TECHNICAL REPORT

TR-370

Fixed Access Network Sharing - Architecture and Nodal Requirements

Issue: 2
Issue Date: April 2020

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

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
Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

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.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	27 November 2017	12 January 2018	Bruno Cornaglia	Original
2	10 April 2020	10 April 2020	Bruno Cornaglia	Original

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

Editor	Bruno Cornaglia	Vodafone
Work Area Director(s)	George Dobrowski	Morriscreek Consulting
	Bruno Cornaglia	Vodafone

Table of Contents

List of Figures

List of Tables

Executive Summary

This Technical Report specifies technical aspects associated with Fixed Access Network Sharing (FANS) that involve the access network (including access nodes and aggregation nodes). It focuses on the cases of Passive Optical Network (PON) and DSL and G.fast access technologies.

FANS presents business opportunities supporting, the evolution of the fixed access network to enable new, dynamic service offerings, aligned with the Forum's Broadband 20/20 vision, and business relationships. This Technical Report identifies a new type of Virtual Network Operator (VNO), while specifying the technical requirements associated with both the VNO and the Infrastructure network Provider (InP).

This Technical Report, based on TR-101 [2], TR-178 [3] and TR-156 [4], documents a set of architectures for sharing multi-service broadband access networks, implemented using legacy equipment or based on ETSI NFV virtualisation standards. Starting from the above architectural models, this Technical Report defines topologies, deployment scenarios and specific requirements needed to successfully deploy a shared access network.

This Technical Report defines three models that all include a centralised management system capable of supporting a multi-vendor environment, with the goal of maintaining backwards compatibility in a shared access network infrastructure. The centralised management system is in charge of managing the network sharing and the above models correspond to differentiated solutions based on the operating methods.

The first solution relies on the centralised management system to perform the network slicing of existing (legacy) or new network equipment at the management system level (not directly in the equipment itself), while the second solution implements slicing on the equipment itself and also can use virtualisation as described by ETSI NFV standards. The second one is also capable of coordinating the virtual Access Node (vAN) and virtual Aggregation Nodes (vAggN) instances of the different VNOs. The SDN-based approach relies on vAN and vAggN instances which are Management and Control (M&C) Plane entities accessed by VNOs to manage their virtual network resources via the mediation of SDN M&C elements. The Data Planes of all VNOs' virtual networks remain respectively within the physical Access Nodes and the Aggregation Switches/Switch Fabrics.

Finally, the document also includes the OAM, privacy and security considerations necessary to support multi-operator access sharing.

1 Purpose and Scope

1.1 Purpose

“FANS - Architecture and Nodal Requirements” specifies the technical aspects associated with Fixed Access Network Sharing (FANS) that involve the access network, including both access and aggregation nodes. Slicing logically partitions and isolates network resources among Virtual Network Operators (VNOs). FANS Technical Report covers Passive Optical Network (PON) and DSL and G.fast networks, addressing typical infrastructures, topologies and FTTx deployment scenarios.

This Technical Report specifies technical aspects related to the migration of TR-101, TR-178, and TR-156 based architectures towards a shared, broadband access network that supports slicing for multi-tenant operation. Functionalities over and above TR-178 are identified. This includes specifying which access node functions would continue to be managed by the Infrastructure Provider (InP) and which would be managed by a VNO. Access and backhaul interface sharing may require additions to the required transport encapsulations, QoS and OAM capabilities.

“FANS - Architecture and Nodal Requirements” defines three different models for resources sharing or slicing:

- Management System based, which performs network slicing at management system level and not directly in the equipment itself.
- Virtual Access Node based, which extends the capabilities of physical access and aggregation nodes to support multiple, virtual functions, each containing ports and forwarding resources directly managed by a VNO.
- The SDN-based approach relies on vAN and vAggN instances which are Management and Control (M&C) Plane entities accessed by VNOs to manage their virtual network resources via the mediation of SDN M&C elements. The Data Planes of all VNOs’ virtual access networks remain respectively within the physical Access Nodes and the Aggregation Switches/Switch Fabrics.

This Technical Report also identifies the relationship between FANS and the ETSI and BBF TR-359 NFV architecture.

For both the Management System and Virtual Access Node approaches, this Technical Report defines the architectural options and requirements intended for implementation on existing TR-101/TR-178 access networks through software upgrade, as well as requirements that would only apply to new access nodes.

Finally, the document considers the security and privacy aspects necessary to support multi-operator access sharing/slicing.

1.2 Scope

The scope of “FANS - Architecture and Nodal Requirements” is to address Fixed Access Network Sharing with an analysis of the access network, in terms of the following functions:

- Physical and Logical Network Architecture
- Technical and Functional Node Requirements
- User/Network Interfaces (T, U / V, A10)
- Layer 2 interconnection
- Management Interfaces
- Virtual Node Framework and Interfaces
- Virtualisation Techniques
- OAM and other Operational Aspects
- Privacy and Security

1.3 Business Context

The primary FANS scenario is related to VNOs and InP being different entities. In addition, this Technical Report specification can also apply to a network operator that wants to slice its own access network in order to offer services to different market segments (e.g., for residential or enterprise markets), and wants to be able to use a vertical structure within its organization for aspects related to the customers, services and resources.

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 [1].

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 behaviour is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behaviour 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.

Document		Title	Source	Year
[1]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[2]	TR-101i2	*Migration to Ethernet Based DSL Aggregation*	BBF	2011
[3]	TR-178i2	*Multi-service Broadband Network Architecture and Nodal Requirements*	BBF	2017
[4]	TR-156i3	*Using GPON Access in the context of TR-101*	BBF	2012
[5]	802.1Q-2014	*Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks*	IEEE	2014
[6]	802.1ad-2014	*Virtual Bridged Local Area Networks Amendment 4: Provider Bridges*	IEEE	2014
[7]	TR-359	*A Framework for Virtualisation*	BBF	201??

[8]	TR-167i2	*GPON-fed TR-101 Ethernet Access Node*	BBF	2010
[9]	TR-221	*Technical Specifications for MPLS in Mobile Backhaul Networks*	BBF	2011
[10]	TR-198i2	*DQS: DQM systems functional architecture and requirements*	BBF	2012
[11]	IEEE 1588-2008	*IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*	IEEE	2008
[12]	GS NFV-INF 001 V1.1.1	*Network Functions Virtualisation (NFV) – Infrastructure; Infrastructure Overview*	ETSI	2014
[13]	GS NFV 002 V1.2.1	*Network Functions Virtualisation (NFV) - Architectural Framework*	ETSI	2014
[14]	GS NFV-INF 003 V1.1.1	*Network Functions Virtualisation (NFV) – Infrastructure; Compute Domain*	ETSI	2014
[15]	GS NFV-INF 004 V1.1.1	*Network Functions Virtualisation (NFV) – Infrastructure; Hypervisor Domain*	ETSI	2014
[16]	GS NFV-INF 005 V1.1.1	*Network Functions Virtualisation (NFV) – Infrastructure; Network Domain*	ETSI	2014
[17]	GS NFV-MAN 001 V1.1.1	*Network Functions Virtualisation (NFV) - Management and Orchestration*	ETSI	2014
[18]	G.8013/Y.1731	*OAM functions and mechanisms for Ethernet based networks*	ITU-T	2013
[19]	802.1ag-2014	*Connectivity Fault Management*	IEEE	2014
[20]	RFC 7348	*Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualised Layer 2 Networks over Layer 3 Networks*	IETF	2015
[21]	GB921	*Business Process Framework (eTOM)*	TM Forum	2016
[22]	TR-197i2	*DQS: DSL Quality Management Techniques and Nomenclature*	BBF	2004
[23]	TR-386	*Fixed Access Network Sharing - Access Network Sharing Interfaces*	BBF	2019
[24]	TR-384	*Cloud Central Office (CloudCO) Reference Architectural Framework*	BBF	2018
[25]	TR-413	*SDN Management and Control Interfaces for CloudCO Network Functions*	BBF	2018
[26]	TR-402	*Functional Model for PON Abstraction Interface*	BBF	2018
[27]	F.Slyne, B.Cornaglia, M.Boselli, M.Ruffini	*3-stage Hierarchical Quality of Service for Multi-tenant Passive Optical Networks*	ONDM	2019
[28]	CLOUDCO-APPN-006	*Virtual Access Node (vAN)-based FANS service [https://www.broadband-forum.org/technical/download/CloudCO-APPN-006.pdf]*	BBF	2018

[29]	CLOUDCO-APPN-007	*SDN-based FANS service [https://www.broadband-forum.org/technical/download/CloudCO-APPN-007.pdf]*	BBF	2018
[30]	TR-301i2	*Architecture and Requirements for Fiber to the Distribution Point*	BBF	2019

2.2.1 Draft References

The reference documents listed in this section are applicable to this Technical Report but are currently under development 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-411	*Definition of interfaces between Cloud CO Functional Modules*	BBF	unspecified
[32]	WT-435	*NETCONF Requirements for Access Nodes and Broadband Access Abstraction*	BBF	unspecified

2.3 Definitions

The following terminology is used throughout this Technical Report.

Access Network	The Access Network encompasses the elements of the broadband network from the NID at the customer premises to a Broadband Network Gateway (not included). This network typically includes one or more types of Access Node and may include an Ethernet aggregation function.
Access Node (AN)	The Access Node (also called physical Access Node, pAN) may implement one or more access technologies based on copper or fiber. It may also aggregate traffic from other access nodes. It can be placed in a variety of locations from climate controlled (central) offices to outside environments that require climate hardening of the equipment to avoid the need for additional cabinets or enclosures. As per TR-156 a PON Access Node is a logical entity whose functions are distributed between the OLT and ONUs.
Aggregation Network	The part of the network between the Access Node and the Broadband Network Gateway(s).
Aggregation Node (AggN)	The Aggregation Node (also called physical Aggregation Node, pAggN) aggregates traffic from multiple Access Nodes.
Infrastructure Provider (InP)	The Infrastructure Provider is responsible for maintaining the physical network resources of the network. An InP can make resources available to Virtual Network Operators (VNOs).
Virtual Access Network	The Virtual Access Network is a virtual representation of a portion of a shared physical access network. Virtual access networks are defined by an Infrastructure Provider (InP) and can be controlled and managed by Virtual Network Operators (VNOs)
virtual Access Node (vAN)	The abstraction of the Access Node element as seen by a VNO.

virtual Aggregation Node (vAggN)	The abstraction of the Aggregation Node element as seen by a VNO.
Virtual Network Operator (VNO)	The Virtual Network Operator operates, controls, and manages the Virtual Access Network. The VNO can be a business entity separate from the InP, or can be a separate business entity within the InP.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AAA	Authentication Authorization Accounting
AggN	Aggregation Node
AN	Access Node
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
BAA	Broadband Access Abstraction
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BSS	Business Support System
CO	Central Office
CMS	Centralised Management System
CoS	Class of Service
COTS	Commercial Off The Shelf
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DCF	Data Collection Function
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSM	Dynamic Spectrum Management
EM	Element Manager
EMS	Element Management System
E-NNI	External Network to Network Interface
ETSI	European Telecommunications Standards Institute
E2E	End To End
eTOM	Enhanced Telecom Operations Map
FANS	Fixed Access Network Sharing
FTTB	Fibre To The Building
FTTC	Fibre To The Curb/Cabinet
FTTdp	Fibre To The Distribution Point
FTTH	Fibre To The Home

FTTx	Fibre To The x (generalization for several types of fibre deployment)
GEM	GPON Encapsulation Method
GPON	Gigabit Passive Optical Network
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
I-NNI	Internal Network to Network Interface
InP	Infrastructure Provider
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPTV	Internet Protocol Television
ISG	Industrial Study Group
ITU-T	International Telecommunication Union – Telecommunication Standardisation Bureau
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LSP	Label Switched Path
MAC	Medium Access Control
MANO	Management & Orchestration
MDF	Main Distribution Frame
MPLS	Multi-Protocol Label Switching
MS	Management System
NBI	Northbound Interface
NERG	Network Enhanced Residential Gateway
NETCONF	Network Configuration Protocol
NFV	Network Functions Virtualisation
NFVI	Network Function Virtualisation Infrastructure
NFVO	NFV Orchestrator
NIC	Network Interface Card
NID	Network Interface Device
NMS	Network Management System
NNI	Network-to-Network Interface
NSP	Network Service Provider
NT	Network Termination
OAM	Operation, Administration and Maintenance
ODN	Optical Distribution Node
OLT	Optical Line Termination
ONT	Optical Network Terminator
ONU	Optical Network Unit
OSS	Operational Support System

O-Tag	Operator Tag
O-VLAN	Operator VLAN
pAN	Physical Access Node
PCE	Power Control Entity
PCP	Priority Code Point
PE	Provider Edge
PHY	Physical
PNF	Physical Network Function
PON	Passive Optical Network
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PTP	Precision Timing Protocol
QoS	Quality of Service
RG	Residential Gateway
SBI	Southbound Interface
SDAN	Software Defined Access Network
SDN	Software Defined Networking
SDN M&C	SDN Management and Control
SLA	Service Level Agreement
SNI	Service Node Interface
TE	Traffic Engineering
TLS	Transparent LAN Services
TR	Technical Report
UNI	User-to-Network Interface
vAggN	Virtual Aggregation Node
vAN	virtual Access Node
vBNG	Virtual Broadband Network Gateway
VIM	Virtual Infrastructure Manager
VLAN	Virtual LAN
VNF	Virtual Network Function
VNFM	Virtual Network Function Management
VNI	VXLAN Network Identifier
VNO	Virtual Network Operator
VPN	Virtual Private Network
VTEP	VXLAN Tunnel End Point
vRG	Virtual Residential Gateway
VXLAN	Virtual Extensible LAN
YANG	Yet Another Next Generation

3 Technical Report Impact

3.1 Energy Efficiency

FANS introduces the concept of Fixed Access Network Sharing that splits the physical access network into a number of virtual access networks, which can be shared by multiple Virtual Network Operators (VNOs). By allowing multiple VNOs to share a single physical network infrastructure, FANS enables energy efficiency improvements in the network.

3.2 IPv6

FANS uses current specifications of IPv6 and no specific impact is foreseen. Sharing methods in this document are at Layer 2, so each VNO can have its own specific IP range, both IPv4 and IPv6.

3.3 Security

Sharing the same infrastructure among different operators can create issues of security. In order to address these, it is necessary to have robust methods for isolating the resources, including data, control and management planes, of all operators. The document provides recommendations to address security issues.

3.4 Privacy

Sharing the same infrastructure between different operators can create issues of customer privacy. It is necessary to define methods for isolating the control and management planes of all operators as well as customers' networks and information. The document will provide recommendations to address privacy issues.

4 Architecture and Topologies

The accelerating demand for capacity and the need for new business and service models calls for network operators to seek cost-effective ways to modernize their networks.

The model of physical network assets ownership by market players acting as Network Operators and Service Providers is beginning to be challenged under the light of the above business and cost considerations. Competing players may now wish to cooperate in network-sharing schemes.

With technology advances, access networks can be shared to a greater extent than they currently are. The current methods for access network sharing (e.g., Bitstream, VULA), where service packages are only differentiated by bandwidth, limit the ability of VNOs to provide richer service differentiation.
Fixed Access Network Sharing (FANS) is a resource sharing approach that allows to expose a broader set of access functions to VNOs.
In FANS, a physical Access Network owned by an Infrastructure Provider (InP) can be shared by multiple Virtual Network Operators (VNOs). Each VNO operates and manages a virtual slice of the physical network to provide customized services. Each slice spans the physical network between the following reference points as defined in TR-101[2]/TR-178[3]/TR-156[4]:

- U/U1 between shared network and CPE
- A10 (E-NNI L2) between shared network and BNG

Neither the CPE nor the BNG are part of the Virtual Access Network – instead, each of these network elements is owned by the VNO.
Infrastructure Providers are responsible of the Access Network infrastructure and the deployed FANS solution and services.
This defines three resource sharing models that can be chosen:

- Management System [section 5.1]
- Virtual Node [section 5.2]
- SDN-based [section 5.3]

In the Management System model, network slicing is performed in the management plane. A Centralised Management System, administered by the InP, controls the physical network and provides to each VNO a management view of a virtual network slice. The Centralised Management System includes an abstraction layer that maps each virtual network to the physical network. In this model, the devices in the physical network are unaware of the virtual slices, and each VNO is unaware of resources outside its own slice. This model is well suited to access networks which still have legacy devices.

In the Virtual Access Node model, network slicing is performed in both the management and data planes. In the Virtual Access Network, each VNO controls virtual Access Nodes (vANs) as well as potentially other L2 virtualised functions in the data plane via the brokerage and mediation of the Centralised Management System.

The SDN-based FANS model leverages on the so called Software Defined Access Network (SDAN) to deliver network automation, interfaces programmability, FANS service flexibility and agility, separation of VNO domains while the InP retains full operational control the FANS infrastructure and services. A key element of SDAN is the Access SDN Manager and Controller (M&C) which is capable to manage a multi-vendor and multi-technology Access Network via device adapter that can control legacy and innovative Access Node designs. To support FANS, the SDN M&C implements a Slice Manager and a Resource Mapper that expose vAN representations of the resources allocated to each VNO. They also guarantee brokerage and mediation of VNOs requests towards the shared resources.

4.1 Architecture

Figure 1 shows a high level perspective of the access network. The main network elements in a fixed broadband network are:

- Customer Premises Equipment (CPE)
- Access Node (AN)
- Aggregation Node (AggN)
- Broadband Network Gateway (BNG)

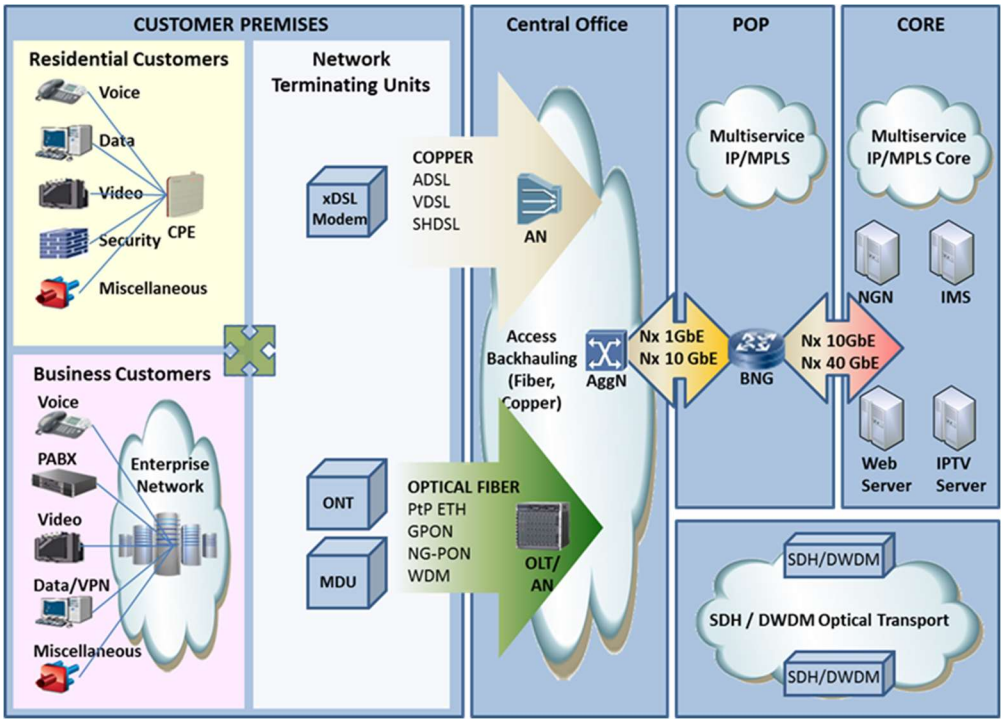


Figure 1 – Integrated Fixed Access Network approach

Fixed Access Network Sharing as specified in this Technical Report does not involve the CPE and BNG; it covers the Access and Aggregation Nodes and all the related interfaces towards the CPE and BNG.
It is important to ensure that connectivity is always available between the ANs and BNGs. Redundant physical paths are required to achieve the highest level of availability between a BNG and AN and this usually requires a protocol to route around failed paths. Typically this is based on a Provider Ethernet or Multi-Protocol Label Switching (MPLS) network with redundancy in the core.

