manager
VLAN	Virtual Local Area Network
VNFM	Virtualised Network Function Manager
VNO	Virtual Network Operator
WT	Working Text
YAML	YAML Ain't Markup Language

3 Technical Report Impact

3.1 Energy Efficiency

This Technical Report may impact energy efficiency, as network functions can now be decoupled from existing standalone nodes. Use of generic hardware, as such not optimized for a specific network application, and migration of network functions to more distributed locations could lead to higher energy consumption. However, on-demand allocation of hardware resources and hardware sharing across multiple applications can produce energy gains. This Technical Report does not intend to quantify these opposite effects on energy efficiency.

Regulatory differences related to electrical power, Heating, Ventilation and Air Conditioning (HVAC) and fire protection between traditional COs and datacenters is out-of-scope for this Technical Report.

3.2 Security

Security provides "a form of protection where a separation is created between the assets and the threat." This Technical Report enables the sharing of a common infrastructure between various use cases that may be operated by different departments (e.g., wireline and mobile) or different companies (other service providers, including other network service providers). This Technical Report also provides an increased opportunity for Operators to dynamically control the network service behavior, with the use of interfaces specified within this Technical Report. In addition, it is expected that management and control plane interfaces specified are protected from security risks.

It is noted that existing threats, safeguards, and enhancements remain applicable to CloudCO deployments, whether in the forwarding or management-control planes. This specification assumes a foundation of current security best practices that have been defined for the existing Multi Service Broadband Network (MSBN). However, some new or amplified concerns also appear and without appropriate precautions, the above conditions could impact a network’s security.

3.3 Privacy

A multi-tenant CloudCO hosts functionality for a set of actors with potentially competing interests that the CloudCO will be required to isolate from each other. At the same time, it is required to enable business interactions between the same set of actors requiring careful design of the points of contact. A multi-tenant CloudCO is a system of sufficient complexity that it will expose new attack vectors to malicious parties that have access to the CloudCO system. For example, the “black box” steady state functionality of a virtualized system may be identical to a corresponding physical network function implementation, but the elasticity and dynamic behavior a virtualized system implies that significantly different system responses to load will be possible, which can be exploited for malicious purposes if poorly designed or executed. Privacy involves the need to ensure that information to, from and between customers can only be accessed by those who have the right to do so. Furthermore, privacy requirements can vary by regulatory region. In general, two ways to ensure privacy is recognized:

- Preventing data, from being copied to a non-intended destination.
- Encrypting data, so that it cannot be understood even if it is intercepted.

This Technical Report does not define any specific mechanisms.

4 Overview

The generic CloudCO framework described in TR-384 [2] provides a framework for the orchestration, management and control of physical and virtual network functions. This Technical Report further defines the framework providing a reference CloudCO architecture with defined functional domains and associated interfaces that provides:

- Well-defined separation for the domains (i.e., Access, Edge) that are comprised in a CloudCO infrastructure.
- A cleaner separation of the functions within the various layers of the SDN hierarchy. For example, the SDN Management and Control functions as described in the CloudCO Application Notes listed in Appendix I.

The domains, and the layers the SDN hierarchy with their associated interfaces are depicted in Figure 1.

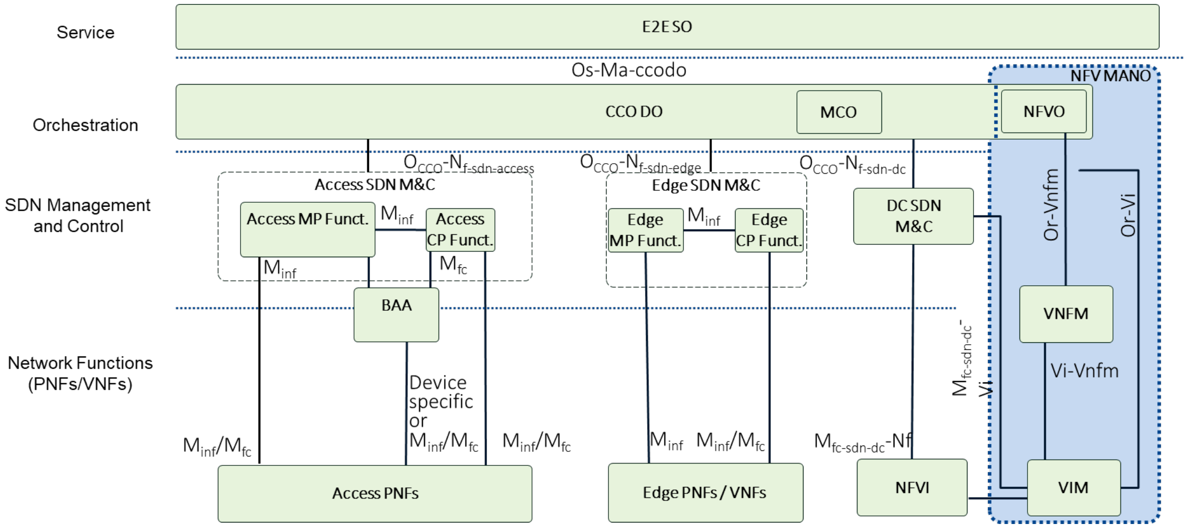

Figure 1 Reference Architecture for the CloudCO framework

The reference used in this Technical Report has the following considerations when defining the requirements, interfaces and information models:

- The M_{inf} reference point provides management plane FCAPS functionality and the associated interface protocol is typically based on NETCONF/YANG.
- The M_{fc} reference point provides flow control functionality (e.g., control plane disaggregation) and can utilize a number of control plane protocols and modelling for the various subfunctions of the reference point (e.g., configuration of the control plane, control of the user plane based on the control plane's state, redirection of control plane PDUs).
  For example:
  a. PFCP as described in TR-459 [6]
  b. NETCONF/YANG
  c. gRPC/gPB
  d. RFC 8772 [24]
  e. OpenFlow
- Management (MP) and Control Plane (CP) functions can be deployed in various ways.
  For example, the functions can be embedded within a SDN Management and Control application or they could be deployed as standalone functions or VNFs. This is applicable to all CloudCO domains.
- The MP and CP functions are shown in the SDN Management and Control layer. But vendor implementations and/or Operators migration strategies can choose to implement some of these functions in PNFs or VNFs.
- Within the Access domain, the User Plane (UP) functions are implemented in the physical network functions (PNF) and hence Access UP functions are not defined as VNFs.

The MP and CP functions refer to the overall management and control functionality that is provided by the specified domain:

- MP functions include device management and resource configuration management. Device management includes management of the physical resources (e.g., ports, cards, device, and related status); resource configuration management is about physical and virtual resources configuration.
- CP functions dynamically exchange and elaborate the Control Plane/User Plane PDUs that determine the forwarding path and forwarding behavior of traffic in the specified domain, through the configuration of the specified domain and the reported status information.

5 Support of multi-tenancy in CloudCO

The multi-tenant service capabilities in CloudCO permits Infrastructure Providers (InP) to offer portions of CloudCO PNF and VNF resources to Virtual Network Operators (VNO) or Enterprises known as Tenants. Typically, these resources are provided on the basis of a Service Level Agreement (SLA) between the InP and the Tenants and are realized within the CloudCO via network sharing techniques (see for example TR-370i2 [1]) or as a network slice where the Service Level Agreement between the InP and the Tenant is monitored through Key Performance Indicators (KPIs). The network sharing and slicing of the InP's network creates a set of virtual networks that is associated with the Tenants, who can then monitor their virtual network and request services from the InP that uses shared network resources or network slices of their virtual network.

5.1 Tenant types and multi-tenancy models

The focus of this section is to provide support for “multi-tenant services” where the Tenants such as VNOs maintain their own services. This is different from a “multi-tenant platform” in which multiple users or systems access the CloudCO system.

ETSI NFVI provides functional requirements for such multi-tenant services from a NFV perspective in ETSI GS NFV-IFA 010 [15] where the objective in the ETSI NFV architecture is to provide isolation between the infrastructure resources and/or isolation between the service resources allocated to different Tenants as shown in Figure 2.

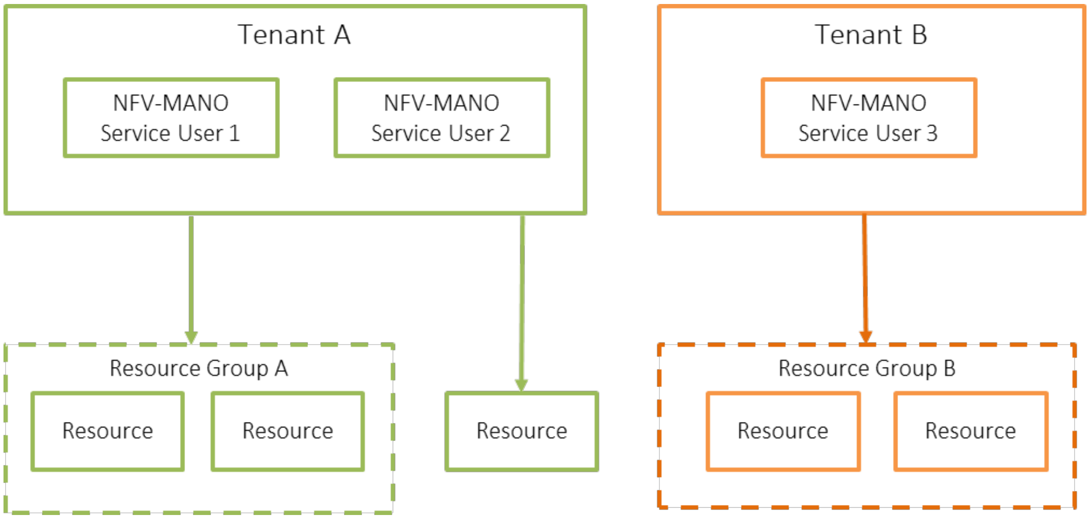

Figure 2 Multi-tenant services in ETSI NFV

Similar to ETSI multi-tenancy there is a need for CloudCO to support similar functional requirements taking into account the SDN Management and Control functions not related to the lifecycle management of VNFs. Following ETSI NFVs multi-tenancy principles following Tenant descriptions can be derived for CloudCO:

- A Tenant to which network resources are shared is referred to as an **Infrastructure Tenant**. For example, a Tenant is assigned specific CPU, memory resources that comprise the NFVI or a Tenant that can share network nodes (e.g., PNFs, VNFs), links or termination points. Infrastructure Tenants can then provide their own PNFs and VNF resources that on the shared infrastructure.
- A Tenant that which network resources are sliced is referred to as a **Virtual Service tenant**. Virtual Service tenants can request network slices via the InP or an Infrastructure Tenant.

Categorizing Tenant types is necessary for managing resource ownership. For example, consider an InP that uses a hybrid cloud infrastructure for providing virtual resources. In this example, different infrastructure owners (e.g., private/public clouds, Access/DC/Edge SDN M&C functions) virtual resources (e.g., link, nodes, CPU, memory) can be consumed by *Infrastructure Tenants* that use them to provide PNFs and VNFs. These VNFs and PNFs can be further consumed through network slicing by *Virtual Service Tenants*.

5.1.1 Multi-Tenancy Use Cases:

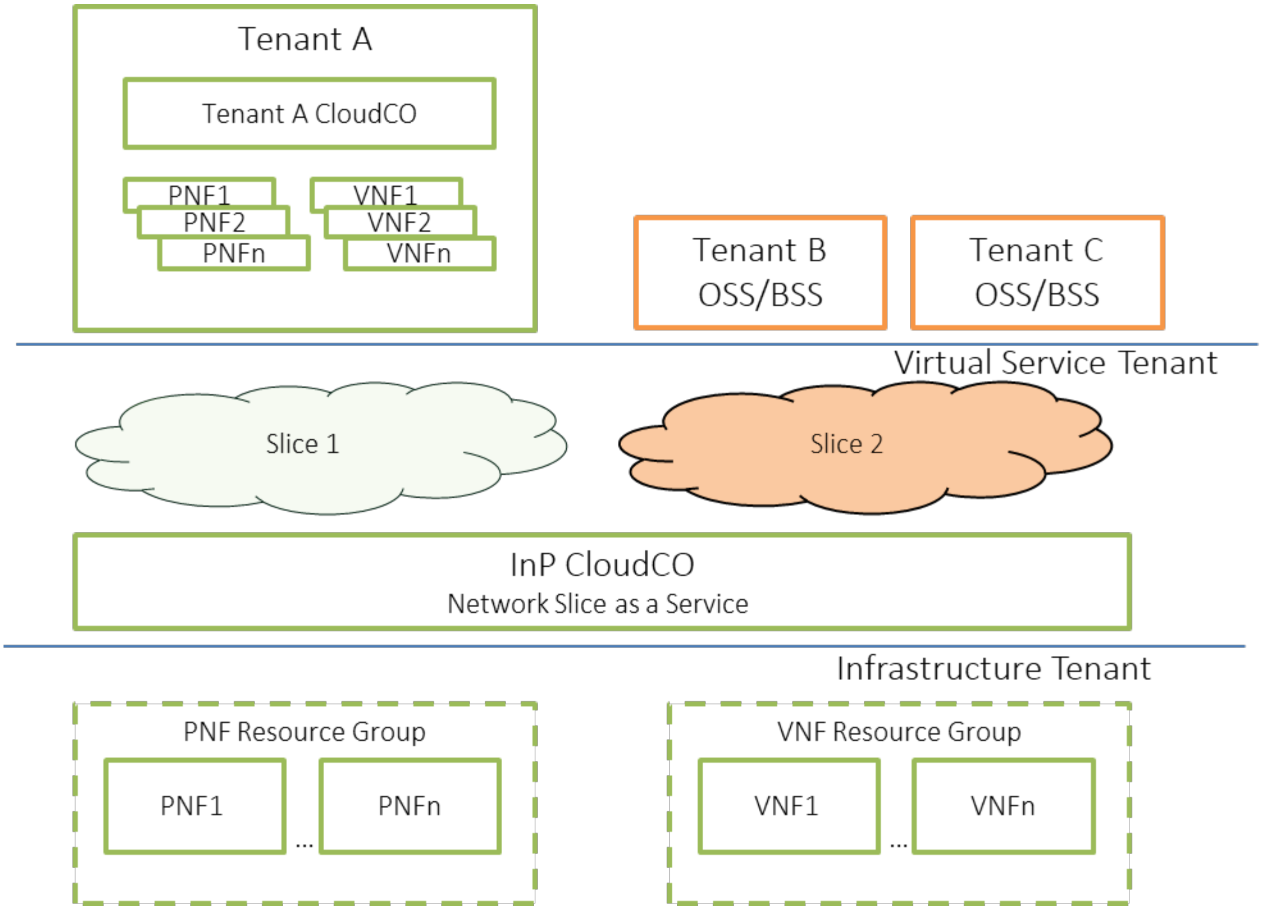

Figure 3 Multi-Tenancy use cases

Figure 3 shows two multi-tenancy use cases:

1) Virtual Service Tenants (Tenant B, C) sharing InP resources as service. Multiple tenants can use the same network slice, the CloudCO Domain Orchestration function ensures mapping, and isolation between the network slices.
2) Virtual service Tenants (Tenant A) using functions of their own CloudCO instance that uses resources allocated from same InP's CloudCO instance. Here the CloudCO Domain Orchestration function ensures granular service abstractions enabling recursive CloudCO deployment.

5.2 Mapping network slices and shared network resources to CloudCO resources

In the CloudCO architecture, the CloudCO Domain Orchestration function is responsible for accepting requests from the Tenant for slices of the InP's network and the sharing of the InP's network resources. Likewise, the CloudCO Domain Orchestration function is responsible for:

- Exposing the Tenant's network map and realized virtual network to the Tenant,

- Tenant, monitoring the overlay network slice or shared network resources using performance metrics for the network slice or shared network resources that spans the domains of the CloudCO.

While the CloudCO Domain Orchestration function provides the CloudCO aggregated view of the network slice and shared network resources, each CloudCO domain's SDN M&C functions is responsible for a subnetwork of the overall CloudCO network slice or shared network resources that is attributed to the domain. Additionally, the SDN M&C functions are responsible for mapping the realized subnetwork overlay of the network slice or shared network resource to the domain's PNF and VNF resources.

The SDN M&C's resource mapping function provides capabilities to realize the Network Slice and Network Sharing subnetwork requests from the CloudCO Domain Orchestration function by determining the PNF and VNF resources needed to fulfill the request. Any domain specific policies and constraints that pertain to the request are accounted for as part of this realization/mapping function. These policies can be defined as part of the request or as part of a set of policies and profiles defined by the InP that are be used for the type of request.

Figure 4 below depicts a scenario where the InP provides a set of policies and profiles for defining a Network Slice. The Tenant then requests Network Slices (a). These Network Slice requests are realized by the CloudCO Domain Orchestration function by orchestrating the request through the relevant CloudCO domain's SDN M&C functions. Each CloudCO domain's SDN M&C function involved uses the policies and profiles that are part of the request and part of the InP setup of the type of network to determine the PNF and VNF resource to be used to fulfill the request.
Using the Network Slice, the Tenant can request to monitor/modify the realized Network Slice connectivity using the realized overlay or underlay network (b) and/or the associated PNF and VNF resources (c). The CloudCO Domain Orchestration function exposes the domain specific Network Slice connectivity along with the parameters associated with the allocated PNF and VNF resources.

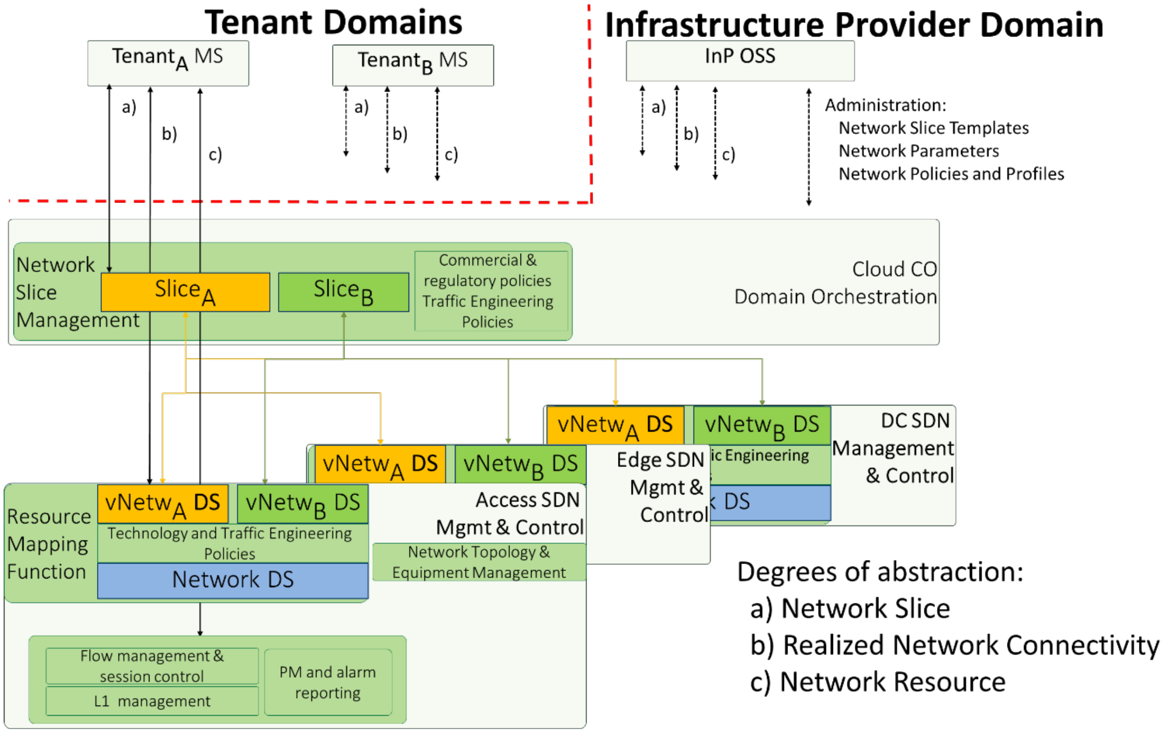
Tenant Domains
Infrastructure Provider Domain
Tenant_A MS
Tenant_B MS
InP OSS
a)
b)
c)
Administration:
Network Slice Templates
Network Parameters
Network Policies and Profiles
Network Slice Management
Slice_A
Slice_B
Commercial & regulatory policies
Traffic Engineering Policies
Cloud CO Domain Orchestration
vNetw_A DS
vNetw_B DS
DC SDN Management & Control
ic Engineering
DS
Edge SDN Mgmt & Control
Access SDN Mgmt & Control
Network Topology & Equipment Management
Resource Mapping Function
Technology and Traffic Engineering Policies
Network DS
Flow management & session control
L1 management
PM and alarm reporting
Degrees of abstraction:
a) Network Slice
b) Realized Network Connectivity
c) Network Resource

Figure 4 Resource Mapper and Slice Manager in the Cloud CO context

5.2.1 Offering CloudCO resources to Tenants

InP's determine which network resources (e.g., PNF, VNF, Termination points, Links) within the CloudCO can be offered to Tenants by allocating the resources to the Tenant's network map from the InP's network map as defined in WT-454 [32] that is exposed across the Os-Ma-ccodo reference point.

R1) The CloudCO Domain Orchestration function MUST provide the capability to expose CloudCO network resources specific to a Tenant through the Os-Ma-ccodo reference point. The network resources that MUST be supported are defined in Table 1 CloudCO Network Resource Creation & OAM.

R2) The CloudCO Domain Orchestration function MUST provide the capability for the InP to configure the CloudCO network resources that can be exposed to the Tenant through the Os-Ma-ccodo reference point.

R3) The CloudCO Domain Orchestration function MUST provide the capability to maintain Tenants.

5.2.2 Requesting network slices and shared network resources by Tenants

Using the resources identified in the Tenant's network map, Tenants then can request network slices or sharing of network resources. These network slices and shared network resources are associated with the Tenant and realized within the CloudCO.

R4) The CloudCO Domain Orchestration function MUST provide the capability for a Tenant to request a network slice through the Os-Ma-ccodo reference point.