Several BNGs, central office ANs and AN options can coexist in the same network, as shown in Figure 2.
Va is the reference point at which the first level of Ethernet aggregation and the rest of the network interconnect. It may or may not be external to the Access Node and it can instantiate logical interfaces such as an I-NNI and/or can instantiate business interfaces such as an E-NNI-L2. In TR-178 [3], an Access Node with an internal Va reference point uses the V reference point for its uplinks.
Within the core network, the migration toward an IP/MPLS infrastructure has been underway for some time. IP/MPLS is ideally suited for such migration because it offers the benefits of an IP-centric control plane while still being able to manage L2 transport services such as ATM, Frame Relay, and Ethernet. It also supports L3 services such as VPNs based on the Border Gateway Protocol (BGP), and can provide end-to-end Quality of Service (QoS) via Traffic Engineering. However, neither the ATM nor the L3 reference points (E-NNI L1 and E-NNI L3) are in the scope of access network sharing as defined in this Technical Report.

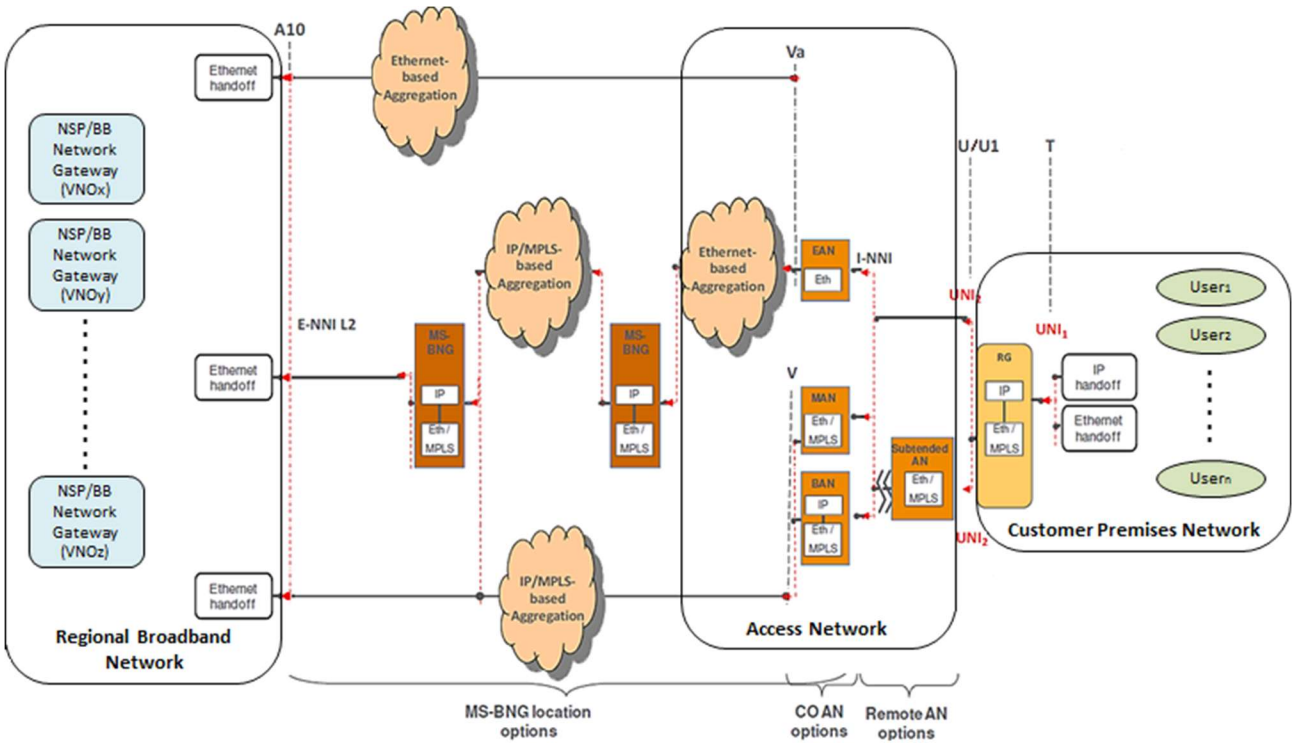


Figure 2 – FANS Architecture scheme derived from TR-101 [2] and TR-178 [3]

Figure 2 shows the reference points and the possible interconnection between InP and VNOs at A10 or V/Va reference point. The traffic coming from U/U1 interfaces can be delivered to VNOs at V/Va reference point if VNOs directly interconnect the InP infrastructure at Access Node or at A10 interface if VNOs interconnect at Aggregation Node.

4.2 Sharing Model

In current fixed access networks, network elements are usually “closed” systems, with vendor-proprietary interfaces. Therefore, once deployed, it is quite difficult for the current network infrastructure to evolve. Those network nodes are designed to meet the features and requirements of the services offered by the various operators, such as:

- real time performance
- resiliency and redundancy
- manageability
- capacity and load balancing mechanism

Nowadays the challenge is to enable new business models for leveraging the access network infrastructure while fulfilling the above requirements for access connectivity services in a more flexible and scalable way. These paradigm shifts in the business and technical scenarios of fixed access deployments could be done by introducing innovative IT solutions and technologies into the Telco environment, using virtualisation and software defined network techniques.
Under the business perspective two new types of players are identified:

- Infrastructure Provider (InP)
- Virtual Network Operator (VNO)

Under a technical standpoint, the InP is responsible for deploying, managing and maintaining the access network infrastructure. Beyond the usual responsibilities of a Network Operator, the FANS offering encompasses:

- Enabling and managing physical resource slicing per the FANS framework agreed with the VNOs
- Exposing FANS APIs to the VNOs to allow them to manage their allocated resources

The VNO leases resources from InPs and creates its own Virtual Access Networks by deploying networking protocols of its choice. The VNOs' main activities are to:

- Operate, control, and manage their own virtual network made of vANs; vANs are Management and Control Plane entities allowing VNOs to access the allocated slice on each physical AN; as mentioned in the introduction of chapter 4, for the Virtual Access Node model, vAN slices may also encompass Data Plane functions.
- Provide customized services over their virtual network

A VNO, via the FANS interface, requests the allocation of the resources to form the VNO's Virtual Access Network, which can coexist with other Virtual Access Networks on the same InP infrastructure. Therefore, the FANS solution has to implement appropriate brokerage and mediation mechanism of VNOs' requests as well as traffic engineering techniques to guarantee the overall fulfillment of the SLAs (bandwidth, priority, packet loss ratio, …) in place with all VNOs. Such traffic engineering has to be somewhat adaptive/reactive since the coverage and topology of the Virtual Access Network can be dynamic, based upon VNO demand. The solution is represented in Figure 3.

Current access network architectures have often led to the deployment of co-located physical access nodes by competing operators. FANS allows serving multiple VNOs via a single physical AN. Figure 4 shows a typical layout for the AN used in a FANS scenario.

As in traditional architectures, there are access nodes capable of supporting all the widely deployed access technologies as well as the newly emerging ones including Subtending Access Node, as shown in Figure 5.

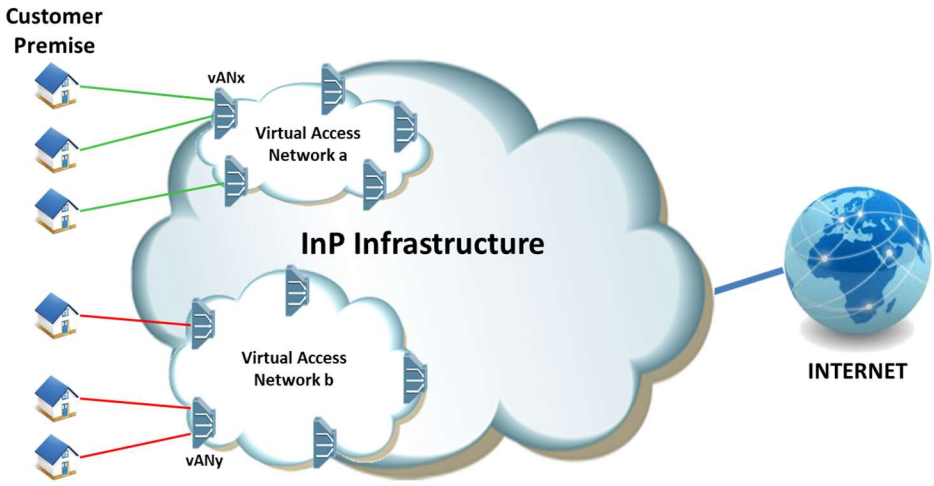


Figure 3 – Virtual Access Network concept

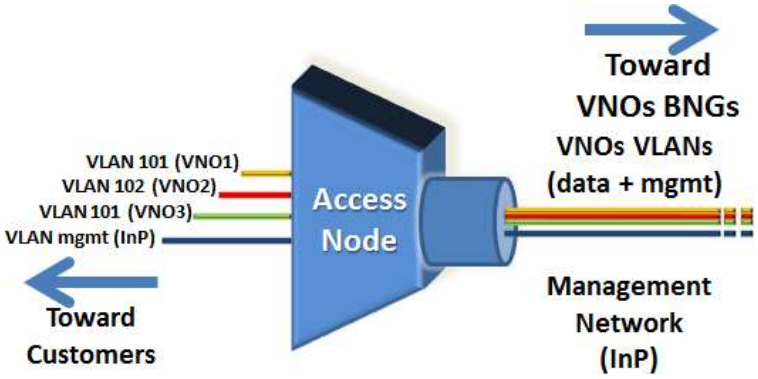


Figure 4 – FANS Physical Access Node Representation

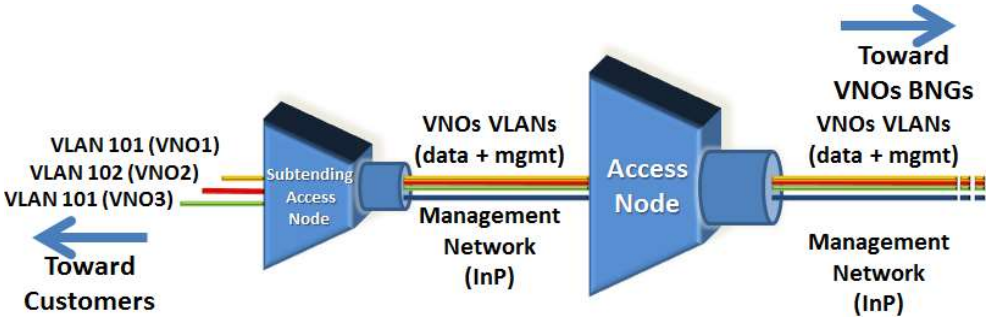


Figure 5 – FANS Chained Access Node Representation

The customer lines terminate directly on the physical ports of the host node and the scope of the customer VLANs is local to the operator that provides their service. As shown in Figure 4 and Figure 5, two VLANs numbered ("101") are present, related to customers handled by different VNOs (VNO1 and VNO3 respectively) on different access node ports.

There are two scenarios with regard to how a VNO may treat the bandwidth allocated to their Virtual Access Network:

- A VNO may care only about the available aggregate bandwidth within their Virtual Access Network. This aggregate bandwidth must meet the Service Level Agreement between the InP and VNO, but performance of individual flows within the aggregate is uncontrolled
- A VNO may define their own forwarding policies for traffic delivery of their services. This forwarding mechanism may require support from the InP in the form of traffic management functions

In the current access networks, traffic is forwarded based on VLAN ID, MAC address or IP address and the three priority bits (PCP) are used to give some traffic higher priority.
In Figure 6 three VNOs share the same physical AN. Each VNO has some user ports connected to its subscribers. The number of ports and bandwidth requirements are laid down, through agreements between the VNO and InP. They need mechanisms to ensure these agreements can be honored.

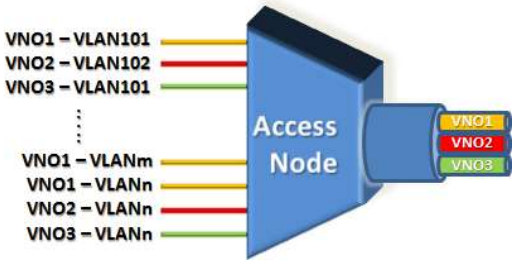


Figure 6 – FANS Interface Sharing

4.3 Network and User Interfaces

As shown in the Figure 3, the Ethernet network infrastructure on which FANS is based, spreads from the A10 (ENNI-L2) reference point to the U/U1 reference point. Briefly:

- A10 (or ENNI-L2) interface is the demarcation point between the access network and VNO network, it can also handle multiple QoS policies in support of different types of services. Note that in some cases A10 is placed at an Access Node, in which case it is also the V/Va reference point.
- U/U1 is located at the subscriber premise between the Access Node and the residential or routing gateway for residential or business services.

4.4 Deployment Models

Nowadays, the interconnectivity between a VNO network and the InP infrastructure can be defined at different levels, using different technologies:

- at AN (Ethernet)
- at Local PoP (Ethernet)
- at Regional PoP (Ethernet or IP, with the latter not in FANS scope)
- at National PoP (IP, not in FANS scope)

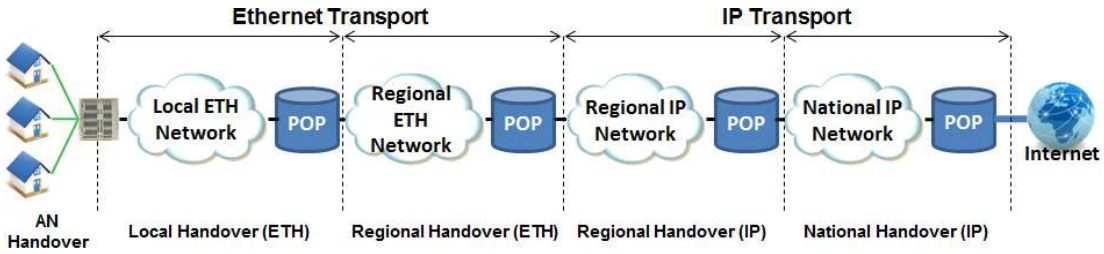


Figure 7 – Interconnectivity Reference Architecture

Figure 7 shows that the Ethernet interconnectivity is typically at Local or Regional level, while IP interconnectivity is typically at Regional or National level. FANS will only specify the following interconnectivity:

- At Regional level, there are distributed interconnection points at a number of regional nodes which act as aggregation points for all VNOs' Virtual Access Networks within a regional geographic area.
- Local level interconnect enables the InP to collect the aggregated traffic of all VNOs directly at the Access Node. A nearby aggregation switch can also be used to groom/distribute traffic of all VNOs to the connected single-homed Access Nodes (i.e supporting a single network interface) otherwise this type of interconnect requires to dedicate to each VNO a network interface of multi-homed ANs.

Figure 8 shows the reference architecture of a VNO, including the protocol stacks.
The interconnectivity between VNO and InP networks is defined at the External Network to Network Interfaces (E-NNIs). E-NNI is intended to support the extension of Ethernet services across multiple Operators, and the TR-178 [3] standard defines A10 and V as reference points for these interfaces, as shown in Figure 9.

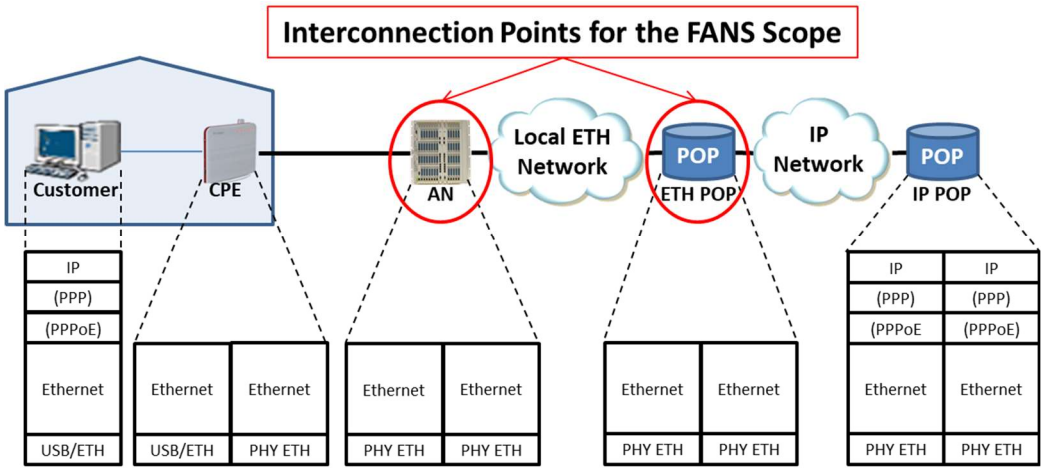


Figure 8 – Reference Architecture and Protocol Stack
Note: PPP/PPPoE are optional

Access networks may have different types of physical interfaces at the customer premises. Within the FANS context, fibre access technologies (FTTx) are considered and, for instance, where the Network Termination (NT) is tightly coupled to the access network (e.g., GPON), a deployment of a L2 NT in addition to a CPE can be required.

In general, in FTTx the distribution point varies with the legacy hardware and the topology of sites, leading to a variety of scenarios. Deployment options are also dependent on the physical layout of the existing infrastructure.

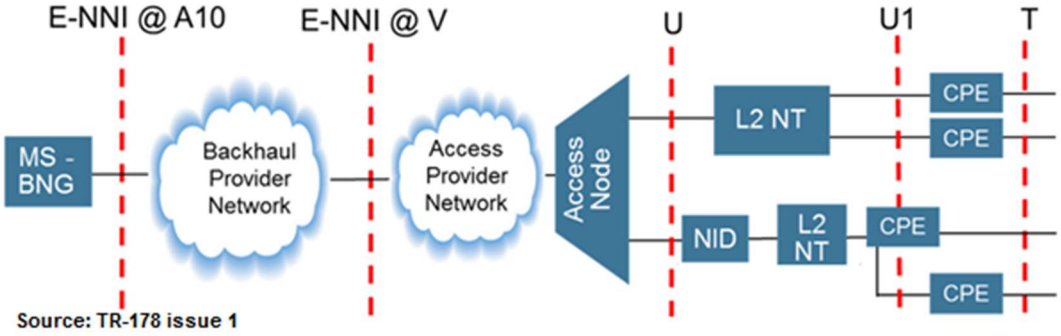


Figure 9 – L2 NSP Wholesale Model (TR-178 [3])

Two main interconnection options are considered for a virtual Access Node (vAN) model in FANS:

- **PoP/Aggregation** – vAN is deployed in a Point of Presence or equivalent facility, and where potentially several thousands of optical fibres cables are terminated
- **Remote** – vAN is deployed in a data centre within the Ethernet Access Network

In the remote deployment model, it is important to choose the correct location for the vAN, in terms of distance from the customer location. The maximum distance depends on the network performance requirements and SLAs. Typically, a remote option needs an excellent Quality of Service including low latency.

4.5 QoS / bandwidth allocation models

The FANS architecture enables VNOs to share the same physical network infrastructure. This includes sharing of the access links between the access node and the customer premises and the backhaul links within the broadband access network. Therefore the VNOs need to agree the allocation of capacity on these shared links with the InP.

Broadband internet services are typically offered with a high peak-to-mean bandwidth requirement. For example, consider a Fiber-to-the-Premises service marketed as 1 Gbit/s downstream and delivered over GPON infrastructure. Owing to statistical multiplexing, this service may be delivered with capacity overprovisioned both on the PON and on the backhaul. However, the service would also need to be able to burst to 1 Gbit/s on demand from the customer to deliver the marketed service.