R5) The CloudCO Domain Orchestration function MUST provide the capability for a Tenant to request shared network resources from a portion of the InP's network through the Os-Ma-ccodo reference point.

R6) A consumer of an Os-Ma-ccodo interface, which supports multi-tenancy, MUST provide the identification and type of an appropriate Tenant when performing an operation across the Os-Ma-ccodo interface.

5.2.3 Exposing virtual networks to Tenants

The realized network slices and shared network resources comprise the Tenant's virtual network which is exposed to the Tenant for monitoring.

R7) The CloudCO Domain Orchestration function MUST provide the capability for a Tenant to monitor the Tenant's realized network slices as a logical overlay through the Os-Ma-ccodo reference point.

R8) The CloudCO Domain Orchestration function MUST provide the capability for a Tenant to monitor the underlay connections that comprise the Tenant's realized network slices through the Os-Ma-ccodo reference point.

R9) The CloudCO Domain Orchestration function MUST provide the capability for a Tenant to monitor the network PNF and VNF resources used in the Tenant's realized network slices through the Os-Ma-ccodo reference point.

R10) The CloudCO Domain Orchestration function MUST provide the capability for a Tenant to access their shared network resources through the Os-Ma-ccodo reference point.

R11) The CloudCO Domain Orchestration, SDN M&C, VIM and VNFM functions MUST support the capability to isolate resources assigned to different Tenants.

R12) The CloudCO Domain Orchestration, SDN M&C, VIM and VNFM functions MUST support the capability to limit the scope of operations only to the virtual resources' groups (e.g., VNF/PNFs) assigned to the requesting Tenant.

6 Definitions of Reference Points

6.1 Definition of Os-Ma-ccodo

The Os-Ma-ccodo reference point exposes an abstracted view of the resources within the CloudCO Domain to E2E Service entities that consume the CloudCO Domain's resources in a Network- /Subscriber-as-a-Service paradigm.

6.1.1 CloudCO Domain Orchestration Function

The CloudCO Reference Architectural Framework described in TR-384 [2] is a combination of a SDN and NFV architecture applied over a hybrid physical and NFV infrastructure (NFVI). The NFV components are used to orchestrate and manage the virtual functions and their supporting infrastructure. While the SDN portion is used orchestrate and manage the MP, CP and UP functions and control user plane interactions among the PNFs, the VNFs and the switch fabric. Additionally, the SDN portion controls redirecting of certain in-band control packets to the relevant SDN controller applications.
In order to build service segments, including forwarding across the NFVI, as well as configuring and setting up connectivity to PNFs and VNFs (onboarded on the NFVI), all these resources have to be orchestrated together. This is the role of the CloudCO Domain Orchestration function.

The CloudCO Domain Orchestration function performs this role by operating or orchestrating the resources of the CloudCO Domain across domains (e.g., Access, Edge, NFV infrastructure) through the functionality defined by the MCO Engine and the NFVO function.

6.1.1.1 Management Control Orchestration (MCO) Engine Functionality

The MCO Engine within the CloudCO Domain Orchestration function oversees all tasks related to exploiting the CloudCO Domain as a network assets that include:

- CloudCO State Control & Optimization Function, which includes a closed-loop control and optimization of the state of CloudCO resources, on a time-continuous basis.
- An aggregated high-level orchestration of similar functionalities exercised in turn by the specific SDN Management and Control and relevant MANO functions. For example: Fault, Configuration, Accounting, Performance and Security capabilities and derived Service Assurance (SA) logic and algorithms.

The following list expresses the set of functions performed by the MCO Engine:

- Provides the interfaces for Os-Ma-ccodo reference point by acting as the interaction module between the CloudCO Domain and service level systems (e.g., E2E Service entities, OSS, BSS).
- Exposes an abstract view of the infrastructure network map and inventory of related status for physical and virtual resources that represent the CloudCO Domain.
  Examples of exposed information related to the CloudCO Domain status are the full configuration and Tenant ownership of the instantiated resources or their current availability for consumption from E2E Service entities, as well as any notification of resource alarms status or resource out of order maintenance conditions.
- Orchestrates the SDN hierarchy domains (e.g., Edge, Access) enabling real time dynamics and advanced network automation of resources (i.e., PNF, VNFs, DC Networking I/O resources) that collectively realize the CloudCO Domain. This includes the exposure of the instantiated resource facing services.
- Orchestrates the tasks of the SDN Management and Control functions related to PNFs, VNFs and DC Networking I/O resources.
- Provides a Data Collection Function (MCO-DCF) related to monitoring and surveillance of network performance parameters and other data related to the CloudCO Domain resources. The data

provided by the MCO-DCF is needed to diagnose, troubleshoot and monitor the CloudCO Domain resources and is used for enabling feedback responses within the CloudCO Domain. The MCO-DCF can be reused by other CloudCO components.

In order to achieve the above, the MCO Engine includes the following requirements:

R13) The CloudCO Domain Orchestration's MCO Engine MUST provide a Service Building Framework, where service developers can use ‘building-block’ services to create their own aggregate services, along with an API to consume them. Aggregate services can be used to create yet other aggregated services. Building-block services can be single-tenant or can be an instance of a multi-tenant application.

R14) The CloudCO Domain Orchestration's MCO Engine MUST provide interactions with the NFVO via an orchestration reference point internal to CloudCO Domain Orchestration Function.

R15) The CloudCO Domain Orchestration's MCO Engine MUST provide the infrastructure network map and inventory of Nodes and Termination Points that comprise the CloudCO domain.

R16) The CloudCO Domain Orchestration's MCO Engine MUST provide FCAPS management of the CloudCO Domain's resources (e.g., VNF, PNF, NFV Infrastructure) as depicted Figure 13 of TR-384 [2].

R17) The CloudCO Domain Orchestration's MCO Engine MUST provide a State Control and Optimization function as depicted Figure 13 of TR-384 [2] featuring closed loop tracking and optimization of the CloudCO resources. Given the current internal status of the CloudCO Domain and the pending requests from the E2E Service entities, such as for addition/release/reconfiguration of available resources, this function computes and guides the transition to a new stable and resilient state of the CloudCO Domain. This new state is then reached via actuation of a proper set of MCO Engine commands at the SBI towards the SDN Management and Control elements, potentially preceded by an NFVI scale in/out action, requested by the MCO Engine to the NFVO.

6.1.1.2 NFV Orchestrator (NFVO) Function

In the CloudCO Domain Orchestration function incorporates NFVO functionality that includes the following primary responsibilities:

- The orchestration of NFVI resources across multiple VIMs.
- The lifecycle management of Network Services.

The complete list of responsibilities for the NFVO function can be found section 5.4 of ETSI GS NFV-MAN 001[8].

R18) The CloudCO Domain Orchestration's NFVO MUST provide the capabilities of the NFVO functionality as described in section 5.4 of ETSI GS NFV-MAN 001[8].

6.1.2 CloudCO Domain Orchestration Os-Ma-ccodo Interface

The CloudCO Domain Orchestration function is responsible for provisioning, monitoring and maintenance, security and flow control for the CloudCO Domain resources used in a Network- /Subscriber-as-a-Service paradigm.

The information elements along with the associated data model and operations for the services and network function resources that are exposed through the O_s-Ma_{-ccodo} interface are described in Table 1 and .

R19) The CloudCO Domain Orchestration Function MUST support information elements defined in Table 1 exposed by the Os-Ma-ccodo interface.

R20) The CloudCO Domain Orchestration Function MUST support information elements defined in by the Os-Ma-ccodo interface.

6.1.2.1 Exposure of the NFVO Functionality

As the CloudCO Domain Orchestration function contains a Network Function Virtualization Orchestrator (NFVO) functionality, the Os-Ma-Nfvo reference point can be exposed directly to E2E Service entities via the Os-Ma-ccodo reference point and includes:

- Management of Network Service Descriptors and VNF packages
- Lifecycle management of Network Services and VNFs
- Policy management and/or enforcement of those resources and the NFVI in general

Alternatively, the Os-Ma-Nfvo reference point can be embedded inside the CloudCO Domain Orchestration function, between the NFVO and the Management Control Orchestration (MCO) Engine and the MCO Engine would expose the NFVO functionality to the E2E Service entities.

R21) The CloudCO Domain Orchestration Function MUST provide the capability of directly exposing the CloudCO Domain Orchestration NFVO capabilities defined by the Os-Ma-Nfvo reference point across the Os-Ma-ccodo reference point as specified in ETSI NFV SOL 005 [16] including fault and performance management.

R22) The CloudCO Domain Orchestration Function MUST provide the capability of exposing the CloudCO Domain Orchestration NFVO capabilities provided via the MCO Engine functionality across the Os-Ma-ccodo reference point.

6.1.2.2 Protocol Requirements

The programmability and automation of the capabilities provided by the CloudCO Domain Orchestration function along with the types of resources (e.g., network slices, closed loop policies) and the associated scope (e.g., Tenant slice) used in Network- /Subscriber-as-a-Service paradigms require that the interfaces exposed toward E2E Service entities be flexible and utilize REST-like APIs based on well-established Internet transport protocols like HTTP and information definition languages like YAML or JSON.

Likewise, the protocol needs to allow each client to be configurable independently, with at least security attributes, tailored information model including SLA, gatekeeper policy to protect the server from client misbehavior, and other attributes necessary as appropriate.

Using well established and flexible protocols permits resources to be managed and controlled by tailoring different functional scopes, exposing target Tenant(s), features and degrees of abstraction like:

- High-level abstraction for (sub-)network slice/network service creation by a Tenant; this type of interface is typically application specific.
- (*if required by the* Network- /Subscriber-as-a-Service paradigms*)* intermediate abstraction for (sub-)network slice/network service parameters definition and configuration within a Tenant's slice.
- *(if required by the Network- /Subscriber-as-a-Service paradigms)* lower layer abstraction for fine grained Tenant's control of specific parameters within its own slice/resources for those deployments that require such deep access; this type of interface largely relies on TR-413 [4].

The following requirements guide protocol selection for the Os-Ma-ccodo reference point exposed by the CloudCO Domain Orchestration Function to E2E Service entities.

R23) The Os-Ma-ccodo reference point MUST be based on YAML/JSON models and grammars that exposes the CloudCO network resources and services via primitive service elements.

R24) The Os-Ma-ccodo reference point MUST be an HTTP REST-like interface.

R25) The Os-Ma-ccodo reference point's service elements API MUST be consumed via Create, Read, Update, Delete (CRUD) actions issued by E2E Service entities.

R26) The Os-Ma-ccodo reference point MUST allow each E2E service entity to be configurable independently, with at least security attributes, tailored information model including SLA, gatekeeper policy to protect the server from client misbehavior, and other attributes necessary as appropriate.

R27) Certain CloudCO network resources and services MUST proactively interact with northbound elements via Notify (N) actions to initiate or feed workflows by means of network generated information (e.g., status changes, threshold crossings, alarms, end user device Serial Number).

R28) The Os-Ma-ccodo reference point MUST allow programmability to expose a selection of those service elements. This programmability MUST go even deeper to a subset of variables or, in specific cases, to one single variable.

6.1.2.2.1 Support for TM Forum APIs across the Os-Ma-ccodo

The TM Forum has published API specifications that can be used for interactions between the CloudCO Domain Orchestration Function and E2E Service entities. These APIs can be used for:

- Service Inventory: TMF638 [26] offers E2E Service entities a standard means of query, updating and receiving notifications from the CCO DO's Service Inventory including to service state recorded in the catalogue.
- Resource Inventory: TMF639 [27] offers E2E Service entities a standard means of query, updating and receiving notifications from the CCO DO's Resource Inventory.
- Service Catalog Retrieval: TMF633 [25] offers the E2E Service entities a standard means of querying the CCO DO's run-time Service Catalogue to determine the service types available within the CCO domain. In addition, TM633 offers a complete set of CRUD-N capabilities to lifecycle manage the content of the CCO DO run-time Service Catalogue.
- Service Availability: TMF645 [29] offers the E2E Service entities a standard means of validating whether specific service characteristics can be offered at a geographic location.
- Service Fulfillment: TMF641 [28] offers the E2E Service entities a standard means of ordering services from the CCO DO, enabling the Network- /Subscriber-as-a-Service paradigms. Notifications of changes to the order item(s) state and service instance are also offered. Error handling notifications are exposed northbound to the E2E Service entities. When used, TMF641 exposes the NFVO functionality toward the E2E Service entities.
- Service Test: TMF653 [30] offers the E2E Service entities standard means of requesting and managing Service Tests for service orchestrated by the CCO DO (e.g., a temporary vProbe on NFVI).

R29) When integrating the CloudCO Domain Orchestration Function using TMForum APIs, the CloudCO Domain Orchestration Function MUST provide the capability to support the TMF633 [25] Service Catalogue Management API REST Specification across the Os-Ma-ccodo reference point.

R30) When integrating the CloudCO Domain Orchestration Function using TMForum APIs, the CloudCO Domain Orchestration Function MUST provide the capability to support the TMF638 [26] Service Inventory Management API REST Specification across the Os-Ma-ccodo reference point.

R31) When integrating the CloudCO Domain Orchestration Function using TMForum APIs, the CloudCO Domain Orchestration Function MUST provide the capability to support the TMF639 [27] Resource Inventory Management API REST Specification across the Os-Ma-ccodo reference point.

R32) When integrating the CloudCO Domain Orchestration Function using TMForum APIs, the CloudCO Domain Orchestration Function MUST provide the capability to support the TMF641 [28] Service Ordering Management API REST Specification across the Os-Ma-ccodo reference point.

R33) When integrating the CloudCO Domain Orchestration Function using TMForum APIs, the CloudCO Domain Orchestration Function MUST provide the capability to support the TMF645 [29] Service Qualification API REST Specification across the Os-Ma-ccodo reference point.

R34) When integrating the CloudCO Domain Orchestration Function using TMForum APIs, the CloudCO Domain Orchestration Function MUST provide the capability to support the TMF653 [30] Service Test Management API REST Specification Os-Ma-ccodo reference point.

6.1.2.2.2 Support for the Administrative Interface

R35) The CloudCO Domain Orchestration Function MUST provide a client interface to administer the CloudCO Domain environment.

6.1.2.2.3 Network Resources and Service Information Elements

Table 1 and describes a subset of the information elements, operations and data models exposed by the Os-Ma-ccodo reference point.

Table 1 CloudCO Network Resource Creation & OAM

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor[1] (Informative)	Notes/description
Access Network Map	AN-list, AN (next sub-information element)	R	WT-454: Network Map	VNO SP-tenant	
Access Node (AN)	AN-geo-location, Access-netw-termination-point AN-status	R	WT-454: Network Map	VNO SP-tenant	
	AN-NNI-port-info AN-UNI-port-info	R		VNO SP-tenant	Only for the AN resources the actor (partly) controls.
	EUD-Serial-Number	R		VNO SP-tenant	Only for the EUDs the actor controls, e.g., for feeding a VNO/SP-tenant authentication workflow based on the S/N

[1] This column suggests which actor consuming the CloudCO asset typically uses the attributes of the interface described in the corresponding row of the table. For example, with respect to the VNOs, described previously, the concept of SP-Tenants is introduced to designate a more generic consumer of the CCO NaaS portfolio.

SP-tenants could be:

- service departments (Consumer, Business, Enterprise, Mobile) of the same organisation of the CCO-provider
- providers of vertical services
- residential, business, enterprise end-users typically exposed to specific knobs or group of knobs to tailor their service offers on demand

Table 2 CloudCO Network Service Creation & Assurance

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
L2 Access Connectivity	NNI-OVLAN-prof # of O-VLANs Per VLAN: DS-guarant-BW DS-peak-BW US-guarant-BW US-peak-BW priority id	CRUD		VNO, SP-tenant	***O-VLAN is taken for the FANS framework.*** ***O-VLAN ids may be assigned by the CCO-provider***
L2 Access Connectivity	NNI-SVLAN-prof # of S-VLANs Per VLAN: DS-guarant-BW DS-peak-BW US-guarant-BW US-peak-BW priority id	CRUD		VNO, SP-tenant	*S-VLAN ids may be assigned by the CCO-provider*
L2 Access Connectivity	NNI-CVLAN-prof # of C-VLANs Per VLAN: DS-guarant-BW DS-peak-BW US-guarant-BW US-peak-BW priority id	CRUD		VNO, SP-tenant	
L2 Access Connectivity	UNI-CVLAN-prof # of C-VLANs Per VLAN: DS-guarant-BW DS-peak-BW US-guarant-BW US-peak-BW priority id	CRUD		VNO, SP-tenant	
NS Fault Monitoring	L2 alarm reporting	CRUD and N	ETSI NFV-SOL 005 FM interface and data model	VNO, SP-tenant	

NS Performance Monitoring	L2 PM commands	CRUD and N	ETSI NFV-SOL 005 FM interface and data model	VNO, SP-tenant	

6.2 Definition of Occo-Nf-sdn-access/ Occo-Nf-sdn-edge/ Occo-Nf-sdn-dc

The SDN Management and Control functions of the CloudCO provide management and control capabilities for the various domain segments associated with the Central Office. These domain segments include the Access and Edge network segments. In addition, the management and control of the service function chain(s) necessary to provide connectivity through the CloudCO NFVI is specified in the Occ-NF-sdn-dc interface.

6.2.1 Domain based SDN Management and Control

The interfaces associated with the domains are service based interfaces that provide management of a network segment. For management purposes, these network segments are treated as resource facing services (RFS) for subnetworks within the CloudCO. The CloudCO subnetworks can have resources that have been pre-allocated to Tenants as described in section 5 of this Technical Report or subnetworks that comprise the InP's resources which are known as Network Slices. Additionally, the CloudCO subnetworks can host subscriber RFS as connectivity services that can utilize Network Slices and FANS resources as described in section 6.2.1.4.1.2.

6.2.1.1 Management Capabilities of an RFS

The management capabilities needed for RFS are categorized by the following capabilities of a service and associated resources by the domain's Network Functions including the domain's Control Loops:

- Topology and Inventory of the Domain
    - Inventory of the RFS Intents
    - Inventory of Network Functions (Physical and Virtual)
    - Domain Topology with Connectivity Links
- Controlling the Domain
    - RFS Intent Fulfillment
    - RFS Intent Check
    - RFS Intent Realization
    - Network Function Configuration
- Monitoring the Domain
    - RFS Intent Performance and Events
    - Performance Measurements for RFS Intents
    - Network Function Fault, Security and Performance Events
    - Performance Measurements for Network Functions
- Troubleshooting the Domain
    - RFS Intent Condition Detection
    - Network Function Tests
    - Network Function Condition Detection

6.2.1.1.1 Monitoring and Troubleshooting the Performance of the Domain

The capabilities that are exposed for the management and control used in monitoring and troubleshooting the performance of an RFS Intents and the Network Functions of the Domain is specified in TR-436 [5]. This includes capabilities for Data Collection, Data Streaming and Analytic Services as well as the Test and Condition Detection services.

6.2.1.1.2 Management of the Network Function

The capabilities and information elements that are exposed for the management and control of Network Functions by the Network Function's M_{inf}/M_{fc} interfaces are specified in TR-413 [4] and WT-413 Issue 2 [31]. This includes information models for the specific Network Function configuration, tests, performance measurements, fault, security and performance events.

6.2.1.2 Intent Based RFS

The RFS instances are exposed as service-based intents utilizing policies and profiles that express the expectation of the service for a targeted subnetwork. Minimally the service intent contains information related to the type of service and the service level information needed to fulfill, monitor and maintain the service intent. The service fulfillment and monitoring are specific to the type of service and is described using policies or profiles. The RFS Intent is then realized using the FCAPS management and Flow Control functionalities of targeted NFs in the affected network domain or other RFS Intents if the collection of resources can be expressed as an intent. Figure 5 depicts the information model of a generic RFS Intent:

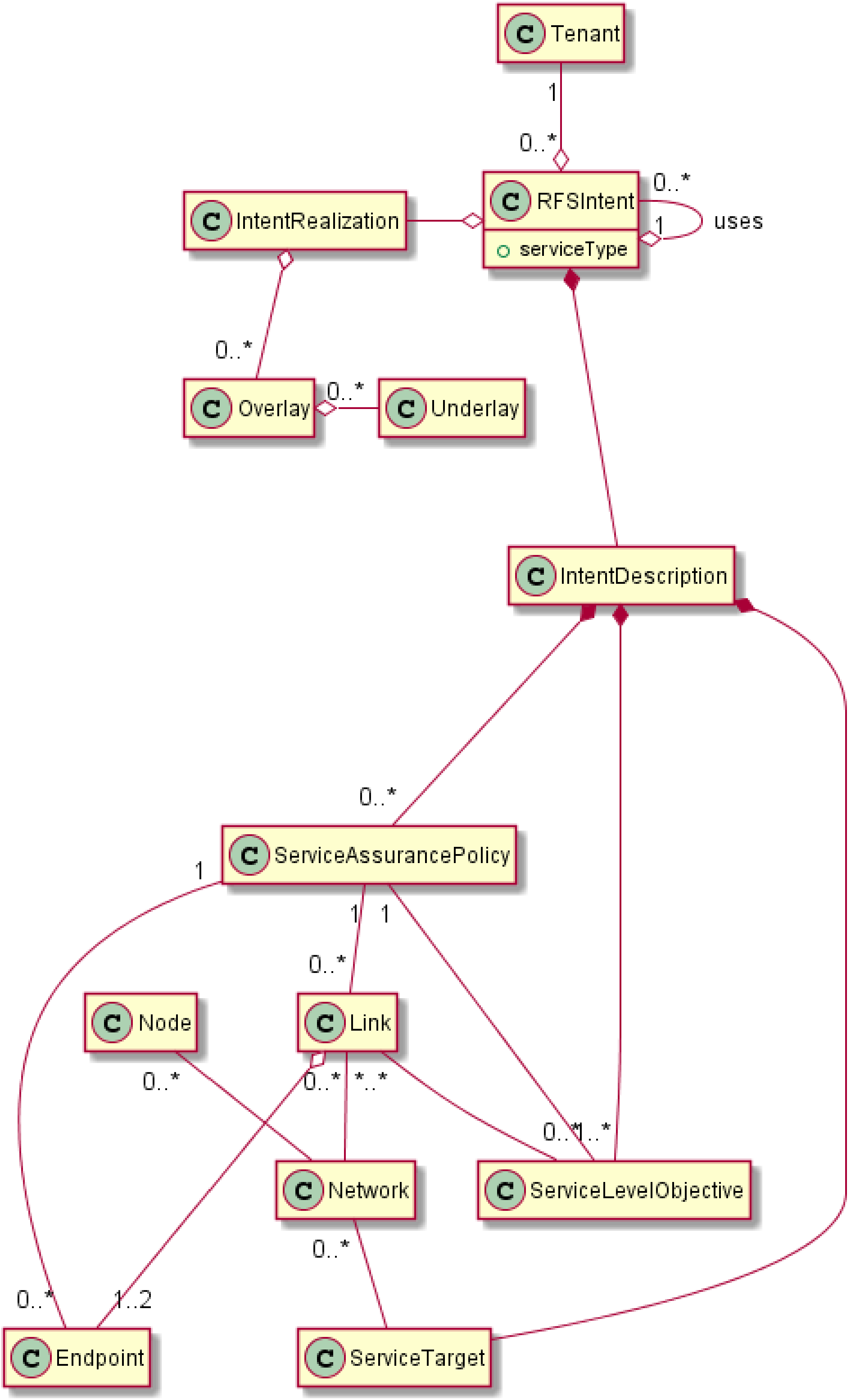

Figure 5 RFS Intent Information Model

In Figure 5 the RFS Intent is described using an IntentDescription and the realization of the RFS Intent is described using the IntentRealization. The IntentDescription contains policies for the fulfillment (ServiceLevelObjective) and assurance (ServiceAssurancePolicy) of the intent. These elements are applied to the target (ServiceTarget) of the RFS Intent. Specifically, Endpoints, Links and ServiceLevelObjectives are associated with a ServiceAssurancePolicy in order to provide the appropriate monitoring of the policy. RFS Intents can use other RFS Intents in order to fulfill the objective of the RFS Intent.

RFS Intents whose goal is to deploy Network Slices within a CloudCO subnetwork should use YANG modules based on the IETF RFC8345 [23] to fulfil the Intent.

R36) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface SHOULD provide the capability to fulfill Network Slice intents using YANG modules based on the IETF Network YANG module as specified by RFC8345 [23].

6.2.1.2.1 RFS Intent Topology and Inventory

The RFS Intent requires an abstract topology of nodes, connectivity links and associated endpoints for the domain. This topology is used by the RFS Intent to identify the underlying subnetworks connectivity points (management, control, user plane) that the RFS Intent uses when realizing the RFS Intent based on its objectives for fulfillment, monitoring and maintaining the service. Likewise, the topology for the RFS Intent is integrated with the domain specific connectivity resource information models that have been realized as part of the RFS Intent fulfillment.

For CloudCO domains, the abstract network topology model defined in IETF RFC8345 [23] can provide the topology that can be used to depict the overlay connectivity that was realized with the RFS Intent. Domain specific topology models that depict the underlay connectivity link with the overlay topology model by augmenting relevant resources (e.g., Termination Points, Links, Nodes).

R37) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to expose the overlay connectivity that was realized for the RFS Intent for the domain (i.e., Access, Edge) as specified by RFC8345 [23].

In order to be useful to the RFS Intent Fulfillment, the CloudCO domain provides an inventory of resources that can be used when specifying the objectives of the RFS Intent. Specifically, the topology of the existing network for a domain and, if shared with the Tenant, is depicted using the topology model defined in IETF RFC8345 [23].

R38) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to expose the inventory of Nodes, Links and Termination Points in the domain (i.e., Access, Edge) as specified by RFC8345 [23].

R39) When network resources have been pre-allocated to a Tenant, the O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to restrict the exposure of the inventory of Nodes, Links and Termination Points in the domain (i.e., Access, Edge) to the resources pre-allocated to the Tenant.

6.2.1.2.2 RFS Intent Control

RFS Intents are controlled through provisioning the RFS Intent. When created, the RFS Intent is checked to ensure the domain can fulfill the RFS Intent. If so, the RFS Intent is then realized in the domain.

R40) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to provision a RFS Intent.

R41) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to automatically validate a RFS Intent prior to realization of the RFS Intent.

R42) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to manually realize a RFS Intent.

R43) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to automatically realize a RFS Intent.

6.2.1.2.3 RFS Intent Monitoring

RFS Intents are an expression of the end-goal (objective) of a Resource Facing Service. Once a RFS Intent is realized, the corresponding RFSs are monitored in order to determine their health. Information about the health (e.g., performance Key Performance Indicators (KPI)s defined during the RFS Intent creation, RFS Health event reporting) of the RFS intent is provided through the O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface. Performance metrics includes the data that the SDN Management and Control function uses to determine if the KPIs defined by the RFS are met and include information about the usage and quality of the RFS Intent as it is realized in the domain.

R44) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability retrieve the performance metrics of a RFS Intent.

R45) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability report events associated with a RFS Intent.

6.2.1.2.4 RFS Intent Troubleshooting

RFS Intents provide information associated with the RFS Intent that can be used in Analytic services as specified.

R46) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability permit subscriptions to the RFS Intent's conditions.

R47) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability report detected conditions for a RFS Intent.

6.2.1.3 Intent Based Network Sharing

Shared network resources are exposed as intents utilizing policies and profiles that express the expectation of the equipment share for a targeted shared resource(s). Minimally the sharing intent contains information related to the sharing objective information needed to fulfill the sharing intent. The sharing fulfillment is specific to the type of sharing and is described using policies or profiles. These sharing-based intents are known as Network Sharing (NS) intents in this Technical Report. The NS Intent is then realized using the FCAPS and Flow Control management of targeted NFs in the affected domain's network segment or other NS Intents if the collection of resources can be expressed as an intent. For example, the sharing of Access network resources realized by the NS intents are described in TR-370 [1]. The following depicts the information model of a generic NS Intent:

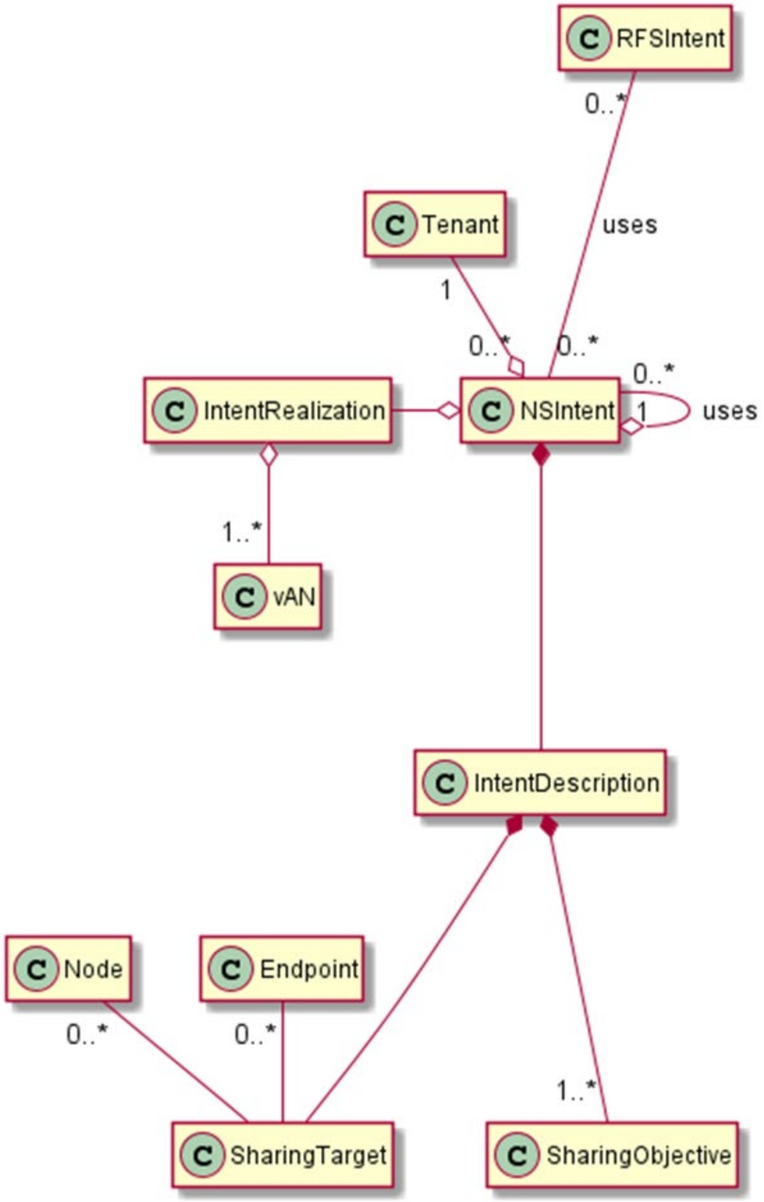

Figure 6 Network Sharing Intent Information Model

In Figure 6 the NS Intent is described using an IntentDescription and the realization of the NS Intent is described using the IntentRealization. The IntentDescription contains policies for the fulfillment of the sharing intent that are applied to the target of the NS Intent. NS Intents can use other NS Intents in order to fulfill the objective of the NS Intent. There is also an association that permits NS Intents to be used by RFS Intents as part of the RFS Intent fulfillment.

6.2.1.3.1 NS Intent Inventory

The NS Intent requires a list of nodes and associated endpoints for the domain. This topology is used by the NS Intent to identify the shared resources that the NS Intent uses when realizing the NS Intent based on its objectives for fulfillment, monitoring and maintaining the service. Likewise, the inventory for the NS Intent is integrated with the domain specific equipment resource information models that have been realized as part of the NS Intent fulfillment.

In order to be useful to the NS Intent Fulfillment, the CloudCO domain provides an inventory of resources that can be used when specifying the objectives of the RFS Intent. Specifically, the inventory of the existing network for a domain and, if shared the Tenant, is depicted using the Network Map model defined in WT-454 [32].

R48) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to expose the inventory of Nodes and Termination Points in the domain (i.e., Access, Edge) as specified by the Network Map in WT-454 [32].

6.2.1.3.2 NS Intent Control

NS Intents are controlled through provisioning the NS Intent. When created, the NS Intent is checked to ensure the domain can meet the objective of the NS Intent. If the domain can meet the objective of the NS Intent, the NS Intent is then realized in the domain.

R49) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to provision an NS Intent.

R50) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to automatically validate an NS Intent prior to realization of the NS Intent.

R51) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to manually realize an NS Intent.

R52) The O_{cco}-$N_{f\text{-}sdn\text{-}x}$ interface MUST provide the capability to automatically realize an NS Intent.

6.2.1.4 Access SDN Management and Control Function

The Access SDN Management and Control function is responsible for provisioning, monitoring and maintenance, security and flow control for the RFS Intents and associated PNF and VNF resources within the Access network segment of the CloudCO.