Within the FANS architecture this service could be delivered in a number of ways:

- **Strict bandwidth partitioning**

  The Centralised Management System or Access SDN Manager & Controller reserves at least 1 Gigabit/s for the VNO on each network segment traversed by the customer service. This has the benefit that all traffic management can be performed within the VNO domain (including in stand-alone VNFs). However, it may result in significant stranded capacity within the access network.

  The stranding of capacity may be limited within the backhaul network. Provided that all VNOs are operating at scale (so the sum of peak average bandwidth per subscriber is in excess of the peak product rate) provisioning strict capacity backhaul circuits for each VNO may be an effective way to keep the management of QoS within the VNO's control.

Strict partitioning raises scalability issues on the GPON access segment which may need to serve up to 64 premises with a total downstream capacity of only 2.5Gbit/s. In practice this means that if service rates exceed 100Mbit/s downstream, VNOs must be offered some form of statistical access to the total capacity on the PON.

- **Flexible bandwidth allocation between VNOs**

  This is expected to be the more common model of deployment across an access segment (e.g. PON, FTTx backhaul to a CO). Capacity is allocated to the VNOs depending on both a Committed Information Rate and Excess Information Rate. These information rates could be overbooked as part of the Service Level Agreements between the InP and VNO. If the shared link becomes congested, traffic management entities within the InP infrastructure manage the scheduling of traffic onto the link. The VNOs could mark traffic with classes of service and drop-precedence to influence this scheduling behaviour.

Obviously, the latter approach is the preferred one as it is more efficient and it avoids waste of bandwidth, but it introducing some challenges in managing the bandwidth in a proper way in order to avoid malicious behaviours. The technology in this area is improving and today multi-layer Hierarchical Schedulers can be a valid approach to solve this issue. In [27] a 3-levels Hierarchical Scheduler is described and an example is shown in Figure 10. Other methods can be also used. The architecture of the three-stage hierarchical scheduler uses a combination of SP, WRR, WFQ and trTCM functions in each of the level: service/customer, operator and port. The important stage is the second level, that is the operator level, because it is the one where the scheduler allocated in a fair way the bandwidth according to what each operator is paying for. So the scope of this stage is also to make sure that any excess capacity from a VNO is preferentially re-distributed across the ONTs belonging to the same VNO. In [27] the bandwidth allocated with this method is compared with simpler mechanisms only having one or two stage.

While this approach is applicable in all the switching elements and switching matrixes, it cannot be applied for the uplink in a PON environment. For solving this Annex B of TR-402 [26] suggests the usage of virtual DBA. This is really interesting each VNO to have its own scheduling and then all the requests are summarized by the Merging Engine, as shown in Figure 11. The virtual DBA generates the virtual bandwidth map (vBMap) for its PON slice and delivers it to the Merging Engine. For T-CONTs with strict latency and jitter requirements, this vBMap indicates the desired position for each slot allocation. In this way, the VNO obtains full control over the upstream capacity scheduling within each frame. The Merging Engine replaces the physical DBA layer and has two main tasks. Firstly, it relays queue status report messages (BufOcc or report frames) coming from the ONUs (from specific T-CONTs) towards the vOLT serving them. Secondly, it analyzes the virtual bandwidth maps (vBMaps) from all vDBAs, merging them into one physical bandwidth grant (PHY-BMap) sent to all ONUs.

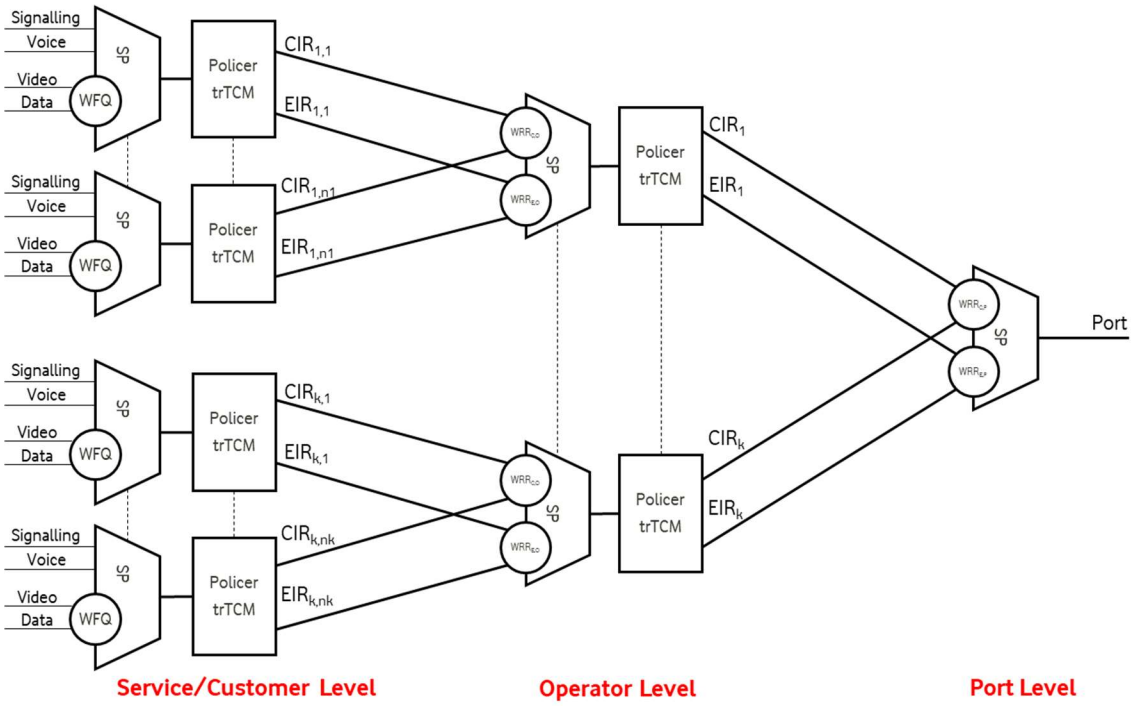


Figure 10 – 3-level Hierarchical Scheduler [27]

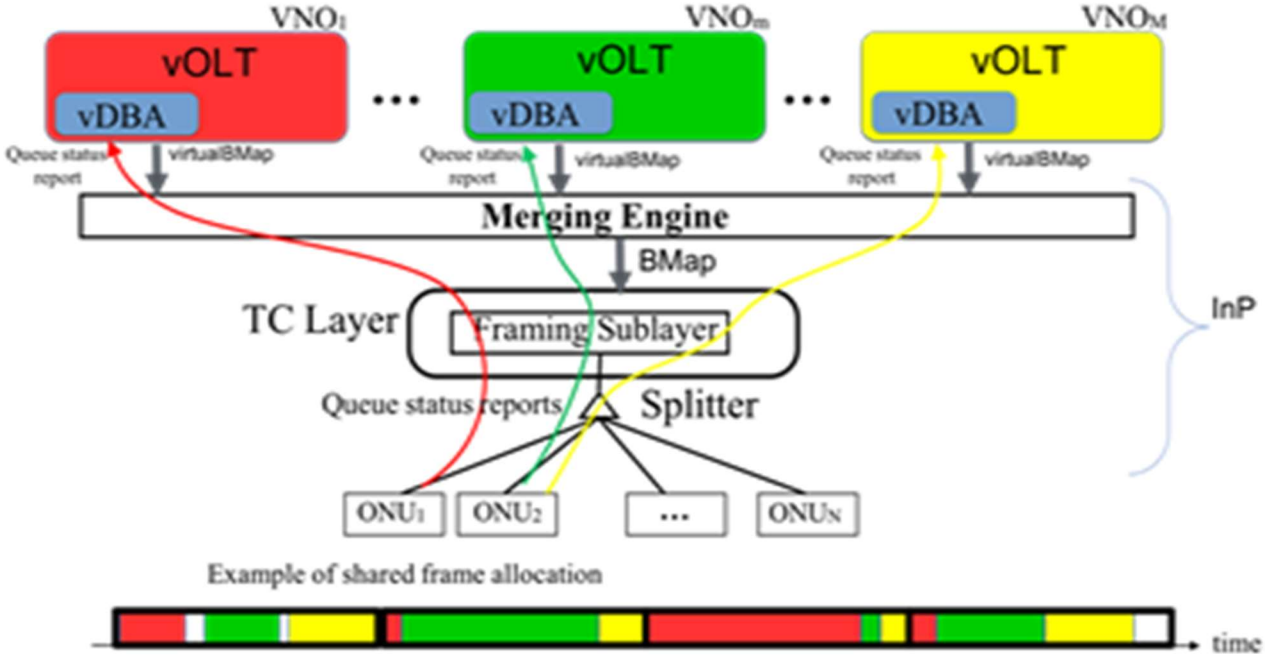


Figure 11 – Virtual DBA [26]

5 Sharing Models

In the following sections three models for resources sharing/slicing are discussed:

- Management System
- Virtual Node
- SDN-based

For all models, a management system enables multi-vendor support for the FANS scope. The main difference between these solutions is that the first and the third one can manage existing (legacy) as well as new network equipment via a centralised management system, while the second solution introduces Virtual Node instances of various operators to manage the multiple slices.
The Management System approach only manages the resources on behalf of VNOs, but the overall resources remain in common within the physical elements.
With the Virtual Node approach each physical element AN is sliced in multiple vAN instances which not only expose to VNOs management and control features but may also perform Data Plane functions and may be deployed either inside the physical AN itself or on an NFVI server.
The SDN-based approach relies on vAN instances which are Management and Control (M&C) Plane entities accessed by VNOs to manage their virtual network resources via the mediation of SDN M&C elements. The Data Planes of all VNOs' virtual access networks remain within the physical elements (i.e. the ANs and the aggregation switches/switch fabrics as shown in Figure 38).

5.1 Centralised Management System

This solution based on a Centralised Management System (CMS) performs the network slicing at the management system level.

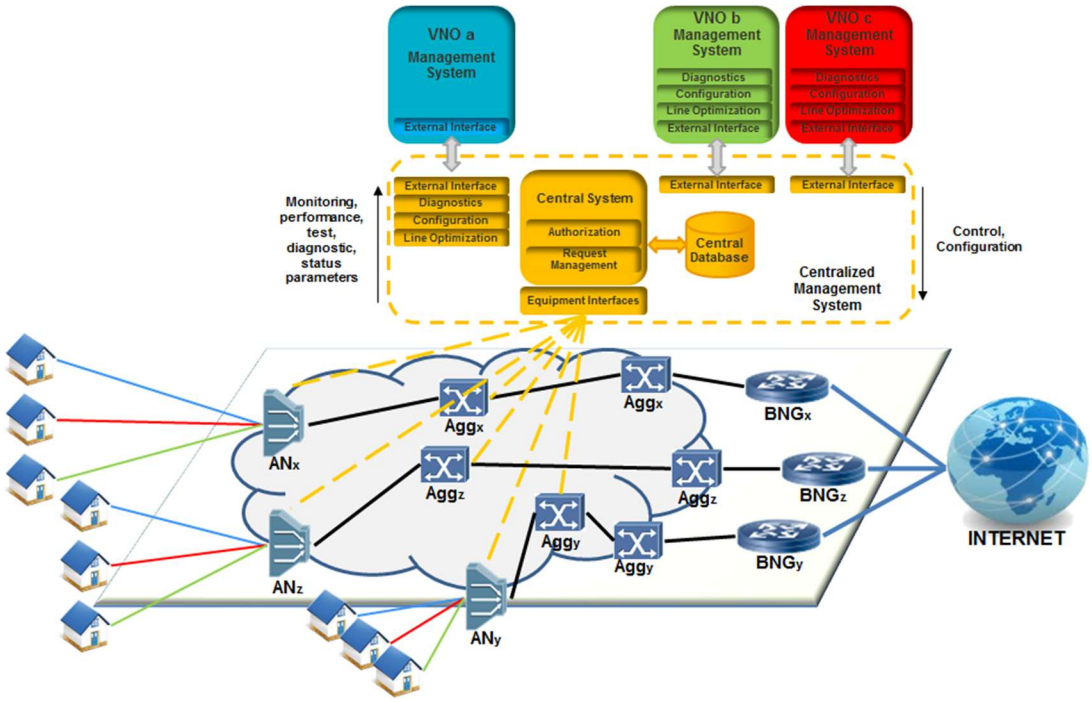


Figure 12 – Generic architecture for Centralised Management System sharing

5.1.1 Management System Sharing Architecture

The Centralised Management System abstracts the central sharing functionality, allowing a modular architecture of network resource management. The system can work with equipment from multiple vendors and it could be applied to both legacy and new types of network equipment. This allows FANS to operate in a provider-neutral and vendor-neutral manner that is capable of supporting multiple VNOs.
Management system sharing separates the management plane from the data plane, with sharing and network slicing performed by the management systems that support the management plane. All data plane functions, such as packet forwarding, continue to be performed in the network elements. Certain control plane functions may also be moved outside the network elements and be subject to sharing but they remain common across all VNOs. Each VNO can decide whether to use them or not.
In Figure 12, the Northbound Interfaces (NBIs) link the Centralised MS with VNOs management systems while Southbound Interfaces (SBIs) link it with network equipment. The “External Interface” to the VNOs should be a standardised interface.

A generic Centralised Management System solution model is depicted in Figure 13.

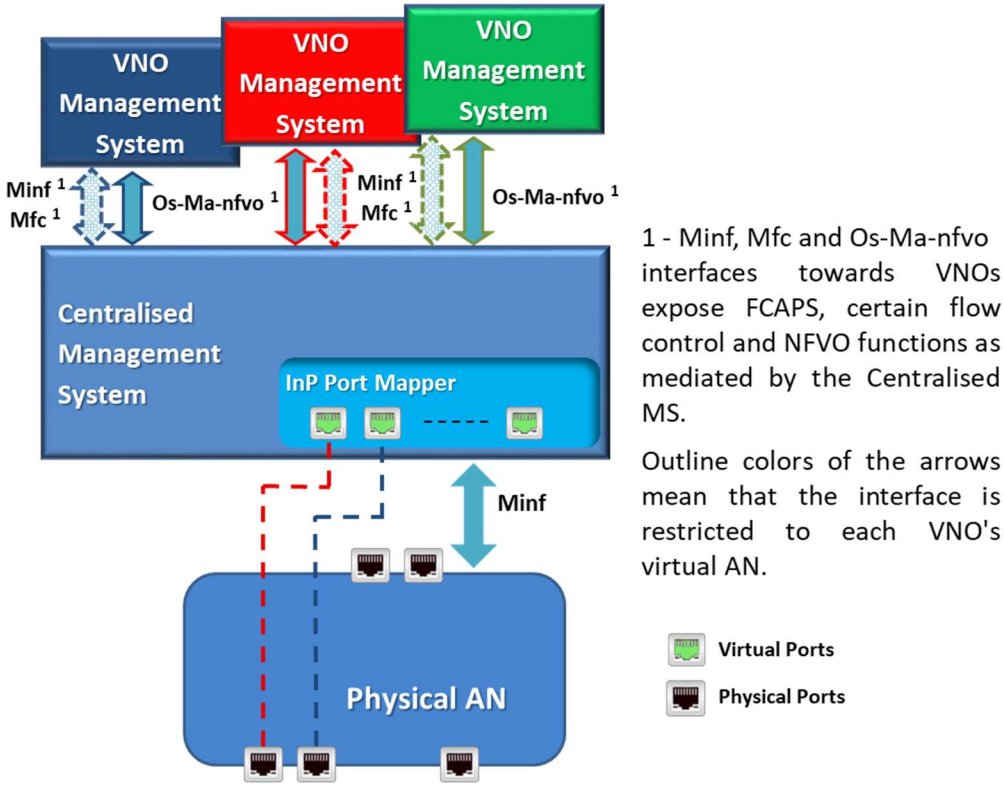


Figure 13 – Generic model for Centralised Management System

As shown in Figure 14, NBIs can be considered to connect to SBIs through an abstraction layer or an adaptation layer which converts signals on one side of the interface to equivalent signals on the other side of the interface. The abstraction or adaptation layer translates FANS transactions between the Southbound equipment interfaces and the Northbound interfaces to the VNOs. An abstraction layer hides the details of equipment interfaces to present a simplified interface toward management systems. An adaptation layer directly translates signals from one format to another format. Adapters can connect the various equipment interfaces on the SBI to the abstraction or adaptation layer. In this way, the NBI can provide data and services to VNOs that are independent of details of the actual equipment deployed.

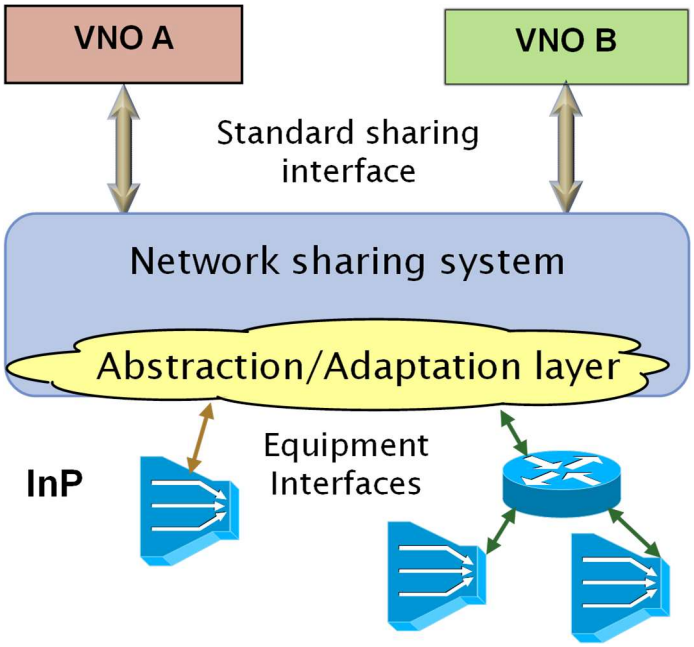


Figure 14 – Abstraction / adaptation layer concept.

Centralised data sharing could also be thought of as being implemented with the various parties writing to and reading from a logically centralised database. In this case all necessary management system functions are still in place, but the interfaces may resemble database read/write actions.
The Data Collection Function (DCF) [10] collects data from network elements. There may be a local DCF, or DCFs, located near the equipment and possibly within the InP domain, this can allow low-delay messaging and good scalability. In this case the data analysis functionality is centralised while data collection is distributed among the local data collectors. A local DCF separate from the management system would need a secure interface between itself and the management system; this interface could be standardised for FANS.
The transactions over the management-system based FANS NBI may either be simplified (coarse-grained) or parameter-level (fine-grained):

- **Simplified NBI transactions** can abstract both the data delivered to the VNOs into simpler summaries, and simplify the control transactions from VNOs into relatively simple “menu” choices or general indications of preferences such as profile selection. Data can be batched. Summaries of tests and diagnostics can be provided to the VNOs.
- **Parameter-level NBI transactions** simply relay requests for data and control to and from VNOs to the equipment, with little or no simplification or batching. There can be some combination of both simplified NBI transactions and parameter-level NBI transactions.

5.1.2 Centralised Management System

The Centralised MS covers and performs centralised functions, providing automated data from network elements (via Equipment Interfaces) to VNOs (via External Interfaces) for a centralised control and configuration of network elements.
As shown in Figure 12, within the Centralised MS there is an authorization engine and request management function to enforce policies and avoid potential conflicts or discrepancies in resource sharing or line settings among VNOs. A Centralised MS can provide for multi-tenancy, perform AAA functions, perform resource allocation and perform arbitrage between the various parties.
The Centralised MS may run some functions common to multiple operators’ lines such as line diagnostics and optimization, including multi-line diagnostics and optimization. Moreover, Centralised MS algorithms can determine some of the finer configuration details.

The management system is logically centralised and may be implemented in multiple physical devices consisting of distributed servers, cloud infrastructure, hosted service, etc.

5.1.3 Resource Management

Resource control allocates available resources such as network capacity, computing capacity and load balancing, and ensures that available resources are properly allocated.
For InPs, resources are generally network elements and network connections, including network interfaces, port assignments, VLAN assignments, internal network element bandwidth, network-facing bandwidth, access bandwidth, network-element internal computational capabilities, the size and frequency of admissible management messages, and the fiber or metallic facilities themselves as well as the management systems for these. Moreover, the resources of the Centralised MS itself may need to be controlled.
Current networks are constrained by limited network resources, and such constraints should be addressed when different VNOs share the same physical infrastructure. Thus, in the management system model, the services and resources should be agreed in advance between each VNO and the InP, in order to assure appropriate allocations. This agreement can be indicated by an exchange of parameters via shared and open interfaces.
VNO A is not allowed to access data about VNO B's lines and cannot control VNO B's lines. This allows VNO A to perform some control actions and line optimization operations on its lines, but it cannot perform any control on VNO B's lines. However, via the FANS-based centralised management system, functions including analysis and diagnostics may access data and perform some control actions on all the VNOs' lines.

5.1.4 Management System Sharing Functions

A single VNO may choose whether to use their own internal MS to support all or part of the MS functionality, or to rely on the Centralised MS or the SDN M&C (for further details see section 5.3) for supporting various functionalities which could be exposed to VNOs for their own slice, which includes the following:

- Security, which includes AAA:
  - Authentication to verify user credentials
  - Authorization to admit requests and limit access
  - Accounting to maintain transactional records for billing and other purposes (AAA)
- Virtual Node configuration
- Line optimization for its own lines, without impacting the performances of the lines of other VNOs
- Testing and gathering of diagnostic data
- Performance monitoring
- Assign bandwidth, VLAN tags and internal AN forwarding cross-connects per virtual port

VNO requests are appropriately subject to the resource brokerage and mediation of the Centralised Management System or the SDN M&C.

The following functionalities are under the InP responsibility:

- Network-element configuration
- Multi-line optimization across multiple VNOs
- Fault correlation, particularly for faults that occur on lines or equipment which impact multiple VNOs
- Maintain inventory, of the physical plant and equipment, as well as the virtual assignment of resources
- Maintain data needed to access VNOs and equipment
- Support an automated data clearinghouse that allows automated operations
- Provide data to assist VNOs with network planning and to assist in development of innovative services and differentiated services
- Assign and track port assignments on both the U-interface and V-interface sides of an AN

5.2 Virtual Node Sharing

5.2.1 Virtual Access Node

The Virtual Access Node model is based on the paradigm that physical access nodes (e.g., AN, ONU or OLT) in the access network can be partitioned by an InP into multiple virtual Access Nodes (vANs), where each vAN is associated with a VNO.
The virtual Access Node sharing solution provides Management and Control Plane functions similar to those of a physical AN (pAN) but in a virtual environment indicated as vAN. The solution is composed of a vAN entity for each VNO and this allows a separate management of the resources allocated to each VNO.
In the traditional architecture, the access node is capable of supporting one or more of the widely deployed access technologies and services as well as the newly emerging ones. The vAN can be applied to any PHY-layer technology. vANs can be deployed as virtual functions inside the physical AN, or on servers in InP datacentres, as shown in Figure 15.

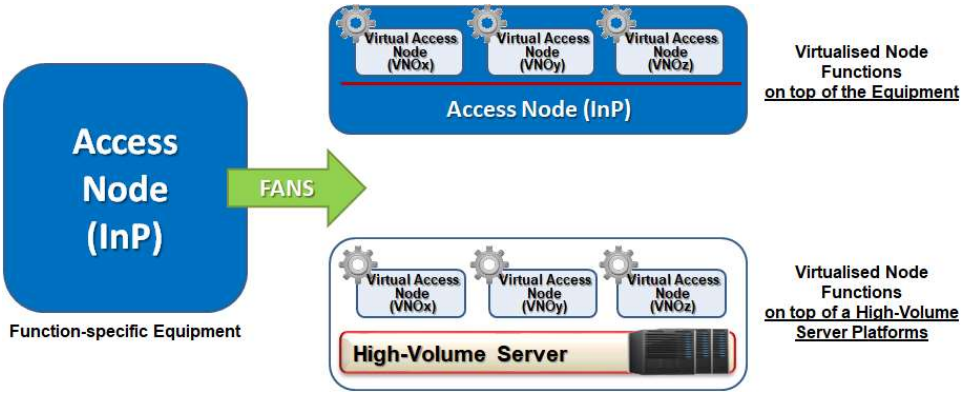


Figure 15 – Deployment scenarios for Virtual Access Node Functions

Note that using vAN instances also to handle data traffic, e.g. packets forwarding via software functions, may not be as performing as hardware based forwarding/switching at least at current state of the art of VNF technologies.
Furthermore when the vAN instances are deployed on the InP's NFVI servers, grooming multiple physical Access Nodes traffic towards Data Plane vANs can lead to bandwidth tromboning.
This is even more critical if the NFVI is not co-located with the physical ANs because the tromboned resource is inter-haul bandwidth.

The two options have the following differences:

- vAN embedded in access node: The vAN implementation is provided by the InP. VNO configures vAN functions using Minf interface.
- vAN running on NFVI: The vAN implementation can be provided by the InP or VNO can deploy vAN software on High-Volume Servers. The Physical AN to vAN interface is Ex-Nd.

As result of applying the Virtual Access Node model, each VNO sees only its virtual representation. Thus, the VNO can handle and provisioning its own virtual resources as it does in the traditional manner for the physical resources.
Like for the other sharing model the VNO Management System accesses to the network resources via the mediation, through the FANS API (Os-Ma-Nfvo), of the Centralised Management System.
Management and control requests issued by the VNOs, especially those that encompass resources allocation, require such Centralised Management System to apply resource brokerage and reconcile the requests from all the VNOs to guarantee that the FANS business framework is fulfilled. This business framework implies that:

a) all VNOs have a fair access to network resources per a FANS service framework collectively agreed among the InP and all the VNOs; this service framework may also incorporate provisions defined by the relevant Regulatory Authority and those players (e.g. for a regulated Wholesale offer)
b) each VNO have access to network resources consistently with the commercial SLA bilaterally agreed with the InP
c) each VNO can access only to the configuration and information related to its own virtual access network, and related customers and services

The Virtual Access Node solution model is depicted in Figure 16 (vAN in physical AN) and Figure 17 (vAN in NFVI server).

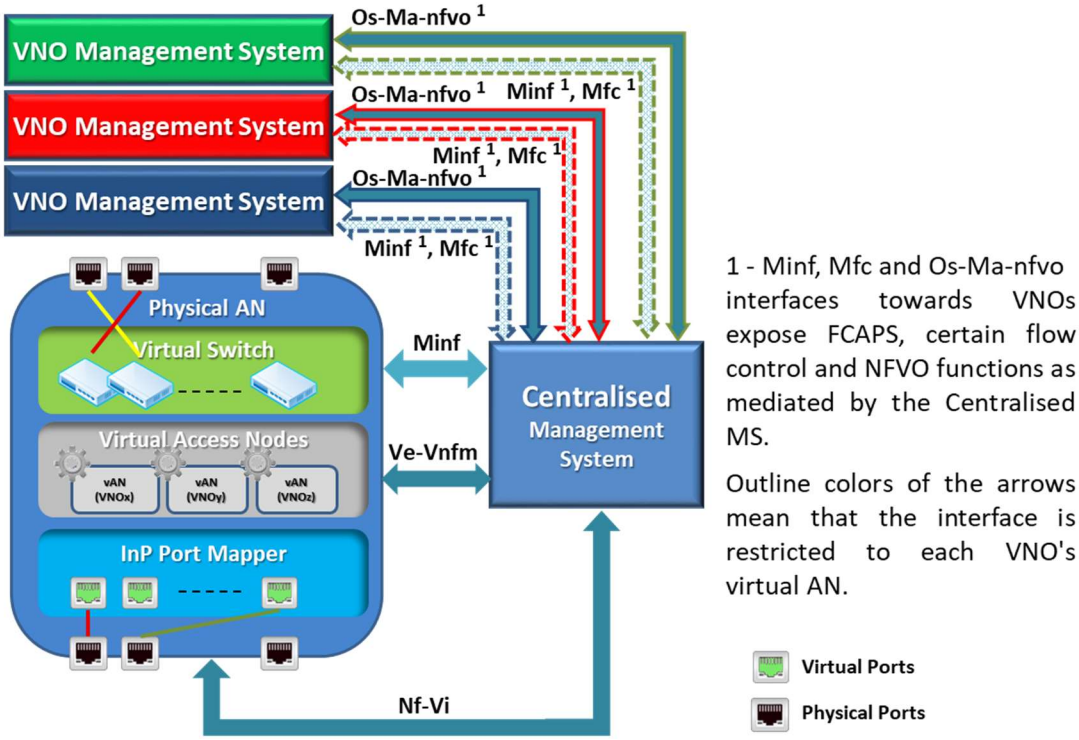


Figure 16 – Virtual Access Node Model (vAN in physical AN)

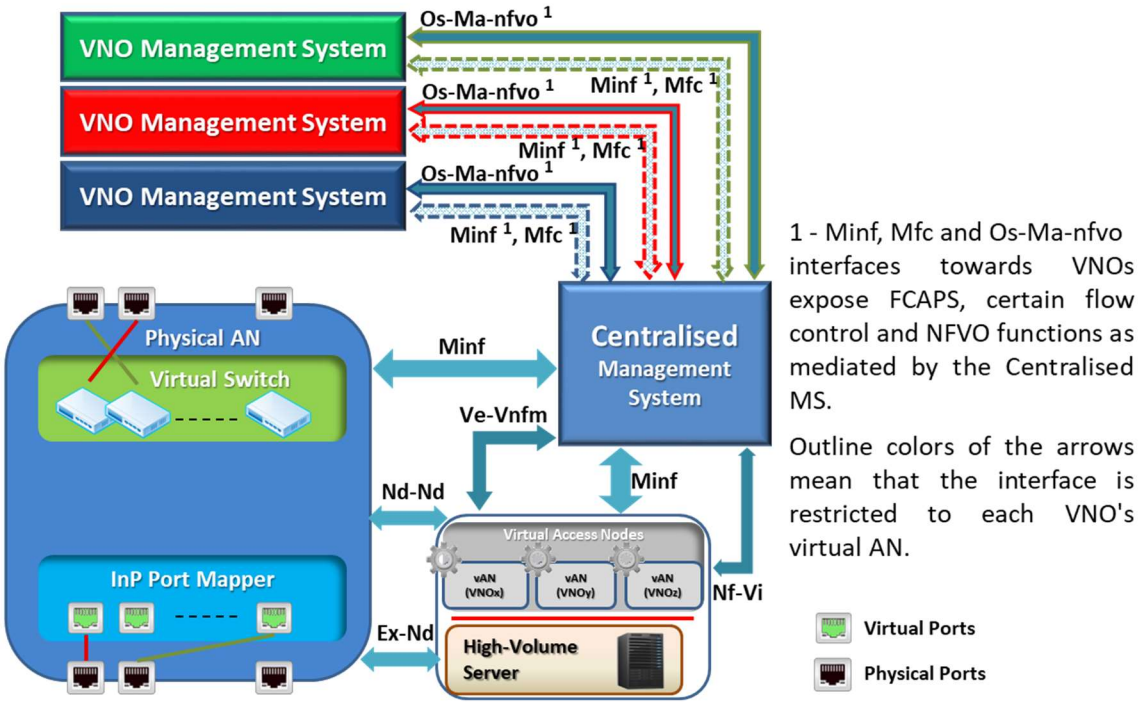


Figure 17 – Virtual Access Node Model (vAN in NFVI server)

As shown in the above Figure 16, the solution is composed of the following components:

- Virtual Switch
- Virtual Access Nodes (vANs) elements
- InP Port Mapper
- Centralised Management System (MS)
- VNO Management System
- Interfaces

A Virtual Switch is a component of a hypervisor. It is located on the top of physical access node and it is responsible for forwarding the customer traffic ensuring traffic isolation.
A virtual Access Node (vAN) element is a Telco Application that represents the whole set of characteristics of a physical Access Node except the NICs and other physical interfaces.
The InP Port Mapper is a virtual entity used to map logical ports to the host physical ports at the U/U1 interface. Detailed information on InP Port Mapper is given in section 5.2.3.
The Centralised Management System (MS) is the main component of the model. It optimizes and orchestrates services between the network and the cloud, as well as resources across the end-to-end infrastructure. Centralised MS allows configuring network connectivity and services based on optimization depending on the pattern of workload, simplifying configurations, and enabling rapid provisioning of networks.
Detailed information on Centralised Management System are described in section 6.3.
Figure 16 also shows the interconnections between the various elements of the solution. Even if the architecture is not exactly the ETSI NFV reference architecture, the interfaces used in the Virtual Access Node model uses the same functionalities and so they are applied at the following reference points:

- Os-Ma-nfvo
- Minf
- Ve-Vnfm
- Nf-Vi
- Nd-Nd
- Ex-Nd

These are the main interfaces representing the model. Other interfaces for managing the virtualised elements are described in section 6.2.
The VNO Management System is used to support various end-to-end telecommunication services. In general, it can be composed of Operations Support Systems (OSS) and Business Support Systems (BSS). An OSS covers at least the following five functions:

- Network management systems
- Service delivery
- Service fulfilment (including the network inventory, activation and provisioning)
- Service assurance
- Customer care

A BSS system usually support customer-facing activities, such as:

- Billing
- Order management
- Customer relationship management
- Call centre automation

The Os-Ma-nfvo reference point is at the interface between VNO Management Systems and the Centralised MS. VNO operators access the Management System service portal via a web-based GUI (which uses this reference point to communicate to the Centralised MS) to perform lifecycle operations on Virtual Access Nodes and transport circuits (e.g. O-VLANS), such as instantiate, terminate, query, etc.
Minf reference point is used by the Centralised Management Systems to communicate with the physical node and the virtual node for FCAPS functionalities (e.g. service parameters).
Mfc reference point is used by the Centralised Management Systems to communicate with the physical node and the virtual node for flow control (e.g. forward table configuration).
Ve-Vnfm reference point is used to manage and perform lifecycle operations on vAN elements passing via the Centralised MS.
Nf-Vi reference point is used to manage the physical resources, networking resources and the hypervisor-accessed resources (e.g., compute, storage and networking, including InP Port Mapper and Virtual Switch).
The Nd-Nd reference point supports connectivity between vANs instances over multiple geographically separated sites.
The Ex-Nd reference point allows vANs to connect to physical Access Nodes.
The Virtual Switch and InP Port Mapper functions implement the slicing system in the Virtual Access Node model.

One possible implementation of Virtual Access Node based FANS is described in CLOUDCO-APPN-006 [28].

5.2.1.1 An Example Procedure of Virtual Access Node Abstraction

A vAN can be abstracted at the time the VNO asks to lease the infrastructure access network. In this case, the InP implements the abstraction according to specific requirements from the VNO, including the virtual resources for the vAN, such as the virtual ports, network functions, etc. After the deployment, users on the related physical AN who belong to this VNO can access the network through the already created vAN.

Alternatively, it is possible to allocate resources for the Virtual Access Network on-demand.
Figure 18 shows the automated vAN abstraction in the FANS environment.

In this case, the virtual resources of the vAN are not assigned at first. When users of the VNO order service, the VNO instantiates the service deployment and communicates with the centralised management system via shared and open interfaces. Some of the configuration parameters related to the vAN can be generated by the management and control system, which include the description of the mapping relationship of the physical port ID and the virtual port ID, as well as the virtual resources and customer line parameters required to support the user's services. The virtual resources include at least one of the following:

- Virtual ports (user side ports or network side ports)
- Network functions

- Service functions or service function chain

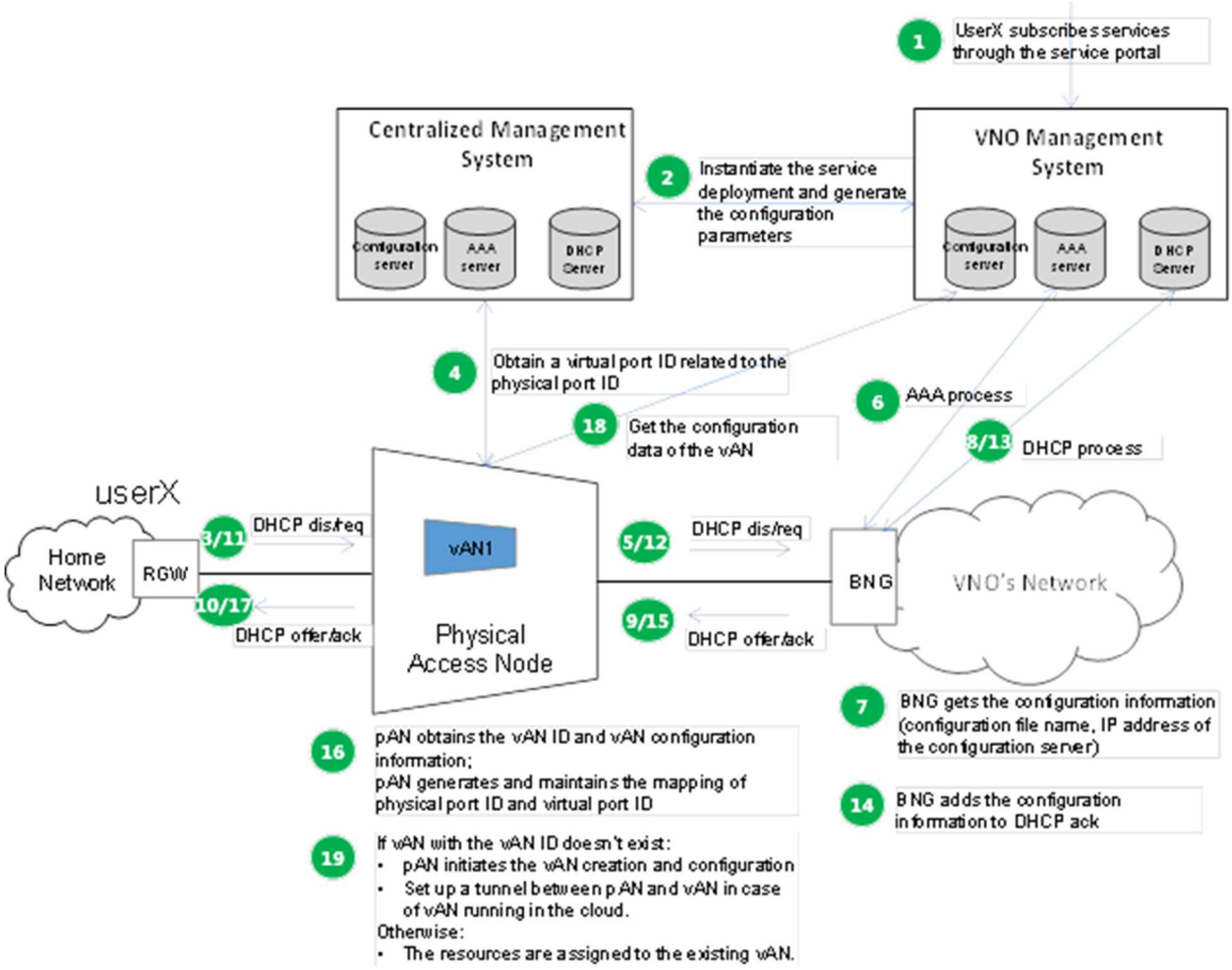


Figure 18 – vAN Automated Abstraction

When receiving the DHCP packet sent by the user, the physical AN gets a virtual port ID according to the physical port which the user is connected to, by looking up the mapping relationship of the physical port ID and the virtual port ID generated previously. This virtual port ID will be used in the VNO's network. The physical AN forwards the DHCP packets with the virtual port ID to the BNG in the VNO's network. After successful authentication, the BNG can get the configuration information of the vAN, which consists of the configuration file name and the IP address of the configuration server. Once the user's IP address is allocated, the BNG adds the configuration information to the DHCP packet and sends it back to the physical AN. The physical AN acquires the vAN ID based on the virtual port ID, and requests the configuration data of the vAN from the configuration server with the configuration information obtained. If the vAN has not been instantiated yet for the VNO, the physical AN will initiate the vAN creation with the virtual resources allocated and the customer line configured. Otherwise, the virtual resources and the customer line parameters will be assigned to an existing vAN.