The information elements along with the associated data model and operations for the network function resources that are exposed through the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface are described in Table 3 Access Network Resource Creation & OAM.

R53) The Access SDN Management and Control function MUST support the exposure of the information elements defined in Table 3 Access Network Resource Creation & OAM through the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface.

The information elements along with the associated data model and operations for the RFS Intents associated within the Access network segment are defined in .

R54) The Access SDN Management and Control function MUST support RFS Intents defined in the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface.

6.2.1.4.1 Access SDN Management and Control $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ Interface

The $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface is the northbound interface of the Access SDN Management and Control function. This section describes the information elements exposed by the interface as well as the requirements for the protocol that conveys the requests, responses and notifications associated with the information elements in Table 3 Access Network Resource Creation & OAM and .

6.2.1.4.1.1Protocol Requirements

The information elements that exposed by the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface is conveyed using the RESTCONF Protocol defined in RFC 8040 [22]. The information elements conveyed by the RESTCONF protocol is encoded in the YANG data modeling language defined in RFC 7950 [21].

R55) The information elements and services for resources and RFS Intents conveyed over the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface MUST represented using the YANG data modeling language defined in RFC 7950 [21].

R56) The $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface MUST support the RESTCONF protocol defined in RFC 8040 [22].

Requests received via the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface uses the capabilities of the RESTCONF protocol and YANG data model specifications that permit the request to scope the request to specific targets (e.g., network function) and information element or sub-information element.

R57) The $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface MUST provide the capability to scope requests received across the interface to:

1) Specific targets for RFS Intents and Network Functions
2) Sets of Information elements and Sub-information elements defined in Table 3 Access Network Resource Creation & OAM and .

Notifications produced by the $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface uses the Subscription capabilities of the RESTCONF protocol.

R58) The $O_{cco}\text{-}N_{f\text{-}sdn\text{-}access}$ interface MUST provide the capability for management systems to subscribe to be notified of events (e.g., status change, threshold crossing, alarms, notifications) associated with RFS Intents and resources exposed by Network Functions using the subscription capability defined in RFC 8040 [22] with the transport and encoding protocols appropriate for the type of event.

R59) The O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface MUST provide the capability for management systems to subscribe to be notified of performance monitoring data to be reported that is associated with RFS Intents and resources exposed by Network Functions using the subscription capability defined in RFC 8040 [22] with the transport and encoding protocols appropriate for the type of event.

R60) The O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface SHOULD provide the capability to extend the event streams <access> information element defined in section 6.2 of RFC 8040 [22] to include Kafka transports. The <encoding> element value for a Kafka transport stream MUST be either "xml+kafka" or "json+kafka". When the <encoding> element is “xml+kafka” or “json+kafka”, the <location> element value MUST be of the format “kafka://ip1:port1[,ip2:port2..ipN:portN]/<topic-name>”.

Once subscribed, notifications and performance monitoring data that are transmitted across the O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface uses various technologies (e.g., RESTCONF, HTTPS, Kafka) to transport the notification to the subscribed entity.

R61) The O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface MUST provide the capability to notify entities that have subscribed for notifications.

R62) The O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface MUST provide the capability to notify entities that have subscribed for reporting of performance monitoring data.

The information elements that are exposed across this interface require control to ensure access to the information elements and RFS Intents are not exposed to unauthorized agents. The capability to restrict the information element and associated operations has to be programmable such that individual attributes of information elements associated with instances of resources for Network Functions or RFS Intents can be selected to be exposed to a user of the O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface.

Likewise, any information elements exposed through the O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface is required be exposed to only authorized management systems. This is necessary to ensure direct access to the SDN Management and Control function by VNO/SP-tenants is not permitted as these users are required to access the CloudCO resources through the CloudCO Os-Ma-ccodo interface.

R63) The O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface MUST provide the capability to ensure access to the information elements and RFS Intents are not exposed to unauthorized agents. The capability to restrict the information element and associated operations MUST be programmable such that individual attributes of information elements associated with instances of resources for Network Functions or RFS Intents can be selected to be exposed to a user of the O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface.

R64) The O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface MUST restrict access to the SDN Management and Control function to authorized users.

Note: Requirement R63) permits the scope of information elements to be restricted to specific VNO/SP-tenants and requirement R64) restricts the VNO/SP-tenants access to the SDN Management and Control function.

6.2.1.4.1.2 Fixed Access Network Sharing

TR-386 [3] and TR-370 [1] specifies how fixed access network resources can be allocated to a Tenant where the allocation creates a "virtual" Access Node (vAN). These vAN resources are made available to the Tenant when creating network slices through the CloudCO's domain orchestration function. For the Access network segment, this includes the creation of RFS connections within the Access network segment using the allocated resources of the vAN.

6.2.1.4.1.2.1 Offering Fixed Access Resources for Sharing

In the Access network, the Network Map as defined in WT-454 [32] and identified in Table 3 Access Network Resource Creation & OAM provides the list of candidate Access Nodes and associated termination points that are **available to be allocated** to a Tenant. The CloudCO's domain orchestration function then exposes the Network Map toward the Tenant.

6.2.1.4.1.2.2 Allocating Fixed Access Resources for Sharing

In the Access network, resources that have been identified by the CCO-provider for sharing can be allocated to the Tenant for their use in creation of network slices. These resources are allocated using the Network Sharing Intents defined as L2 Profiles in .

6.2.1.4.1.3 Network Function Resources and RFS Intent Service Information Elements

Table 3 Access Network Resource Creation & OAM and describes the information elements, operations and data models exposed by the Occo-Nf-sdn-access interface.

Table 3 Access Network Resource Creation & OAM

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
Access Network Map	AN-list, AN (next sub-service element)	CRUD	WT-454: Network Map	CCO-provider	Service elements may be exposed to VNOs/SP-tenants but never via direct access to SDN elements but always via the CloudCo NB API. E.g., see APPN-007 about exposing an AN geo map of OLTs to VNOs consuming a CloudCO FANS (marco-) service.
Access Node (AN)	AN-geo-location, AN-site, AN-topo-connect, AN-prop-resp-info *(opt.)* Access-netw-termination-point	CRUD and N	WT-454: Network Map	CCO-provider	
	AN-hw-info, AN-swfw-info, pAN-inst-info	CRUD and N	WT-454: Equipment Inventory RFC 7317	CCO-provider	When applicable, pAN-inst-info refers to the information related to the AN's virtualised Management Entity, i.e.,

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
			RFC 8348		the pAN instance residing in the Broadband Access Abstraction layer
End User Device (EUD)	EUD-geo-location, EUD-site, EU-info	CRUD and N	WT-454: Equipment Inventory	CCO-provider	EU-info refers to the customer information (id and contact details), not to the device info
	EUD-hw-info, EUD-swfw-info	CRUD and N	WT-454: Network Map	CCO-provider	Accessibility of these service elements to VNOs/SP-tenants depends on the agreement with CCO provider and may depend on a possible 2-box split of the EUD in Netw. Termination and End User Gateway. In this latter case this sub-service element would be split into two related to NT and EU-Gtw devices. As indicated in APPN-006 and APPN-007 VNO/SP-Tenant access to CCO resources and network services is mediated by the logics implemented in the CCO Domain Orchestration Function and the CCO NB API tailored to each actor.
L1 profiles library	L1-prof-list List of L1-prof	CRUD		CCO-provider	This information element contains a library of L1 profile templates
L1-prof	not exhaustive	---	High level description in TR-413		This information element exposes CRUD-N actions to apply L1 profiles to ANs with copper and fiber tributary interfaces. Profiles can be applied in bulk mode or via sub-profiles per the Vector of Profiles structure defined in relevant models. Sub-service elements define also L1 PM profiles, PM gathering, alarms, and other diagnostic features.
	FAST-VDSL-xDSL configuration		TR-355, TR-383i1a1	CCO-provider	

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
	Ghs-prof xTU-info TDD-prof DS-datarate-prof US-datarate-prof LowPwr-DR-prof Line-spectr-prof UPBO-prof DPBO-prof RFI-prof NoiseMargin-prof FRA-prof ReTx-prof INP-Delay-prof SOS-prof Vectoring-prof DataGath-prof Re-Init-prof Fast-retrain-prof	CRUD	RFC 7223		
	FAST-VDSL-xDSL status Line-status Channel-status Sub-carrier-status	N		CCO-provider	Accessibility of these status service elements to VNOs/SP-tenants depends on the agreement with CCO-provider
	FAST-VDSL-xDSL PM and alarms Line-PM-Thr Channel-PM-Thr Alarm-sever-prof L1-PM-collection-task Line-PM Channel-PM DataGath-report L1-alarms	CRUD and N		CCO-provider	The L1-PM-collection-task information element is not currently modelled but permits PM tasks to be tailored to one or more parameters associated with an AN or AN port. The L1-PM-collection-task allows for different types of monitoring campaigns.
	Copper Line Test MELT SELT	CRUD and N		CCO-provider	
	PON XPON-wavelength-prof	CRUD and N	WT-385 RFC 7223	CCO-provider	The L1-PM-collection-task information element is not currently modelled but permits PM tasks to

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
	ANI-power-management-prof vANI-power-management-prof GEM-TCONT-traffic-descriptor-prof GEM-TCONF-traffic-management-prof L1-PM-collection-task XPON-PM L1-alarms				be tailored to one or more parameters associated with XPON-PM. The L1-PM-collection-task allows for different types of monitoring campaigns.
	P2P ethernet pppoe-intermediate-agent-prof L1-PM-collection-task	CRUD and N	TR-383i1a1	CCO-provider	The L1-PM-collection-task information element is not currently modelled but permits PM tasks to be tailored to one or more parameters associated with PPPoE Intermediate Agent. The L1-PM-collection-task allows for different types of monitoring campaigns.

Table 4 Access Network Service Creation & Assurance

	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
L2 profiles library	L2-prof-list L2-prof	CRUD		VNO, SP-tenant	The L2 profiles library is exposed via the Occo-Nf-sdn-access interface to VNOs/SP-tenants. This information element contains a library of L2 profile templates
L2-prof	not exhaustive	---	High level description in TR-413		This information element exposes CRUD-N actions to apply technology-agnostic L2 profiles to ANs. Profiles can be applied in bulk mode or via sub-profiles defined in relevant models. Sub-information elements define also L2 PM profiles, PM gathering and alarms.
	L2-forwarding-prof LAG-LACP-prof	CRUD	TR-383i1a1 RFC 7223	VNO, SP-tenant	

	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
	Multicast-prof PPPoE-prof L2-authentic-prof L2-QoS-prof L2-VPN-prof DHCP-prof		draft-ietf-bess-l2vpn-yang-08		
	NNI-zVLAN-profile (z =O, S, C) UNI-CVLAN-profile	CRUD		VNO, SP-tenant	The NNI-zVLAN (V ref. point) and UNI-CVLAN (U ref point) profiles are used by RFS L2 connectivity services.
	Share-NNI-zVLAN-profile (z =O, S, C) Share-UNI-CVLAN-profile	CRUD	TR-370	VNO, SP-tenant	The NNI-zVLAN (V ref. point) and UNI-CVLAN (U ref point) profiles are used by FANS services.
	L2-alarm-profile	CRUD	RFC 8632 Alarm profile	VNO, SP-tenant	The alarm profile to be applied to L2 uplink or L2 downlink ports. The alarm profile is applied to the specific AN and AN port alarms.
	L2-PM Ethernet-OAM L2-PM-collection-task	CRUD	TR-383i1a1 Std 802.3.2 802.1Qcx IEEE CFM OAM	VNO, SP-tenant	The L2-PM-collection-task information element is not currently modelled but permits PM tasks to be tailored to one or more parameters associated with an AN or AN port. The L2-PM-collection-task allows for different types of monitoring campaigns.
Broadband Service	Access Broadband Resource Facing Service (RFS) intent - Subscriber Required attributes: service-type (i.e., HSIA, VoBB, Multicast service) L3US-peak-BW L3DS-peak-BW Optional attributes: UNI-port (e.g., PON UNI) UNI-C-VLANid UNI-S-VLANid NNI-port (e.g., OLT NNI) NNI-C-VLANid	CRUD		CCO-provider	Access Broadband RFS intent is an abstraction of a L2 connectivity service for a subscriber composed by NNI-zVLAN profiles (z =O, S, C) And the UNI-CVLAN profile. expected-EUD-id is used when the service is pre-provisioned and the ONT has not yet been attached. Value is the PLOAM ONTID. With the abstraction, typical broadband services including HSIA, VoBB and Multicast service can be realized by using the same YANG data model.