Note that the vAN created may reside inside the physical AN, or run in the datacentre/cloud. In the latter case, a tunnel between the physical AN and the vAN will also be setup at the same time.

The mapping between the physical port ID and the virtual port ID obtained above is then maintained by the InP Port Mapper.

The detailed message flow is depicted in Figure 19. The procedure is depicted regarding the vAN deployed as virtual function inside the physical AN. In case of vAN deployed in external data server, it is the DHCP VNF implementing the DHCP process.

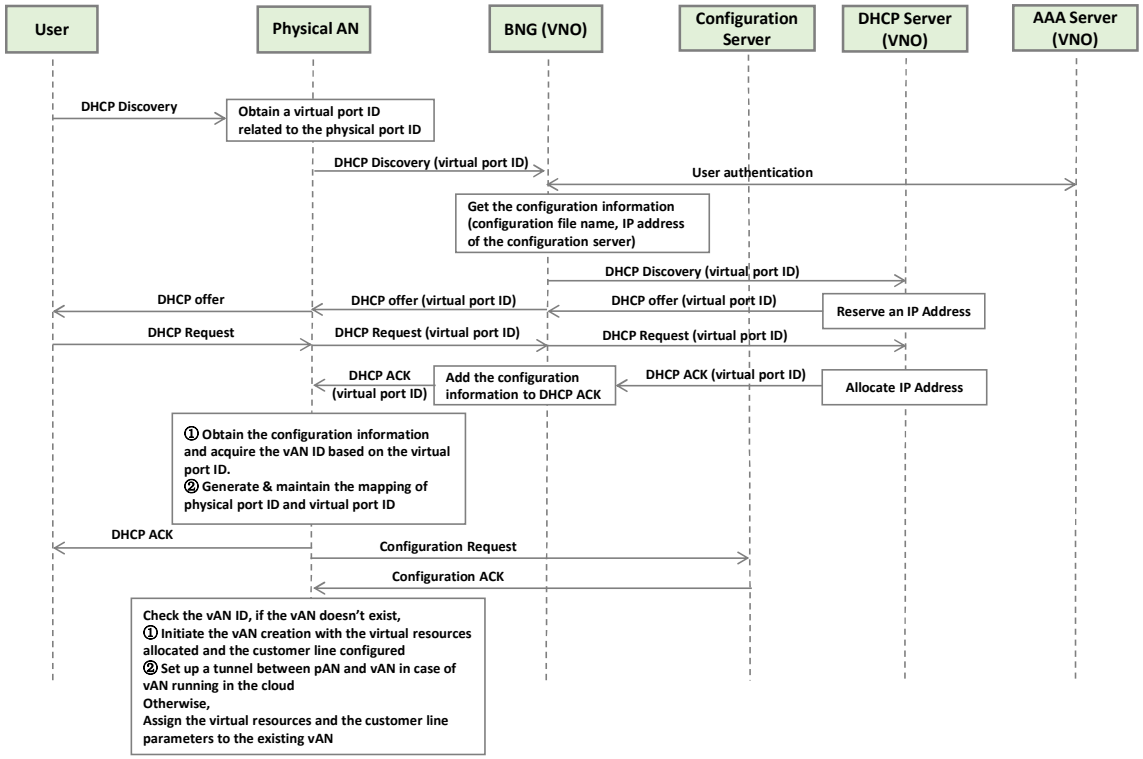


Figure 19 – Detailed Message Flow for the vAN Automated Abstraction

Since the resources are allocated to the vAN only when required and most static resource allocations are avoided, costs can be reduced.

5.2.2 Virtual Aggregation Node

The Aggregation Node (AggN) aggregates traffic from multiple Access Nodes (AN) in the fixed aggregation network.

There may be multiple layers of traffic aggregation. For instance, an Access Node may connect to a Central office terminal which in turn connects to an Ethernet Aggregation Switch, or multiple levels of Ethernet aggregation switches can exist.

The "Aggregation" function of the AggN can be implemented in one or more Virtual Network Functions (similarly to the virtual Access Node) in other physical node(s), or it can be logically implemented in the Central Office, as shown in Figure 21.

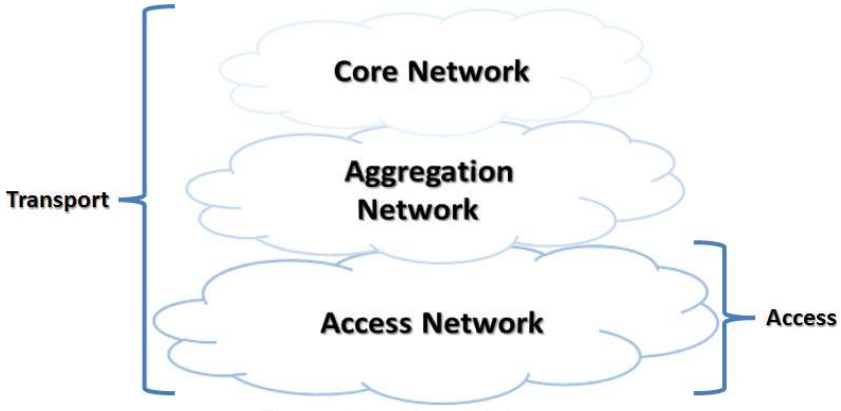


Figure 20 – Network Layers

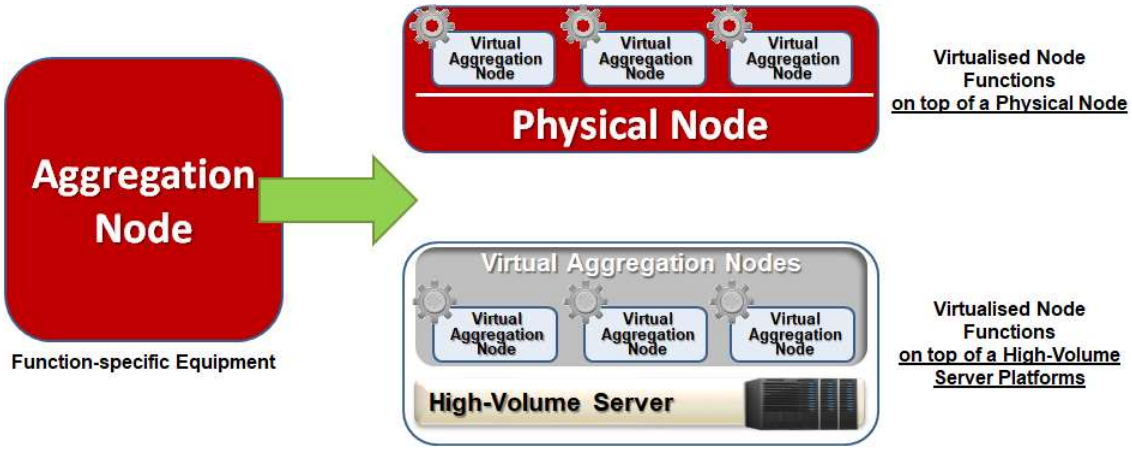


Figure 21 – Deployment scenarios for Virtual Aggregation Node Functions

Note that Traffic Engineering (TE) capability, in virtual Aggregation Nodes is based on Operator VLAN (O-VLAN), MPLS identifiers or VXLAN tunnel as described in section 5.2.6.

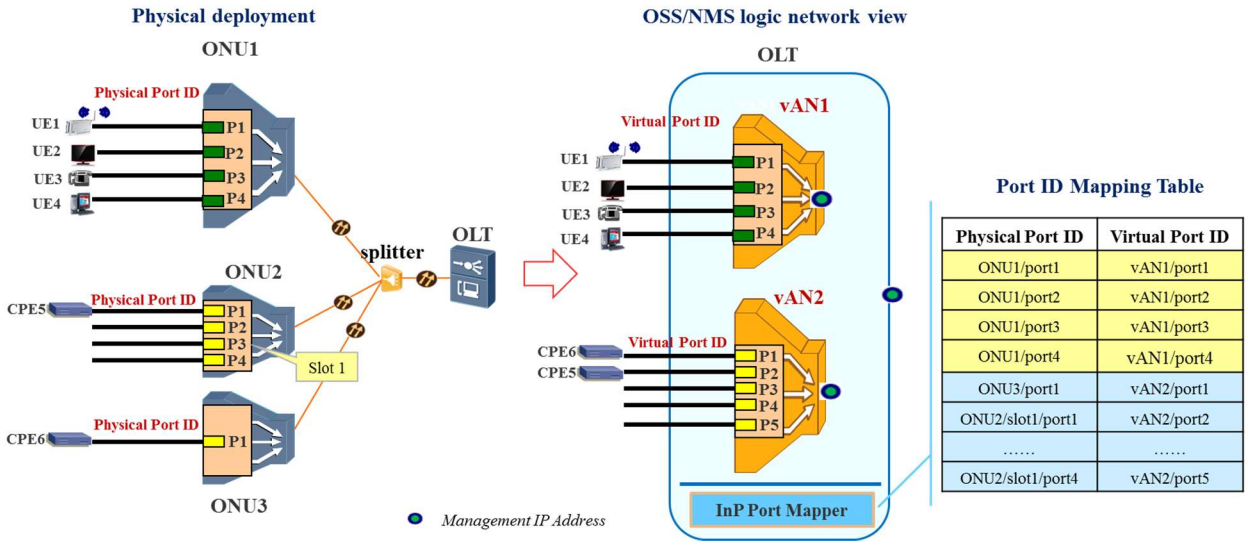
The virtual Aggregation Node (vAggN) element is technology agnostic and provides similar functions to those of a physical AggN but in a virtual environment. Its control function is provided by a logically centralised controller in the Centralised MS. In general, some node-related features can be implemented via a set of Virtual Network Functions (VNFs), such as:

- Ethernet bridging
- IPv4 and IPv6 routing
- Seamless MPLS
- MPLS and multicast forwarding
- Class of Service (CoS)
- OAM and network resiliency
- IEEE 1588v2 Precision Timing Protocol (PTP) [11]

5.2.3 InP Port Mapper

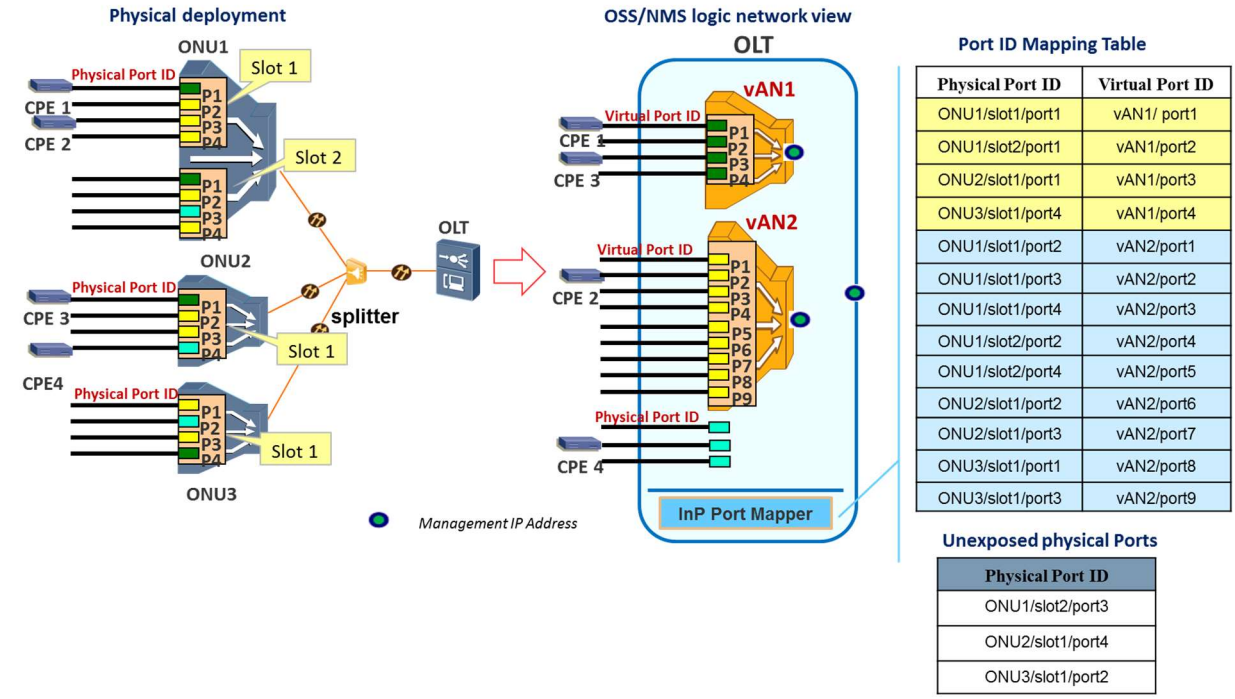
In the FANS scenario, physical nodes (e.g., DSLAM, ONU or OLT) in the access network can be abstracted by an InP into multiple virtual Access Nodes (vANs). As mentioned, vAN is a logical entity that represents a physical access node or part thereof, together with its virtual ports, which are mapped to physical customer ports. The virtual ports are identified through virtual port IDs.

The mapping between physical ports and virtual ports is maintained by an InP Port Mapper, managed by the Centralised MS. This mapping functionality managed by InP Port Mapper converts a physical port of the access node in the received control packets that include port information (e.g., DHCP, PPPoE) to a virtual port related to the vAN, and also converts a virtual port identity in the received control packets (e.g., DHCP, PPPoE) to a physical port of the access node. Two scenarios can be identified when abstracting the AN:



Physical Port ID	Virtual Port ID
ONU1/port1	vAN1/port1
ONU1/port2	vAN1/port2
ONU1/port3	vAN1/port3
ONU1/port4	vAN1/port4
ONU3/port1	vAN2/port1
ONU2/slot1/port1	vAN2/port2
……	……
ONU2/slot1/port4	vAN2/port5

Figure 22 – InP Port Mapper for Dedicated ONU



Physical Port ID	Virtual Port ID
ONU1/slot1/port1	vAN1/ port1
ONU1/slot2/port1	vAN1/port2
ONU2/slot1/port1	vAN1/port3
ONU3/slot1/port4	vAN1/port4
ONU1/slot1/port2	vAN2/port1
ONU1/slot1/port3	vAN2/port2
ONU1/slot1/port4	vAN2/port3
ONU1/slot2/port2	vAN2/port4
ONU1/slot2/port4	vAN2/port5
ONU2/slot1/port2	vAN2/port6
ONU2/slot1/port3	vAN2/port7
ONU3/slot1/port1	vAN2/port8
ONU3/slot1/port3	vAN2/port9

Physical Port ID
ONU1/slot2/port3
ONU2/slot1/port4
ONU3/slot1/port2

Figure 23 – InP Port Mapper for Shared ONU

Dedicated ONU – all the ONU logical/physical ports are assigned to a single VNO
Shared ONU – ONU logical/physical ports are assigned to different VNOs

Note that some physical ports of the ONU can be hidden. The following Figure 22 and Figure 23 show the configuration table of InP Port Mapper for the two scenarios.

In case of the Dedicated ONU, all the physical ports owned by a single VNO can be grouped and exposed as a single entity by exposing the GEM logical ports as virtual ports.
For both cases, the vAN has visibility of those virtual ports assigned to it.
In essence, the InP Port Mapper is a mapping table. The case of customer migrations between different VNOs terminating on the same physical access node is shown in Figure 24.

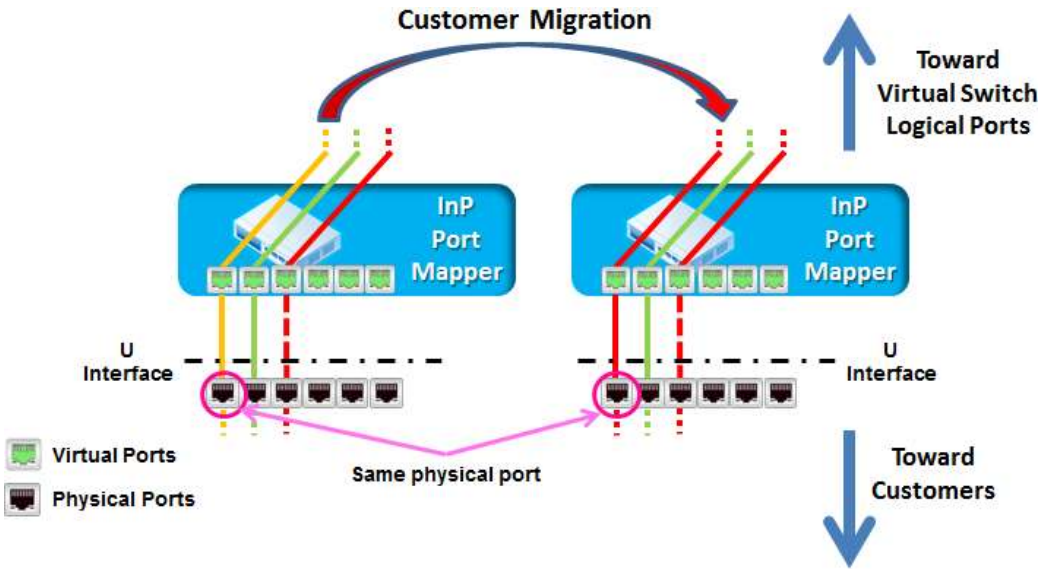


Figure 24 – Customer Migration in FANS

The customer is a subscriber to services (represented by the yellow line) of VNOx, but needs to migrate these services to VNOy. Where the migration leaves the customer on the same physical AN, there is no need for manual intervention on that AN, just a simple change in the mapping between virtual and physical ports. The physical port which the customer is connected to remains the same after the migration.

Virtual Port state information is a convenient way of providing O&M status to the VNO. Providing a set of retrievable states, allows the VNO to manage virtual ports with regard to deployment, migration and trouble-shooting.
The InP Port Mapper establishes the relationship between physical ports of an Access Node and the virtual ports of a vAN. Virtual ports represent a group of physical InP ports to which customers are connected, and this mapping is retrievable by the Centralised MS. The Centralised MS is in charge of virtual port state management when the VNO leases resources from InPs.
The VNO monitors and administrates virtual port state for most operations. When trouble-shooting network problems, the status message records and correlation between vAN virtual port and InP physical port may help to locate the problem.
The Port State of a virtual port is retrievable and settable by the Centralised MS. The following states represent the physical link connection of the port, port operational and administrative state exists when several states are valid simultaneously.

Port State:

- LINKUP –physical port has no alarm/defect, which implies the link connection is good.
- LINKDOWN –physical port has alarm/defect, which implies the link connection has failed.
- PORTUP – port is administratively up. This is the default state when a port is added, and it transits to the LINKUP/LINKDOWN/PORTDOWN state after system power-up.
- PORTDOWN – follows the LINKUP/LINKDOWN/PORTUP when port is administratively down.

The Port Status of a virtual port is transient and reported as event message which is retrievable on Centralised MS.

Port Actions:

- ADD – Add a virtual port to a given vAN.
- DELETE – Delete a virtual port from a given vAN.
- MODIFY – Bring virtual port administratively up or down.

The following Figure 25 demonstrates the virtual port state machine and associated status.

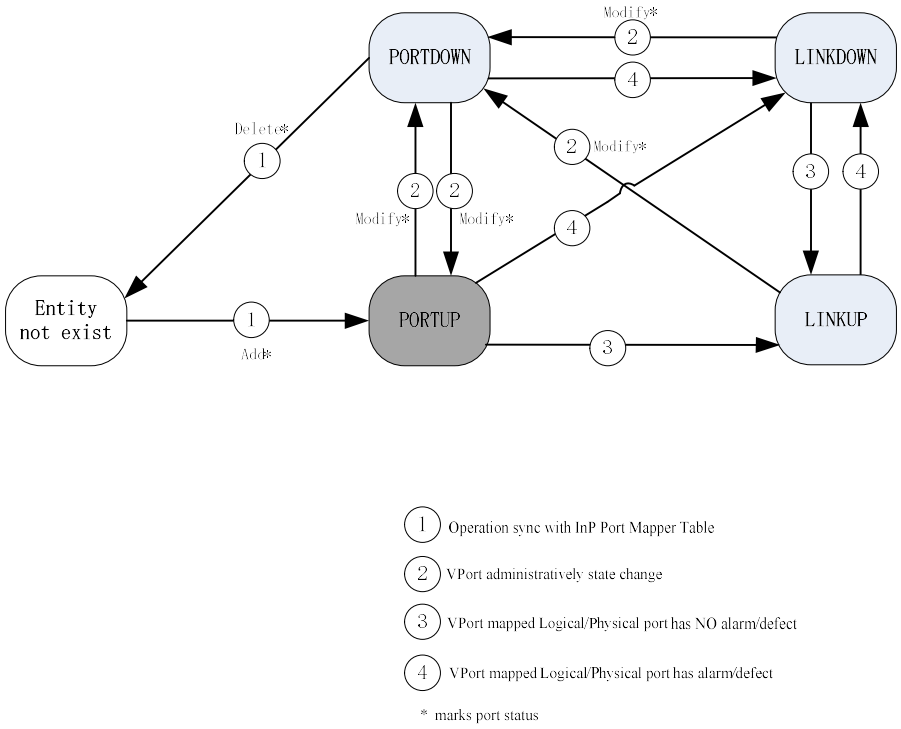


Figure 25 – Virtual Port State Machine

Figure 26 demonstrates an example of customer migration that includes a virtual port state transitions and associated status in the case of a physical port released by a VNO and then leased by another VNO. The InP physical port “A” was leased to VNO1 (yellow) as VPort1, this network resource is then reallocated to VNO3 (red) as VPort20.

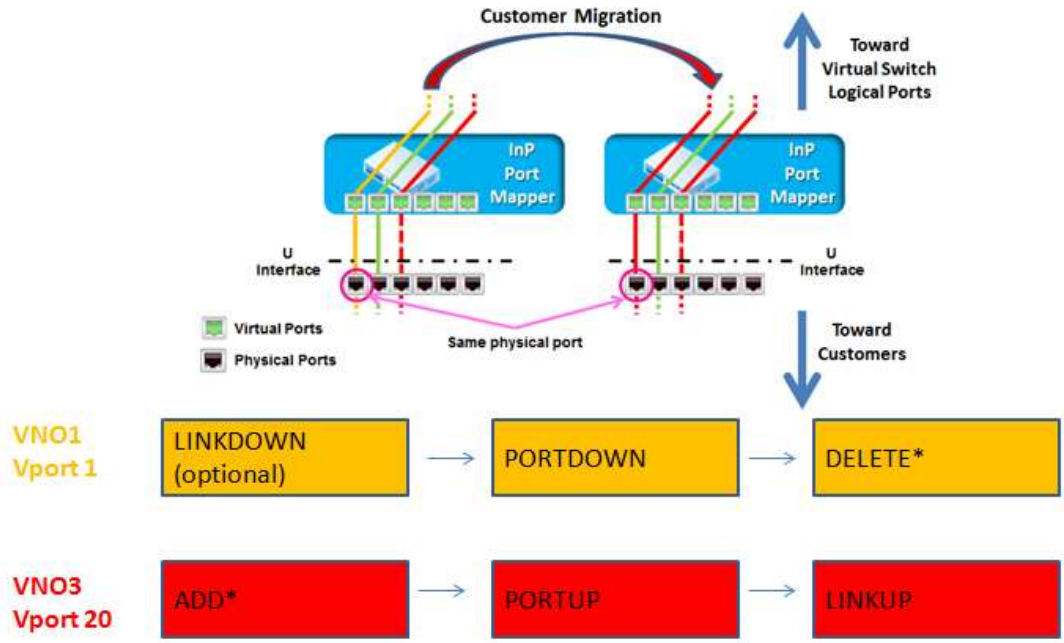


Figure 26 – Virtual Port State/Status of Customer Migration in FANS

During the customer migration, VNO1 needs take down virtual port1 in VNO1's management system, and release the virtual port by deleting it from VNO1. VNO3 maps physical port "A" to VNO3's management system as VPort20, takes the port up administratively, and then VPort20 appears as LINKUP or LINKDOWN depending on the condition of link connection. Note that these migrations should synchronize with InP Port Mapper table operation, and vice versa.

Figure 27 shows another case where a given VNO detects MAC spoofing and prompt action is taken to block this traffic by putting the virtual port VPort1 into Linkdown State.

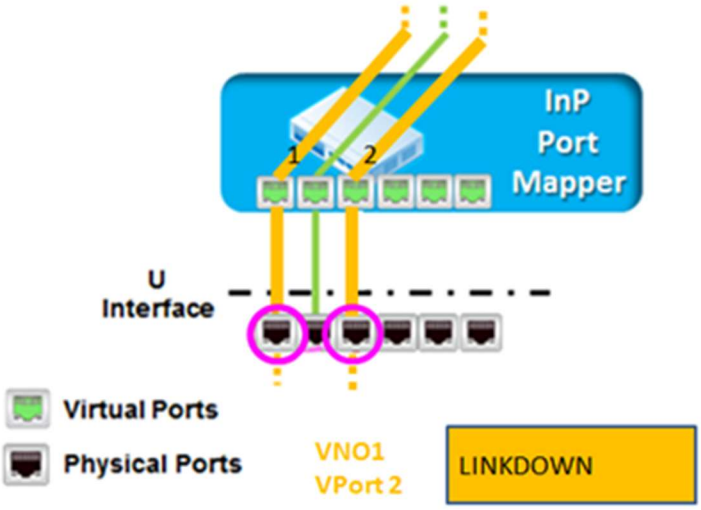


Figure 27 – VNO Block Traffic when MAC Spoofing is Identified

In this case, the VNO detects that data from VPort1 and VPort2 has the same MAC address.
As per the subscriber and VNO contract, only VPort1 is legitimately associated with a given MAC. The VNO blocks the data from VPort2 immediately and modifies the VNO MAC learning process accordingly so the port in not re-enabled.

5.2.4 Access Network Function as a Service

A vAN and its virtual ports can be deployed and maintained by an InP who implements the access network abstraction and slicing. Physical nodes in the access network can be combined or segregated to form different vANs. As part of ensuring network isolation, VNOs can control and manage their own vAN instances and virtual port IDs.

A vAN can be deployed as a single, complete AN virtual function or it can have a subset of access network functions (in control plane or data plane) to support different services as required by a given VNO. These functions are already defined in TR-101 [2], TR-178 [3], TR-156 [4], TR-167 [8] and TR-221 [9]. The granularity of the network function is flexible so that several functions can be combined as a service, as illustrated in Figure 28.

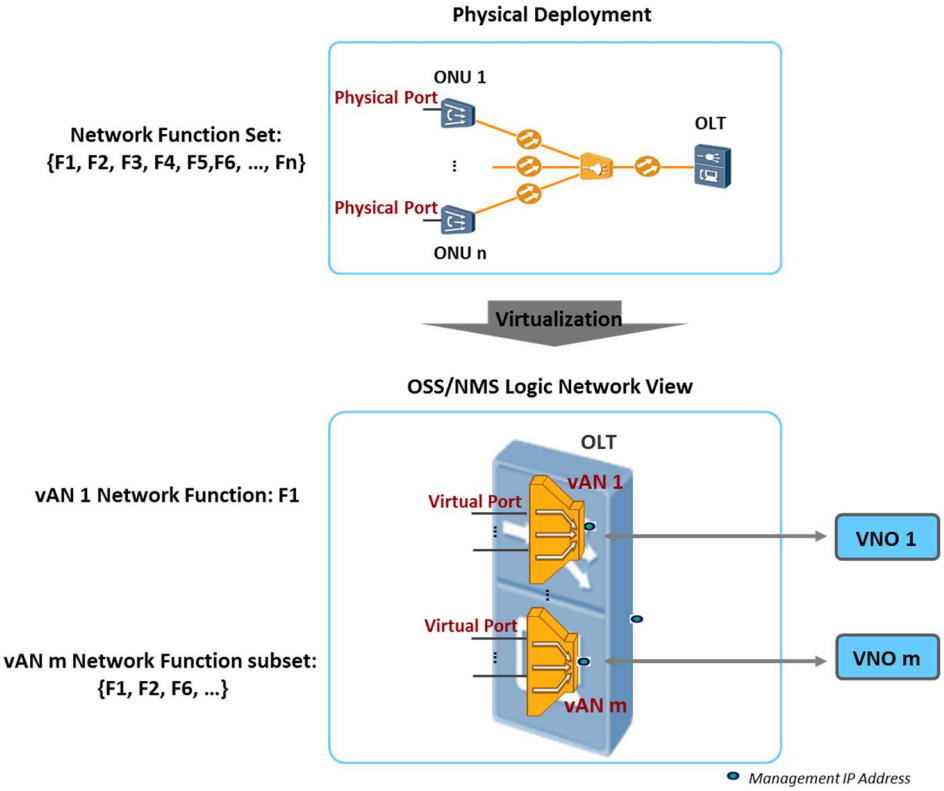


Figure 28 - Access Network Function Virtualisation and Allocation

As a further example, the vAN is abstracted based on the physical OLT/ONU combination. The requirements from VNOs are that VNO1 wants to deploy a mobile backhaul service and VNO2 a residential service, (supposing the InP's infrastructure has the capability to support these different requirements).
Based on the resources of the physical PON, InP will abstract one vAN which is vAN1 for VNO1, and another vAN which is vAN2 for VNO2.

In order to support the mobile backhaul service, InP will allocate one subset of network functions to vAN1 which includes clock synchronization, MPLS forwarding, and IP/MPLS signalling. For the residential service, InP will allocate another subset to the vAN2 which includes AAA authenticator/proxy, DHCP relay/proxy, IGMP proxy/snooping, flow classification and QoS mapping. The Optical Distribution Node (ODN) interface connects the OLT with one or more ONU/ONTs and packets arriving at the OLT will then be sent to the corresponding vAN for further protocol processing. The protocols that support the corresponding network function processing can be either instantiated on demand during vAN allocation or be pre-configured in the

physical nodes. With this solution, different services can be provisioned through different vANs, but based on the same physical infrastructure.

5.2.5 Relationship to ETSI NFV Architecture

Figure 29 shows how the ETSI NFV architecture can be leveraged to enable FANS for both existing and new deployments.

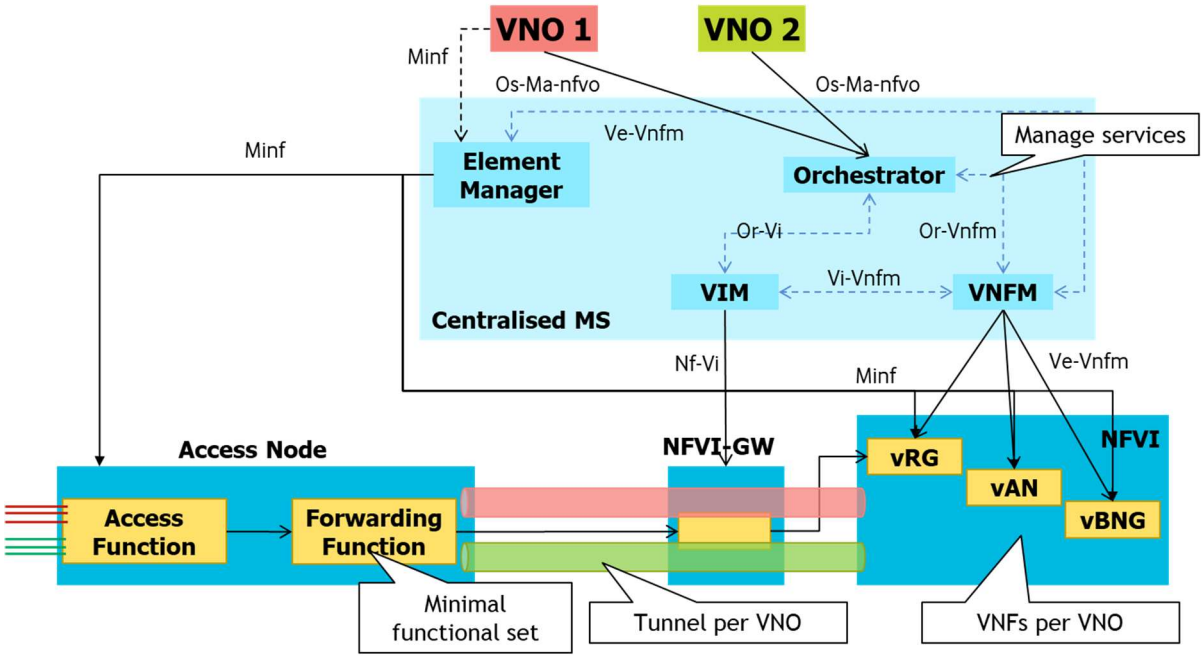


Figure 29 – Applicability of ETSI NFV architecture for Fixed Access Network Sharing

The vRG and vBNG are not required as part of Fixed Access Network Sharing architecture. However in the case where the RG and BNG are virtualised, the vRG and vBNG functions may reside in the same NFVI which also hosts vAN functions, or in an NFVI in the VNO domain.

As can be seen, several of the concepts in Figure 29 are aligned with the Virtual Access Node Model, outline in Figure 16/Section 5.2.1.

The Access Node is shown to consist of two functions:

- The **Access Function** provides physical layer access (e.g. terminating the G.fast interface) and framing, offering an Ethernet layer 2 service towards the Forwarding Function
- The **Forwarding Function** provides connectivity across the aggregation network, via the NFVI-GW into the NFVI where some Virtual Access Node functions may be hosted. These tunnels are instantiated per Virtual Network Operator (VNO) and carry the traffic of one or more access lines (e.g. one or more UNIs on a GPON ONT) towards the vAN in the NFVI.

The NFVI maintains a set of VNFs that implement the service model for each of the VNOs. These VNFs may include the existing vRG (NERG), but may also include other VNFs that implement some of the functions that traditionally reside in the Access Node and/or the Broadband Network Gateway. In general, one or more subscriber management related features can be moved into the NFVI and implemented via a set of VNFs.

The management layer for this FANS model is based on ETSI NFV MANO (section 6.3).
The MANO architecture is used for the service-related configuration, implemented through VNFs that are managed in the NFVI. An orchestration layer is expected between the VNOs and the VNFM.

Some of the subscriber management functions that could be considered to be moved into the NFVI are listed in subsection 5.2.5.1, while functions such as particularly configuration, may be performed in the InP domain or coordinated with the InP domain.

For multicast services it is better to maintain these functions as part of the Access Node platform. This avoids bandwidth inefficiencies, as replication needs to be done within the access network. Supporting multicast for multiple VNOs is possible using TR-101 [2] constructs (e.g., separate VLAN for multicast content per VNO).

5.2.5.1 Potential AN VNFs for Layer2+

- VLAN translation / addition / removal: the Access Node would focus on basic connectivity, whereas additional VLAN tagging could be performed in the NFVI
- Per subscriber QoS enforcement (e.g. policing or shaping), QoS policy enforcement, allocation of Quality of Service (QoS) and Class of Service (CoS) levels
- Port-based access control / authentication (e.g. by using a centralised 802.1x agent)
- Traffic management, traffic filtering, traffic shaping, flow control
- Traffic steering, forwarding, SDN
- Load balancing
- DHCP

5.2.5.2 Potential AN VNFs for Layers 1 and 2

- Control and configuration – Each VNO controls and configures their own virtual access node dataset of configuration objects
- Diagnostics and state information – Each VNO accesses virtual functions providing test, diagnostic, performance, and status information
- Management and Control of bandwidth allocation, such as configuring PON Dynamic Bandwidth Allocation (DBA)
- Traffic scheduling within VNO assigned transport service (O-VLAN / MPLS LSP / VXLAN) path)

The following functions should be coordinated by a single centralised management system or by a single InP in most cases:

- Data sharing: here a centralised system links to virtual access node functions, each of which distributes control and data to each VNO
- On-line reconfiguration management
- Dynamic Spectrum Management (DSM) [22]
- Power Control Entity (PCE), cross-layer low-power mode control, for G.fast – there are a number of thresholds and other settings that can be varied to configure low-power mode on individual transceivers and these settings and primitives can be determined in a virtualised power control entity and communicated to the transceivers
- Vectoring control and management – Virtualised functions can control part of the vectoring configuration, and could even calculate vectoring coefficients

5.2.6 VNO Traffic Encapsulation Models

VLANs play an integral role in the design and implementation of the FANS architecture. In the shared scenario, Internet services can have very different requirements and thus it is difficult to accommodate all these services (among different customers) in a single network.
To cope with this, a possible approach is to set up isolated networks for the different customers by using VLAN, MPLS or a VXLAN tunnel approaches. These tunnelling approaches are implemented by the physical access

and aggregation nodes. The tunnels are not visible to the VNO or any VNFs implementing the virtual access node. Selection of the tunnelling mechanism will depend on the hardware capabilities of the physical access node.

5.2.6.1 VLAN Tunnel

In the FANS context, the VLAN approach introduces “Operator VLAN (O-VLAN) Tag” tagging and forwarding rules. O-VLAN tag information is agreed between the VNO and InP and is added to the Ethernet frame at the interconnection point (at the A10 reference point). The following Figure 30 depicts the end-to-end VLAN scheme used in FANS.

In a network with multiple VLANs, it is important to correctly configure the VLANs which the network elements use to send management traffic.

Thus, it is necessary to extend the O-VLAN tag up to the vAN which represents the access point which terminates the customers’ lines, in order to handle the configuration of the same network element.

As shown in Figure 30, the C-VLAN tag information is transmitted through the network. In the downstream direction, the operator VLAN (O-VLAN) information is added to the Ethernet frame at the switch adjacent to the A10 reference point. These information tags remain up to the pAN. Conversely, in the upstream direction, the S-VLAN and O-VLAN tag information is added to the C-VLAN tag within the Ethernet frame at the pAN. It is important to note that O-VLAN information is discarded at the switch adjacent to the A10 reference, while the S-VLAN information continues to be forwarded in the VNO’s network.

Some operators use Q-in-Q (IEEE 802.1ad [6]) tunnelling (which extends IEEE 802.1Q [5]) and VLAN translation to create L2 Ethernet connections. Q-in-Q increases the VLAN number to 16 million (4094 * 4094) which results in the Ethernet frame size being increased (from 1522 to 1526 bytes).

The second tag is inserted in front of the first tag i.e. closer to the Ethernet header. Any third or subsequent tag imposition will be inserted in front, i.e. closest to the Ethernet header. The frame's original EtherType is always located above all the tags, next to the payload, as shown in the following Figure 31.

The Q-in-Q-in-Q VLAN Tag is shown in Figure 32.