	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
	NNI-S-VLANid circuit (TR-101 circuit-id) remote-id (TR-101 remote-id) subscriber-id (RFC-4580 Subscriber-ID) expected-EUD-id: EUD-vendor EUD-Ser-Num EUD-Pwd Multicast-VLAN (Valid for Multicast service)				As identified, for the optional attributes, the Multicast VLAN is only valid for Multicast service. ONAP BBS use case nomenclature (AccessConnectivity: Required elements: service-type (i.e., HSIA) up-speed down-speed Optional elements: cvlan svlan expected-ont-id remote-id) EUD-Pwd is used for ONU authentication when using password authentication. ONAP SDN-C passes the same HSIA upstream and downstream bandwidth info to the Edge and Access SDN M&C (L3 DS and US b/w). The Access SDN M&C converts them into L2 DS/US b/w values based on the actual IP encapsulation method. For the BBS use case The cvlan and svlan are used to identify the subscriber in the context of the PON. The svlan is the same as the NNI-S-VLANid. The cvlan takes a default value (e.g., 4001) and equates to the NNI-C-VLANid.
Enterprise service	Access Enterprise Resource Facing Service (RFS) intent Required attributes:	CRUD		CCO-provider	

	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
	service-type (i.e., Enterprise business service) L3US- committed-BW L3DS- committed-BW Optional attributes: UNI-port (e.g., PON UNI) UNI-C-VLANid UNI-S-VLANid NNI-port (e.g., OLT NNI) NNI-C-VLANid NNI-S-VLANid circuit (TR-101 circuit-id) remote-id (TR-101 remote-id) subscriber-id (RFC-4580 Subscriber-ID) expected-EUD-id: EUD-vendor EUD-Ser-Num EUD-Pwd EUD-UNI-port (e.g., ONU UNI Eth Port) EUD-UNI-tag-mode (e.g., untagged/tagged)				
Broadband Service	EUDRegistration event Required attributes: EUD-id: EUD-vendor EUD-Ser-Num EUD-Current-sw-rel Access-netw-termination-point (PON UNI attachment point) UNI-C-VLANid UNI-S-VLANid NNI-C-VLANid NNI-S-VLANid	N		CloudCO network Access PNFs	The Access SDN M&C MUST only emit new PNFRegistration events when the UNI attachment point has changed. ONAP BBS use case nomenclature (PNFRegistration: PNFID (vendorName-serialNumber), attachment-point (PON UNI), cvlan, svlan, remote-id, circuit-id) For the BBS use case the svlan is the same as the NNI S VLANid. The cvlan equates to the NNI-C-VLANid.

	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
	circuit-id (TR-101 circuit-id) remote-id (TR-101 remote-id) subscriber-id (RFC-4580 Subscriber-ID)				

6.2.1.4.1.4Mapping of L2 Information Elements to L1 Information Elements

Table 3 Access Network Resource Creation & OAM and describes information elements for abstracted entities (e.g., L2 Profiles, L2 RFS service intents) that are realized using actual resources provided by the physical device or network function. The translation from the abstract information elements into the associated resources varies based on the type of request and the abstracted information element. The translation function is programmable and once the translation is affected, the mapping between the abstracted information element and the associated resources can be maintained.

R65) The Access SDN Management and Control function MUST provide the capability to translate abstracted information elements to associated resources that implement the abstracted behaviour. The capability to translate the abstracted information MUST be programmable such that service providers can define the translation behavior.

R66) The Access SDN Management and Control function SHOULD maintain the association between the abstracted information element and the associated resources.

6.2.1.4.2 Access Network PNF and VNF Minf/Mfc Interface

The M_{inf}/M_{fc} interface exposes to the resources of the Access network PNF and VNF as well as the BAA layer. These resources are used by the Access SDN Management and Control function.

R67) The resources exposed for the Access network PNF and VNFs MUST comply with the M_{inf}/M_{fc} interfaces specified in TR-413 [4].

R68) The resources exposed for the Access network PNF and VNF by the BAA layer MUST comply with the M_{inf}/M_{fc} interfaces specified in TR-413 [4].

6.2.1.5 Edge SDN Management and Control Function

The Edge SDN Management and Control function is responsible for provisioning, monitoring and maintenance, security and flow control for the RFS Intents and associated PNF and VNF resources within the Edge network segment of the CloudCO.

The information elements along with the associated data model and operations for the network function resources that are exposed through the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface are described in Table 5 Edge Network Resource Creation & OAM.

R69) The Edge SDN Management and Control function MUST support the exposure of the information elements defined in Table 5 Edge Network Resource Creation & OAM through the O_{cco}-$N_{f\text{-}sdn\text{-}access}$ interface.

The information elements along with the associated data model and operations for the RFS Intents associated within the Edge network segment are defined in Table 6 Edge Network Service Creation & Assurance.

R70) The Edge SDN Management and Control function MUST support RFS Intents defined in Table 6 Edge Network Service Creation & Assurance through the Occo-Nf-sdn-edge interface.

6.2.1.5.1 Edge SDN Management and Control O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ Interface

The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface is the northbound interface of the Edge SDN Management and Control function. This section describes the information elements exposed by the interface as well as the requirements for the protocol that conveys the requests, responses and notifications associated with the information elements in Table 5 Edge Network Resource Creation & OAM and Table 6 Edge Network Service Creation & Assurance.

6.2.1.5.1.1Protocol Requirements

The information elements that exposed by the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface is conveyed using the RESTCONF Protocol defined in RFC 8040 [22]. The information elements conveyed by the RESTCONF protocol is encoded in either the YANG 1.1 data modeling language defined in RFC 7950 [21] or the YANG 1.0 data modeling language defined in RFC 6020 [20].

R71) The information elements and services for resources and RFS Intents conveyed over the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface SHOULD be represented using the YANG 1.1 data modeling language defined in RFC 7950 [21].

R72) The information elements and services for resources and RFS Intents conveyed over the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface SHOULD be represented using the YANG 1.0 data modeling language defined in RFC 6020 [20].

R73) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST support the RESTCONF protocol defined in RFC 8040 [22].

Requests received via the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface uses the capabilities of the RESTCONF protocol and YANG data model specifications that permit the request to scope the request to specific targets (e.g., network function) and information element or sub-information element.

R74) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability to scope requests received across the interface to:

1) Specific targets for RFS Intents and Network Functions
2) Sets of Information elements and Sub-information elements defined in Table 6 .

Notifications produced by the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface uses the Subscription capabilities of the RESTCONF protocol.

R75) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability for management systems to subscribe to be notified of events (e.g., status change, threshold crossing, alarms, notifications) associated with RFS Intents and resources exposed by Network Functions using the subscription capability defined in RFC 5277 [19].

Once subscribed, notifications that are emitted across the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface uses various technologies (e.g., RESTCONF, HTTPS, Kafka) to transport the notification to the subscribed entity.

R76) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability to notify entities that have subscribed for notifications.

Notifications produced by the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface uses the Subscription capabilities of the RESTCONF protocol.

R77) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability for management systems to subscribe to be notified of events (e.g., status change, threshold crossing, alarms, notifications) associated with RFS Intents and resources exposed by Network Functions using the subscription capability defined in RFC 8040 [22] with the transport and encoding protocols appropriate for the type of event.

R78) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability for management systems to subscribe to be notified of performance monitoring data to be reported that is associated with RFS Intents and resources exposed by Network Functions using the subscription capability defined in RFC 8040 [22] with the transport and encoding protocols appropriate for the type of event.

R79) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface SHOULD provide the capability to extend the event streams <access> information element defined in section 6.2 of RFC 8040 [22] to include Kafka transports. The <encoding> element value for a Kafka transport stream MUST be either "xml+kafka" or "json+kafka". When the <encoding> element is “xml+kafka” or “json+kafka”, the <location> element value MUST be of the format “kafka://ip1:port1[,ip2:port2..ipN:portN]/<topic-name>”.

Once subscribed, notifications and performance monitoring data that are transmitted across the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface uses various technologies (e.g., RESTCONF, HTTPS, Kafka) to transport the notification to the subscribed entity.

R80) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability to notify entities that have subscribed for notifications.

R81) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability to notify entities that have subscribed for reporting of performance monitoring data.

The information elements that are exposed across this interface require control to ensure access to the information elements and RFS Intents are not exposed to unauthorized agents. The capability to restrict the information element and associated operations has to be programmable such that individual attributes of information elements associated with instances of resources for Network Functions or RFS Intents can be selected to be exposed to a user of the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface.

Likewise, any information elements exposed through the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface is required be exposed to only authorized management systems. This is necessary to ensure direct access to the SDN Management and Control function by VNO/SP-tenants is not permitted as these users are required to access the CloudCO resources through the CloudCO Os-Ma-ccodo interface.

R82) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST provide the capability to ensure access to the information elements and RFS Intents are not exposed to unauthorized agents. The capability to restrict the information element and associated operations MUST be programmable such that individual attributes of information elements associated with instances of resources for Network Functions or RFS Intents can be selected to be exposed to a user of the O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface.

R83) The O_{cco}-$N_{f\text{-}sdn\text{-}edge}$ interface MUST restrict access to the SDN Management and Control function to authorized users.

Note: Requirement R82) permits the scope of information elements to be restricted to specific VNO/SP-tenants and requirement R83) restricts the VNO/SP-tenants access to the SDN Management and Control function.

6.2.1.5.1.2 Network Function Resources and RFS Intent Service Information Elements

Table 5 Edge Network Resource Creation & OAM and Table 6 Edge Network Service Creation & Assurance describes the information elements, operations and data models exposed by the Occo-Nf-sdn-edge interface.

Table 5 Edge Network Resource Creation & OAM

Information element name	Sub-information element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
Network Map		CRUD	WT-454: Network Map	CCO-provider	Exposure of the Infrastructure network map that depicts the network nodes and associated geographical location, site and responsible party information of where the nodes are located.