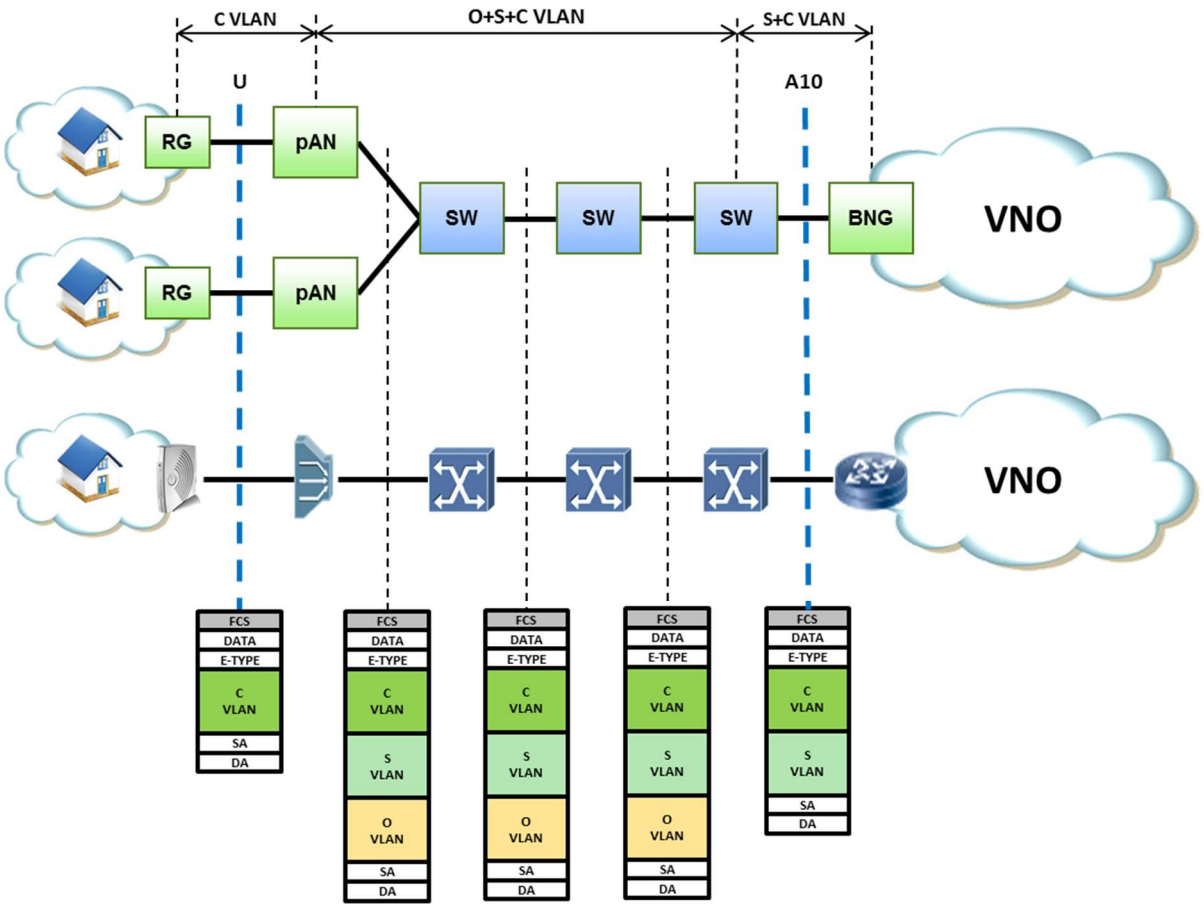


Figure 30 – End-to-end VLAN schema for FANS

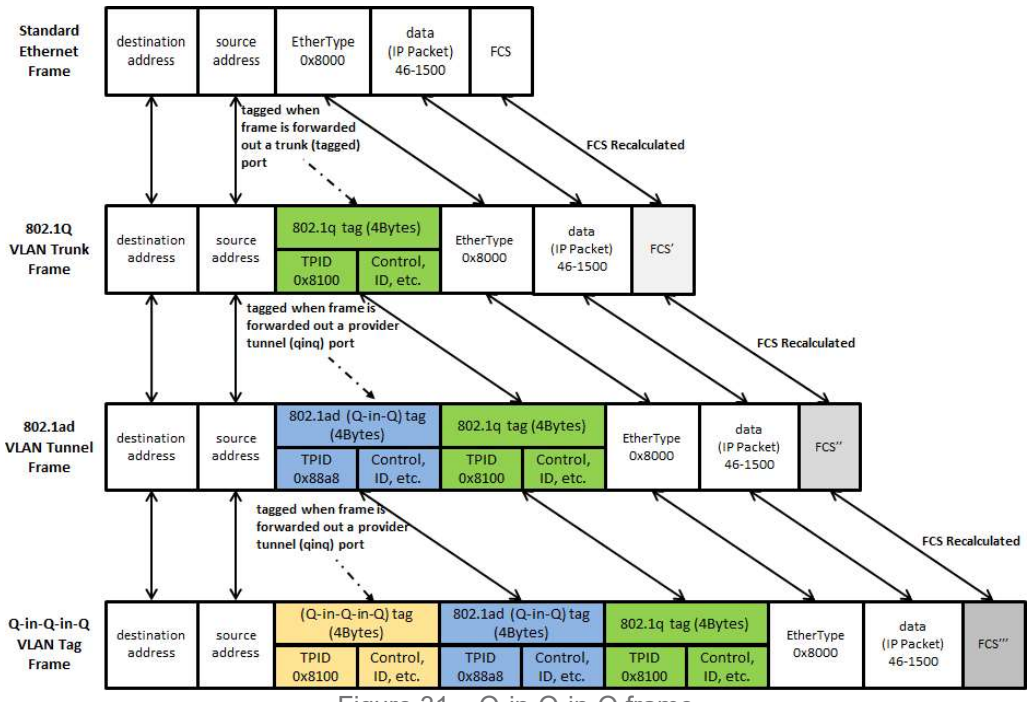


Figure 31 – Q-in-Q-in-Q frame

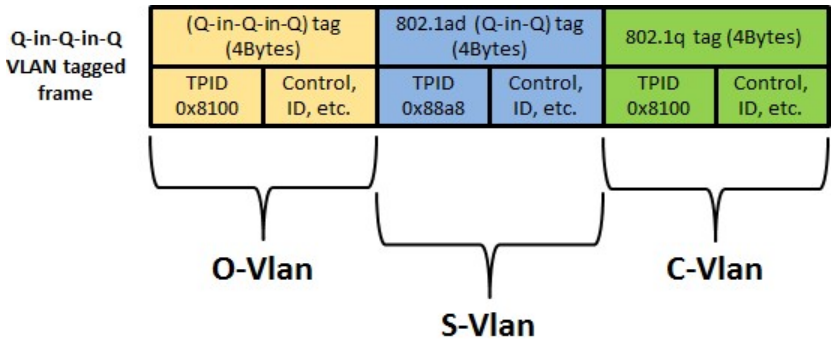


Figure 32 – Q-in-Q-in-Q VLAN frame detail

5.2.6.2 MPLS Tunnel

Another possible technique that could be used in the FANS scenario to manage the operators' data flows, is a label-based switching technique, such as Multi-Protocol Label Switching (MPLS), as depicted in the following Figure 33.

The main difference between the MPLS scheme and the VLAN model is the presence of a MPLS tunnel (defined using LSP labels) which contains the C-VLAN tag and S-VLAN tag information.

As shown in Figure 33, the C-VLAN tag information is transmitted through the network. In the downstream direction, the MPLS LSP information is added to the Ethernet frame at the PE router adjacent to the A10 reference point. These information tags remain up to the pAN, that must act as PE router. Conversely, in the upstream direction, the S-VLAN information is added to the C-VLAN tag within the Ethernet frame at the vAN, while the MPLS LSP information is added to the Ethernet frame at the pAN. It is important to note that MPLS tag information is discarded at the switch adjacent to the A10 reference point, while the S-VLAN information continues to be forwarded in the VNO's network. However, despite the flexible and scalable network architecture brought by about by MPLS, in a purely L2 evolution context, it might be useful to consider the use of the O-VLAN scheme rather than the L2.5 MPLS extension to the access network. Another motivation is that current access nodes may not support MPLS, but adding MPLS capability can increase the complexity and cost of the node.

5.2.6.3 VXLAN Tunnel

In addition to the O-VLAN and MPLS schemes, Virtual eXtensible Local Area Network (VXLAN) can also be deployed in the FANS scenario to separate the operator's traffic. The end-to-end VXLAN scheme is depicted in Figure 34.

VXLAN [20] is a tunneling scheme to overlay Layer 2 networks on top of Layer 3 networks, and the frame format is shown in Figure 35. Each VXLAN overlay network is identified through a 24-bit segment ID, which is the VXLAN Network Identifier (VNI). This allows up to 16 million VXLAN overlay networks to coexist within the same administrative domain. The VNI and VXLAN related tunnel/outer header encapsulation are known only to the VXLAN Tunnel End Point (VTEP).

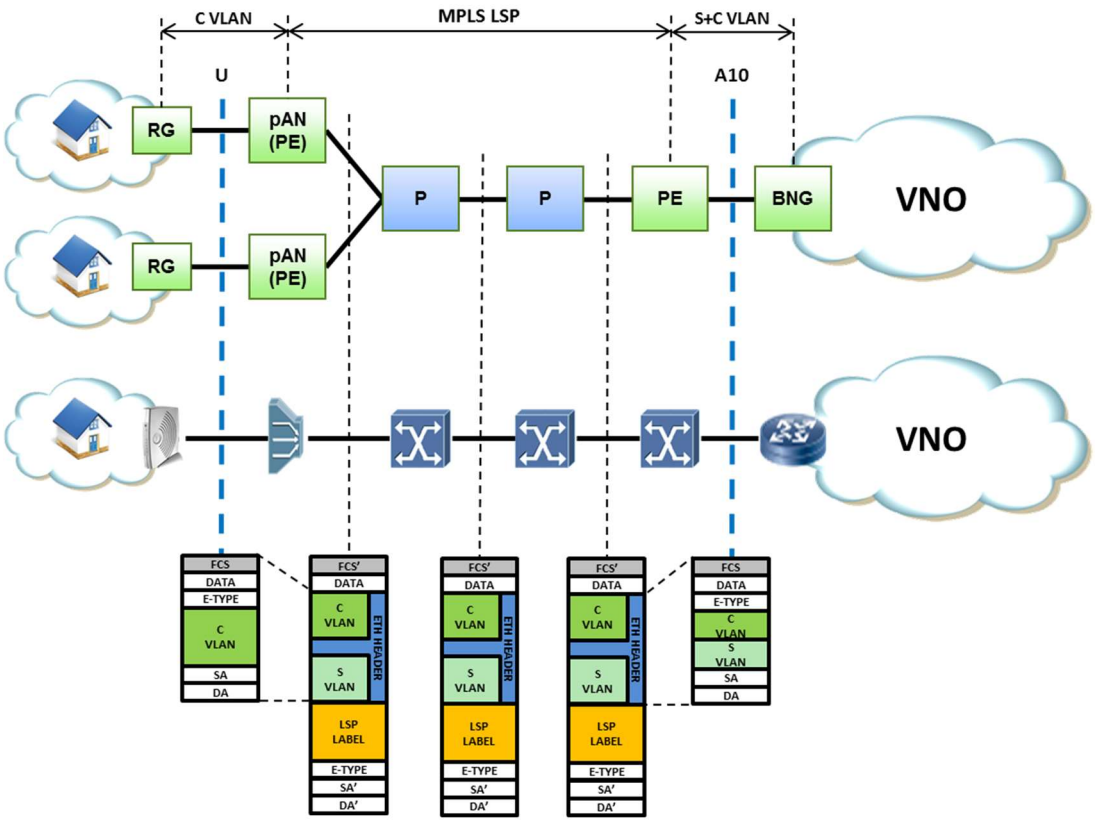


Figure 33 – End-to-end MPLS schema for FANS

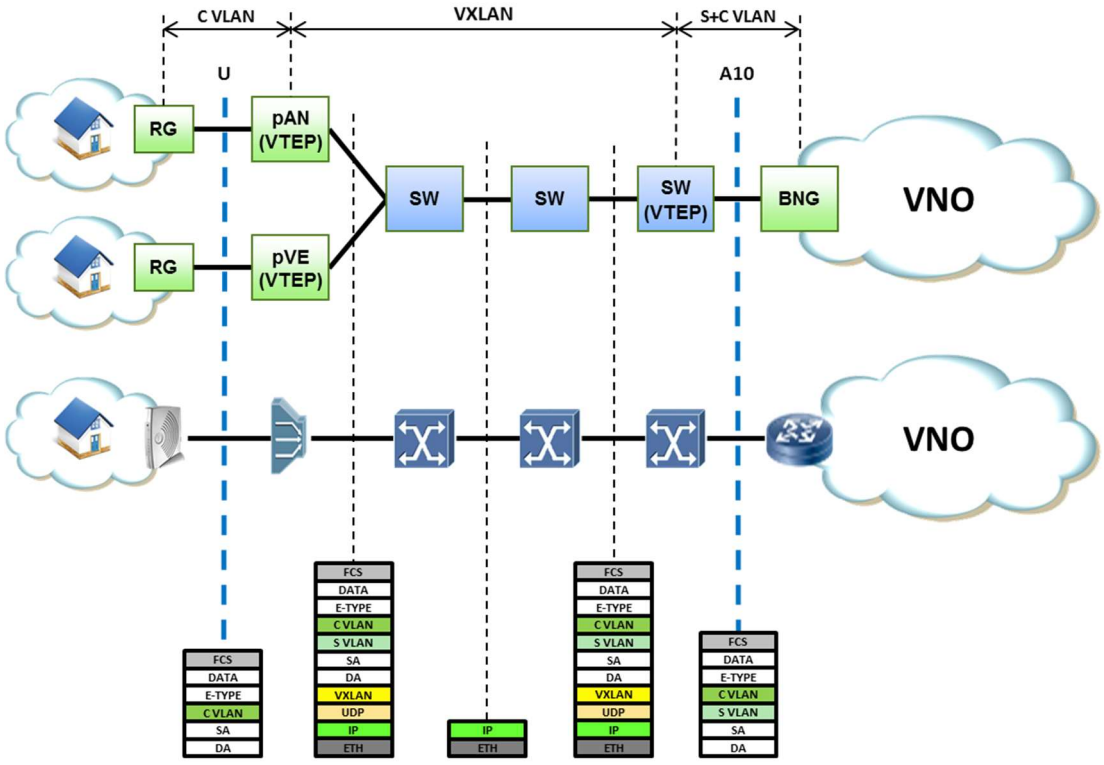


Figure 34 – End-to-end VXLAN schema for FANS

As shown in Figure 34, the C-VLAN tag information is transmitted through the network. In the downstream direction, the VXLAN tag information is added to the Ethernet frame at the switch adjacent to the A10 reference point, acting as a VTEP. These information tags remain up to the pAN, as well acting as a VTEP. Conversely, in the upstream direction, the S-VLAN and O-VLAN tag information is added to the C-VLAN tag within the Ethernet frame at the pAN. It is important to note that VXLAN information is discarded at the switch adjacent to the A10 reference, while the S-VLAN information continues to be forwarded in the VNO's network.

Figure 35 – VXLAN frame format

By introducing VXLAN, instead of doing the provisioning hop by hop, only those network elements which host the VTEP are involved, and no tunnel signalling is required either. In addition, the VXLAN model is backhaul agnostic, which also removes the need to have additional physical infrastructure. The VXLAN approach for FANS can adapt to the evolution towards cloud-like infrastructure with SDN and NFV technologies.

5.3 SDN-based FANS

While the concept of Centralised Management System may be applied, such implementation may not fully leverage the value of SDN in the context of FANS and its key business scenarios:

- Innovative Wholesale service models to improve current offers (e.g. Bitstream and VULA)
- Vertical slicing of the network infrastructure to support services offered by the same Provider (e.g. consumer, enterprise, wholesale, mobile, etc.)
- Greenfield ultra-fast broadband deployments based on infrastructure co-investment

More specifically the concept of Software Defined Access Network (SDAN) is introduced here to indicate the evolution of Access Nodes and more noticeably the innovation of the management and control architecture and interfaces based upon:

- an evolved system called **SDN Manager & Controller** (SDN M&C)
- **automation protocols** (e.g. NETCONF, RESTCONF, OpenFlow, P4, IPFIX, Kafka)
- **standardised and software based Data Models** (e.g. YANG)
- **abstraction and adaptation layer** exposing a vendor and technology agnostic AN view

An innovative FANS solution can rely on SDAN, to be able to provide the following characteristics:

- network **automation**
- **standard model-based** and **programmable** FANS interfaces
- **flexibility and agility** of offered FANS services
- **unified platform** to manage a multi-vendor network
- **strict separation** of the management and control **domains of each VNO**
- **full operational control by the InP** as the subject responsible of the FANS infrastructure and services

The Access SDN Manager and Controller (M&C) is a key element of the SDAN and supports:

- management protocols designed for network automation (e.g. NETCONF)
- programmable NBIs to flexibly expose management and control functions
- persistent abstracted representation (pAN) of the physical Access Node (e.g. in the form of a YANG Data Store),
- multi-vendor AN support via device adapters

The concepts of SDN applied to a broadband network infrastructure as well as of the Access SDN M&C and BAA layer are treated in TR-384 [24] and TR-413 [25].

Depending on the deployment architecture of the SDAN, the BAA layer can be embedded in the Access SDN M&C or deployed as a separate distributed function. In both cases this component guarantees southbound vendor adaptation towards the underlying AN technologies and northbound standard abstraction of the pAN representation.

Beyond the functions and characteristics described above for a SDAN solution, to implement the FANS application, the Access SDN M&C additionally needs to manage the:

- slicing of the access network based on VNOs' resource requests
- mapping of the VNO slices ($vAN_{X, Y, Z}$) to the pAN representation

These tasks are fulfilled respectively by the Slice Manager and the Resource Mapper blocks in Figure 36 and Figure 37 which depict the SDN-based FANS solution with both options of an embedded (hence not shown) or separate BAA layer. These options are coherent with the access domain architecture described in Figure 1 of WT-411 [31].