6.2.1.5.1.3 Network Function Resources and RFS Intent Service Information Elements

Table 6 Edge Network Service Creation & Assurance

Service element name	Sub-service element name	CRUD-N	Ref. model info/YANG	Main actor (Informative)	Notes/description
Broadband Service	InternetProfile Resource Facing Service (RFS) intent Required attributes: service-type (i.e., HSIA) L3US-peak-BW L3DS-peak-BW Optional attributes: UNI-port (e.g., Edge NNI) UNI-C-VLANid UNI-S-VLANid circuit-id (TR-101 circuit-id) nas-port-id (TR-101 NAS-Port-Id) remote-id (TR-101 remote-id) subscriber-id (RFC-4580 Subscriber-ID) EUD-mac-address	CRUD		CCO-provider	APPN_446 depicts the usage of the InternetProfile RFS intent which is an abstraction of a full blown L3 connectivity service. ONAP BBS use case nomenclature (Internet Profile: service-type, down-speed, up-speed, cvlan, svlan, remote-id) **Note:** the cvlan and svlan determine the UNI into the Edge network (NNI of Access network)
Broadband Service	EUDAuthentication event Required attributes: EUD-id: EUD-vendor EUD-Ser-Num OldState, NewState, EUD-mac-address EUD-Current-sw-rel	N		CloudCO network AAA function	The Edge SDN M&C MUST only emit new EUDAuthentication events when the authentication state has changed. ONAP BBS use case nomenclature (CPEAuthentication: PNFID (vendorName-serialNumber), oldState, newState, macAddress, softwareVersion)

6.2.1.5.2 Edge Network PNF and VNF Minf/Mfc Interface

The M_{inf}/M_{fc} interface exposes to the resources of the Edge network PNF and VNFs. These resources are used by the Edge SDN Management and Control function.

R84) The resources exposed for the Edge network PNF and VNFs MUST comply with the M_{inf}/M_{fc} interfaces specified in WT-413 Issue 2 [31].

6.2.1.6 Data Center SDN Management and Control Function

The DC SDN Management and Control function directly accesses the NFVI networking resources to implement functions (e.g., L3 routes in the switch fabric) outside the scope of VIM control.

The content for this section and corresponding subsections is expected to be included in future issues of this Technical Report to include:

- Requirements for the $\text{O}_{\text{cco}}\text{-N}_{\text{f-sdn-dc}}$, $\text{M}_{\text{fc-sdn-dc-Nf}}$ and $\text{M}_{\text{fc-sdn-dc-Vi}}$ reference points
- Further definition and requirements for the Or-Vnfm, Or-Vi, Vi-Vnfm, Ve-Vnfm-vnf, Nf-Vi reference points

6.3 Definition of Or-Vnfm

The Or-Vnfm reference point provides management of NFVI resources for a VNF including information needed for authorization, validation, reservation, allocation and release of NFVI resources. In addition, lifecycle management of VNFs is provided. The information exchanges across this reference point is described in [12].

6.4 Definition of Or-Vi

The Or-Vi reference point provides management of NFVI resources including information needed for allocation and release of NFVI resources. The information exchanges across this reference point is described in [10].

6.5 Definition of Vi-Vnfm

The Vi-Vnfm reference point provides management of NFVI resources including information needed for validation, reservation, allocation, update and release of NFVI resources. In addition, software image management of VNFs is provided. The information exchanges across this reference point is described in [11].

6.6 Definition of Ve-Vnfm-vnf

The Ve-Vnfm-vnf reference point provides lifecycle management of VNFs managed by the VNFM. The information exchanges across this reference point is described in [13].

6.7 Definition of Nf-Vi

The NF-Vi reference point is comprised of sub-reference points for interfaces associated with requesting infrastructure connectivity services ([Nf-Vi]/N), hypervisor services ([Nf-Vi]/H) and compute services ([Nf-Vi]/C). The [Nf-Vi/N] reference point is described in clause 5.2 of [13] and clause 5.7.4 of [8] describes the information exchanges across this reference point.

6.8 Definition of Vn-Nf

The [Vn-Nf]/N reference point provides transparent network services to VNFs as described in clause 5.1 of [13].

Appendix I.Supportive Application Notes to the Interfaces

Table 7 Supportive Application Notes

Interfaces	Supportive Application Notes
Os-Ma-ccodo	CloudCO-APPN-000: Bootstrapping an NFVI into a Cloud Central Office CloudCO-APPN-001: Establish High Speed Internet Access (HSIA) Service CloudCO-APPN-002: Network Enhanced Residential Gateway (NERG) Service Initialization with Flat Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-003: Network Enhanced Residential Gateway (NERG) Service Initialization with Overlay Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-006: Virtual Access Node (vAN)-based FANS service CloudCO-APPN-007: SDN-based FANS service CloudCO-APPN-441: Converged Core-as-a-Service (with PNF based User Plane) CloudCO-APPN-442: Value Added Service (VAS) based on NERG CLOUD-CO-APPN-443: BNG-as-a-Service (with VNF based Control and User Plane) CLOUD-CO-APPN-444: CDN-as-a-Service Cloud-CO-APPN-446: ONAP Integration for Residential Broadband HSIA Service CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System CloudCO-APPN-463: EasyMesh Cloud Controller
Occo-Nf-sdn-access	CloudCO-APPN-446: ONAP Integration for Residential Broadband HSIA Service
Occo-Nf-sdn-edge	CloudCO-APPN-446: ONAP Integration for Residential Broadband HSIA Service
Occo-Nf-sdn-pnf	CloudCO-APPN-000: Bootstrapping an NFVI into a Cloud Central Office CloudCO-APPN-001: Establish High Speed Internet Access (HSIA) Service CloudCO-APPN-002: Network Enhanced Residential Gateway (NERG) Service Initialization with Flat Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-007: SDN-based FANS service
Occo-Nf-sdn-vnf	CloudCO-APPN-001: Establish High Speed Internet Access (HSIA) Service CloudCO-APPN-003: Network Enhanced Residential Gateway (NERG) Service Initialization with Overlay Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-007: SDN-based FANS service CloudCO-APPN-441 Converged Core-as-a-Service (with PNF based User Plane) CloudCO-APPN-442: Value Added Service (VAS) based on NERG CLOUD-CO-APPN-443: BNG-as-a-Service (with VNF based Control and User Plane) CLOUD-CO-APPN-444: CDN-as-a-Service CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System CloudCO-APPN-463: EasyMesh Cloud Controller
Occo-Nf-sdn-dc	CloudCO-APPN-000 - Bootstrapping an NFVI into a Cloud Central Office CloudCO-APPN-001 - Establish High Speed Internet Access (HSIA) Service CloudCO-APPN-002 - Network Enhanced Residential Gateway (NERG) Service Initialization with Flat Logical Subscriber Link (LSL) Connectivity
Mfc-sdn-dc-Nf	Cloud-CO-APPN-446 : ONAP Integration for Residential Broadband HSIA Service (Access)
Or-Vnfm	CloudCO-APPN-006 - Virtual Access Node (vAN)-based FANS service CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System

Interfaces	Supportive Application Notes
	CloudCO-APPN-463: EasyMesh Cloud Controller
Or-Vi	CloudCO-APPN-000: Bootstrapping an NFVI into a Cloud Central Office CloudCO-APPN-001: Establish High Speed Internet Access (HSIA) Service CloudCO-APPN-002: Network Enhanced Residential Gateway (NERG) Service Initialization with Flat Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-003: Network Enhanced Residential Gateway (NERG) Service Initialization with Overlay Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-441: Converged Core-as-a-Service (with PNF based User Plane) CloudCO-APPN-442: Value Added Service (VAS) based on NERG CLOUD-CO-APPN-443: BNG-as-a-Service (with VNF based Control and User Plane) CLOUD-CO-APPN-444: CDN-as-a-Service CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System CloudCO-APPN-463: EasyMesh Cloud Controller
Ve-Vnfm-vnf	CloudCO-APPN-006 - Virtual Access Node (vAN)-based FANS service CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System CloudCO-APPN-463: EasyMesh Cloud Controller
Nf-Vi	CloudCO-APPN-000 - Bootstrapping an NFVI into a Cloud Central Office CloudCO-APPN-001 - Establish High Speed Internet Access (HSIA) Service CloudCO-APPN-002 - Network Enhanced Residential Gateway (NERG) Service Initialization with Flat Logical Subscriber Link (LSL) Connectivityl CloudCO-APPN-003 - Network Enhanced Residential Gateway (NERG) Service Initialization with Overlay Logical Subscriber Link (LSL) Connectivity CloudCO-APPN-442: Value Added Service (VAS) based on NERG CLOUD-CO-APPN-443: BNG-as-a-Service (with VNF based Control and User Plane) CLOUD-CO-APPN-444: CDN-as-a-Service CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System
Vn-Nf	CloudCO-APPN-445: Monitoring, Diagnostics, and Optimization in a Residential Broadband System

Appendix II. Information model for Profiles

This Technical Report defines profile libraries in Table 3 and that are used in fulfillment and maintenance of services and management of resources. This section of the Technical Report defines the information model that is used to convey the profiles across the SDN M&C and CloudCO DO function's northbound interfaces. As the purpose of a profile is for the operator to define a common set of parameters and associated values for a specific purpose that can be applied to the configuration of one or more instances of target resources, the most straight forward way to compose a profile is using name/value pairs for the leaf attributes of the class. Additionally, Profiles can be building blocks of other profiles that can be used to create more complex profiles.

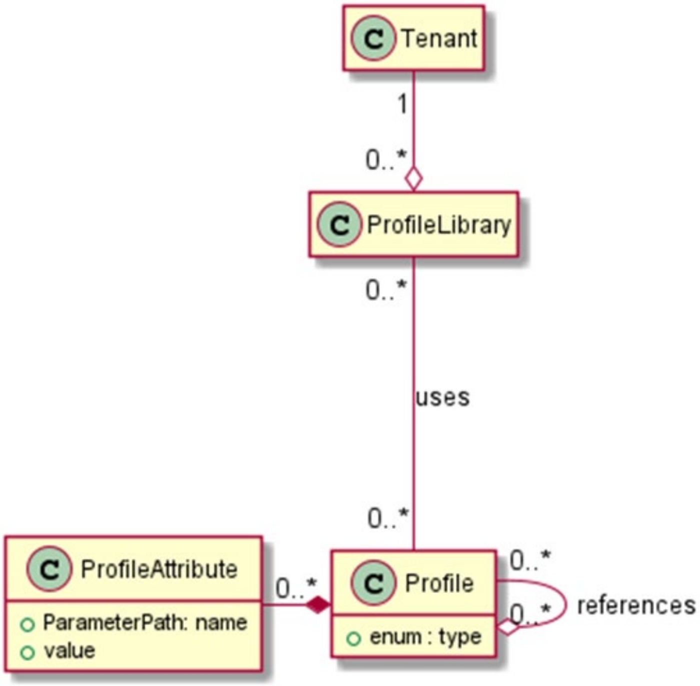

Figure 7 Profile Information Model

End of Broadband Forum Technical Report TR-411