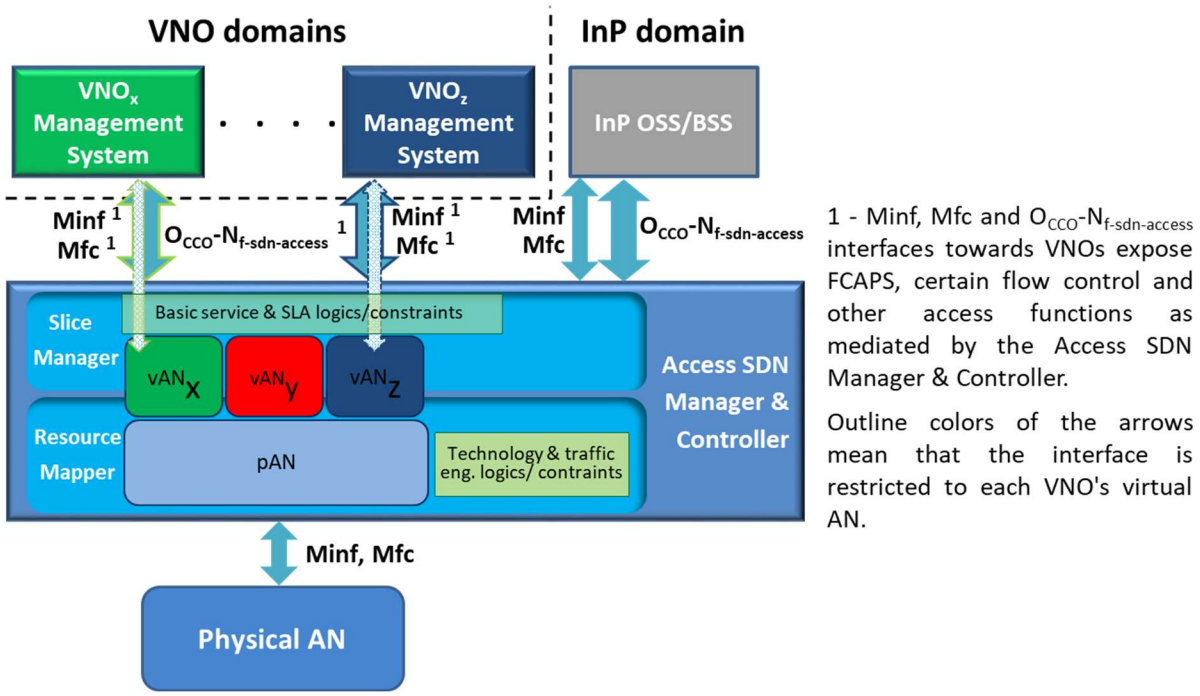


Figure 36 – SDN-based FANS with embedded BAA layer (Access domain)

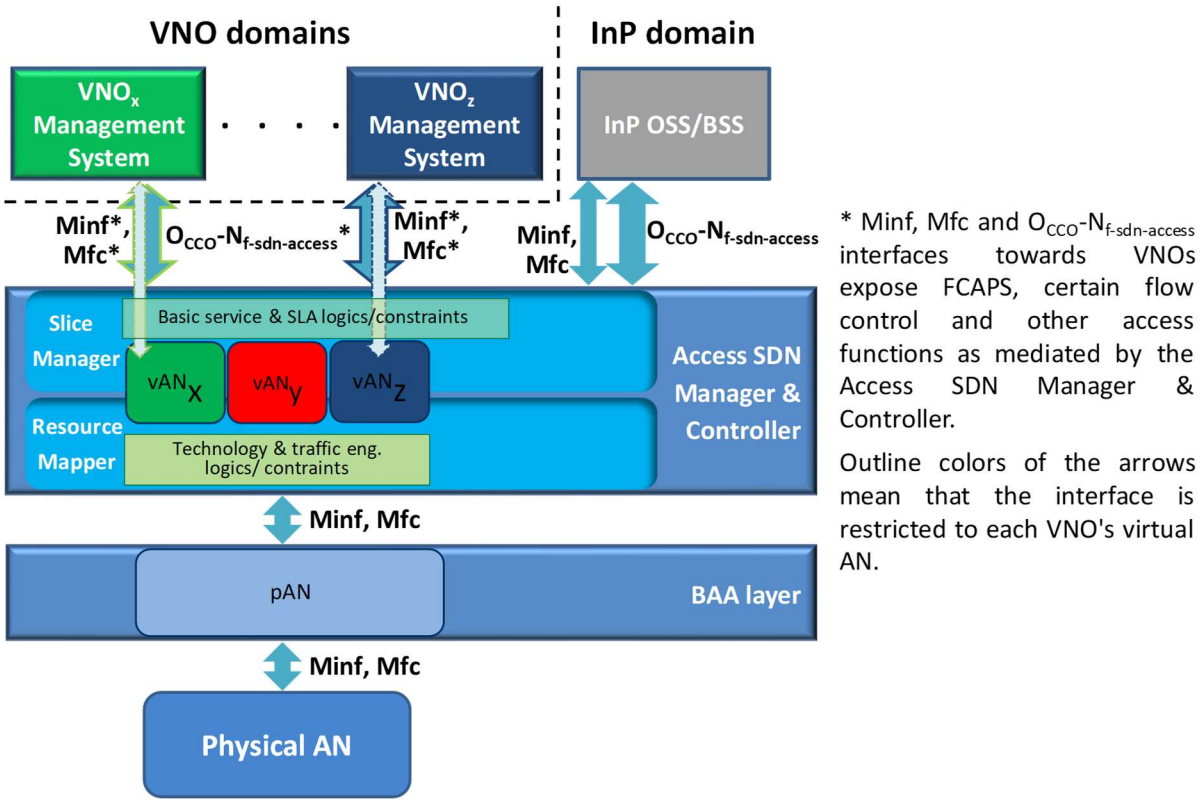


Figure 37 – SDN-based FANS with separate BAA layer (Access domain)

Figure 36 and Figure 37 represent functional diagrams; blocks and functions can be split/combined into different ways.

VNO Management Systems commands, especially those that encompass resources allocation, issued through the FANS API (i.e. the O_{CCO}-$N_{f\text{-}sdn\text{-}access}$ interface per the nomenclature in WT-411 [31]), require the mediation of the Slice Manager and the Resource Mapper that apply resource brokerage and reconcile the requests from all the VNOs.
This is under the InP control who has the responsibility to guarantee that the FANS business framework is fulfilled.
This business framework implies that:

a) all VNOs have a fair access to network resources per a basic FANS service framework collectively agreed among the InP and all the VNOs; in certain jurisdictions, this service framework may also incorporate provisions defined by the relevant Regulatory Authority and those players (e.g. for a regulated Wholesale offer)
b) each VNO has access to network resources consistently with the SLA bilaterally agreed with the InP
c) each VNO can access only the configuration and information related to its own virtual access network, and related customers and services

In Figure 36 and Figure 37, bullet a) is represented by the basic service logics/constraints that may vary over time based on VNOs/InP collective service agreements and/or regulatory provisions.
This first set of constraints defines the FANS service(s) basic characteristics accessible on the same basis to all VNOs.
For mere example sake this set may define:

- connectivity models across the physical AN (e.g. abstract L2 configuration, full L2 configuration, configuration of L2 plus certain L1 parameters, etc.)
- minimum levels of service (e.g. minimum DS/US Committed Information Rate at AN backhaul link, etc.)

Bullet b) is represented in Figure 36 and Figure 37 by the SLA logics/constraints which vary based on the business agreements between each VNO and the InP, and have to be compatible with the basic service constraints.
This second set of constraints defines FANS service(s) specific characteristics for each VNO.
For mere example sake this set may define:

- Committed Information Rate and Excess Information Rate beyond the overall capacity and resources to be guaranteed for the basic FANS service(s).

The Slice Manager is the module that exposes vAN_k representations to each VNOs via the FANS API. It accepts VNO requests only if compliant with the basic service and SLA logics/constraints.
This could be implemented in two alternative ways:

- by programming the FANS API towards each VNO so that the vAN_k representation's exposed parameters and their semantics are shaped according to the constraints
- by allowing any VNO request over the FANS API but accepting/rejecting them upon internal checks against those constraints.

Once the service and SLA constraints are checked by the Slice Manager, it is the Resource Mapper that finally accepts/rejects a VNO request and supervises real-time traffic scheduling to deal with congestions. This is based on resource availability, bandwidth allocation strategies and the overall overbooking agreed with all VNOs, which are programmed via the traffic engineering logics/constraints embedded in the Resource Mapper. VNO Management Systems get a notification whether a request was accepted or not.

The Resource Mapper is the module that maintains the correspondence between the physical/logical resources in the overall pAN representation of the real network with those allocated to the VNOs network representations ($vAN_{X, Y, Z}$). It guarantees VNOs separation, per bullet c), by segregating them to their own vAN representations.

Further details about SDN-based FANS are described in CLOUDCO-APPN-007 [29].

As suggested in Figure 12, the FANS solution may involve also the InP's Aggregation Nodes as the means to aggregate VNOs' customers traffic from the Access Nodes and send groomed flows to each VNO delivery point and vice versa.
This can be achieved by introducing an SDN Manager and Controller for the aggregation domain and a level of network orchestration in the SDN hierarchy as depicted in Figure 38.

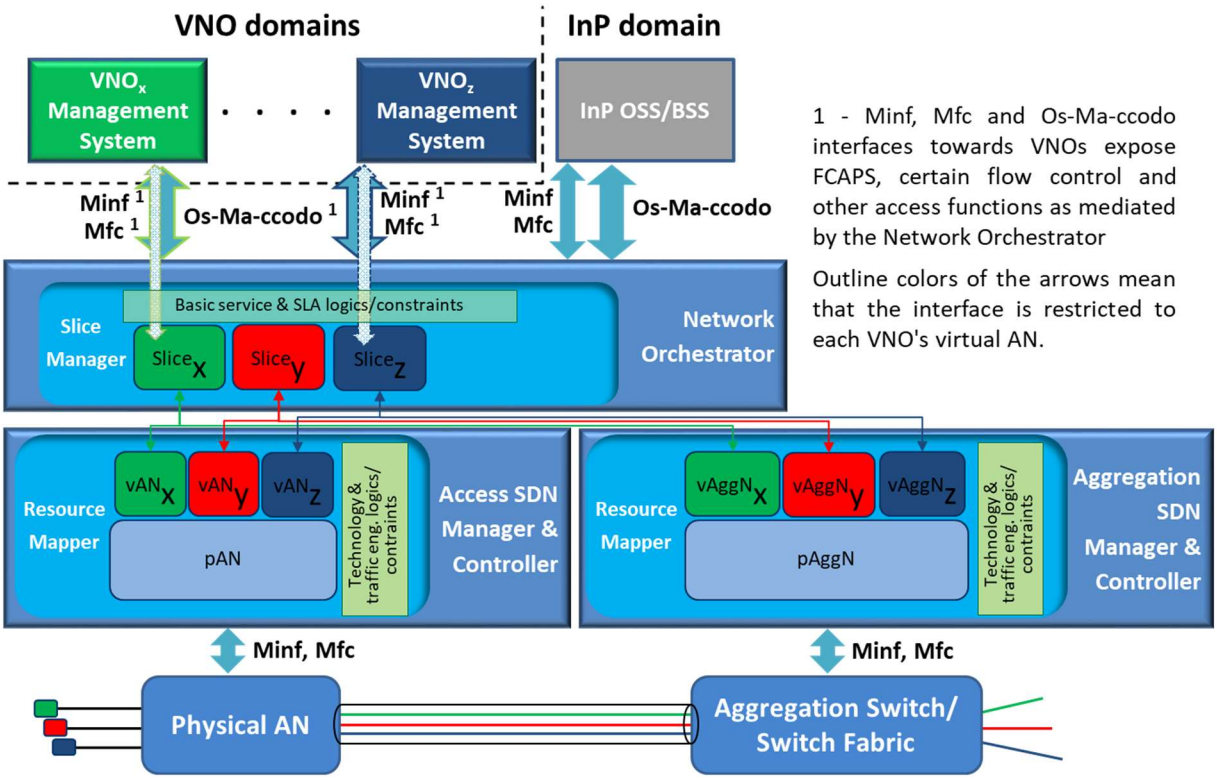


Figure 38 – SDN-based FANS (Access and Aggregation domains)

Figure 38 represents a functional diagram, blocks and functions can be split/combined into different ways. Furthermore the aggregation functions may be implemented as physical switches, virtual switches or a combination thereof.

In this case the VNOs' Management Systems are connected to a Network Orchestrator via the FANS API (i.e. the Os-Ma-ccodo interface per the nomenclature in WT-411 [31]) and exposed to their own virtual network representation ($Slice_{x, y, z}$) which is the combination of the representations of their virtual access network and virtual aggregation network.

VNO resource requests are sent to their slice and validated against the agreed basic service and SLA constraints programmed in the Slice Manager. If they fulfill those constraints, the Orchestrator splits them, if needed, into domain-scoped requests towards the target vANs and vAggNs.

The Resource Mapper in each domain checks if the received requests can be accepted or rejected based on resource availability and traffic engineering constraints.

The support of roll-back on partially executed configurations is fundamental to avoid misconfiguration of services and misalignments across the Access and Aggregation domains and the hierarchy of SDN elements.

5.3.1 FANS API

The FANS API (O_{CCO}-$N_{f\text{-}sdn\text{-}access}$ in Figure 36 and Figure 37 or Os-Ma-ccodo in Figure 38) is a key enabler for service agility and flexibility.

This API allows to implement the described FANS business framework by leveraging the characteristics of network programming and automation protocols (e.g. NETCONF, RESTCONF) and standardised Data Models (e.g. YANG).

This way the FANS API towards each VNO can be programmed to expose the agreed vAN (and vAggrN if applicable) parameters with different granularities or instead via predefined parameter groupings (profiles). The adoption of standardised Data Models (DMs) over the FANS API eases interoperability between the VNO and InP systems and the evolution of FANS service via DMs extensibility and interfaces programmability.

For example exposing a pure L2 vAN representation (either fully detailed or further abstracted) allows VNOs to define service offers in a technology and vendor agnostic way.

At the same time the InP retains a full featured FANS API to perform service and network maintenance over its infrastructure.

Standardised Data Models are fundamental also at the SBI of the SDN Manager & Controller to ease interoperability with ANs from multiple vendors and streamline the introduction of technology and feature upgrades in the InP network.

A useful set of references for NETCONF/YANG interfaces for FANS is represented by TR-386 [24], TR-413 [25], WT-411 [31] and WT-435 [32].

6 Relation of FANS to the ETSI NFV architecture

This chapter relates with the Virtual Access Node FANS model described in section 5.2. As previously mentioned for the Virtual Node model, the access node functions are decoupled from the underlying physical hardware. The main principle of separating network functions from the hardware they run on is called disaggregation that is enabled by Network Functions Virtualisation (NFV) technologies. NFV leverages virtualization techniques to enable the decoupling of some network functions by enabling them to run as Virtual Network Functions (VNF) on COTS hardware.

NFV offers a simplified and more agile network with the flexibility to adjust to changing conditions. Moreover, NFV envisages the implementation of Network Functions (NFs) as software-only entities that run on a NFV Infrastructure (NFVI).

This section describes the relationship of FANS to the ETSI NFV architecture, focusing on the Virtual Access Node model, since the Management System model is not based on NFV paradigm.

6.1 Functional Domains

The ETSI ISG NFV Architectural Framework document [13] identifies three main domains:

- **Virtualised Network Functions (VNFs)** – the collection of VNFs sharing physical hardware.
- **NFV Infrastructure (NFVI)** – includes the actual physical resources and how these can be virtualised. NFVI supports the execution of the VNFs.
- **NFV Management and Orchestration (MANO)** – covers the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualisation, and the lifecycle management of VNFs. NFV MANO focuses on all virtualisation-specific management tasks necessary in the NFV framework.

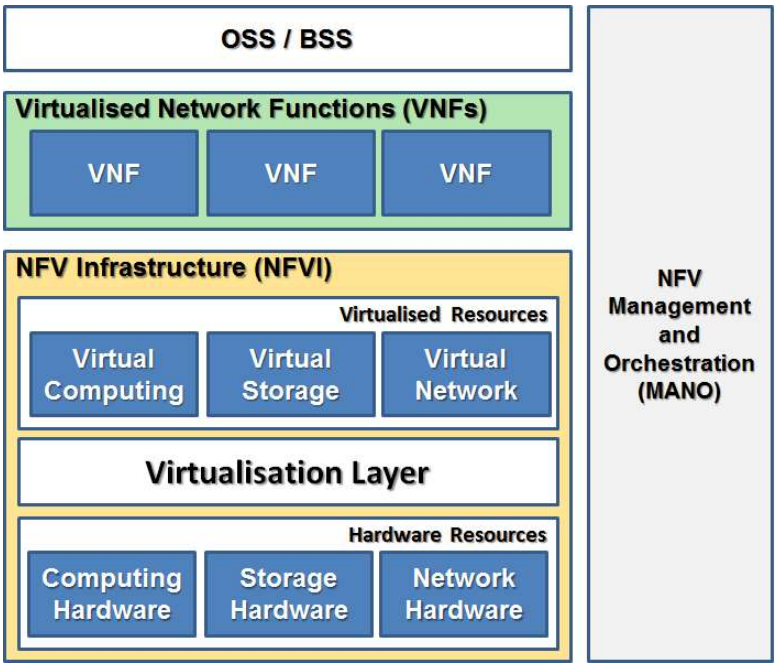


Figure 39 – High-Level NFV Framework

VNFs run on top of the virtualisation layer, which is part of the NFVI. In the FANS Virtual Node model (section 5.2), the VNFs are represented by vAN instances of the various VNOs.

NFV emphasizes the fact that the exact physical deployment of a VNF instance on the infrastructure is not visible from the end-to-end service perspective. However, VNF instances and their supporting infrastructure need to be visible for configuration, diagnostic and troubleshooting purposes.

The Centralised Management System is in charge of these responsibilities, while VNOs use standard interfaces to communicate with Centralised Management System for the above purposes. The end-to-end network service and the delivered behaviour need to be equivalent in the virtualised and non-virtualised scenarios.

In a FANS environment, the VNO instantiates its VNF instances on top of the InP's infrastructure to create an end-to-end network service instance.

The high-level NFV architecture (including NFVI domains) is depicted in the following Figure 40.

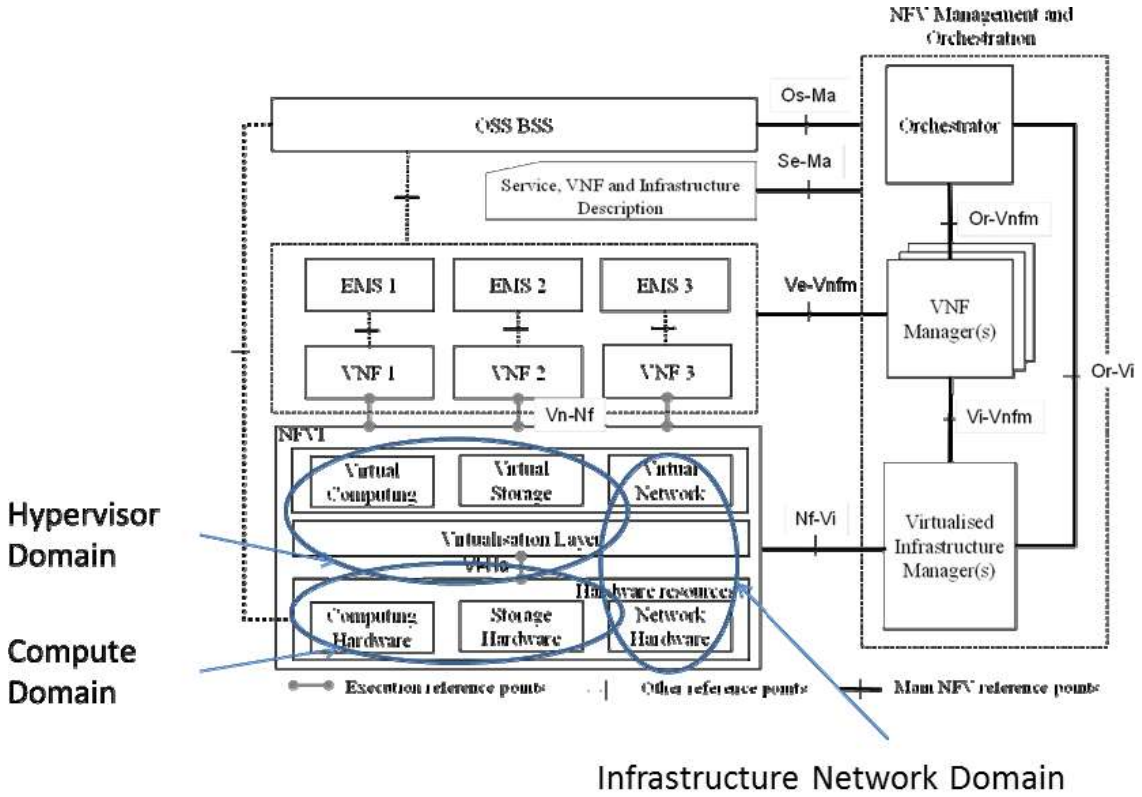


Figure 40 – NFV reference Architectural Framework and identification of NFVI Domains [13]

The NFV architecture is composed of:

- NFV Infrastructure (NFVI)
  - Hypervisor Domain
  - Compute Domain
  - Infrastructure Network Domain
- Virtualised Network Functions (VNFs)
- Element Managements (EMs)
- NFV Management and Orchestration (MANO)
- Virtualised Infrastructure Manager(s) (VIMs)
- VNF Manager(s) (VNFMs)
- Service, VNF and Infrastructure Description
- NFV Orchestrator (NFVO)
- Operations & Business Support Systems (OSS/BSS)

It is important to note that a network operator who uses a traditional network architecture, still needs at least one management system, for instance an EMS (or an NMS), supported by an OSS system.
In the NFV architecture, multiple managers (e.g., VIM Manager, VNF Manager Orchestrator and also the traditional EMS and OSS/BSS) are needed. Moreover, EM, VNFM and any other entity identified by the NFV architecture framework, may be virtualised or not.

The scope of this section is to describe the functional domains of the ETSI NFV architecture [13], as well as the main reference points between these blocks and how the Virtual Access Node model (refer to Figure 16 and Figure 17 above) is related to this architecture.

6.1.1 NFV Infrastructure (NFVI) Domain

The NFV Infrastructure (NFVI) is composed of hardware and software components that build up the environment in which VNFs are deployed, managed and executed. The NFVI may also include partially virtualised Network Functions (NFs), in which a certain part of the functionality is virtualised while other parts remain in hardware (PNF) for performance reasons, protect investment or ease of migration.
The execution environment for VNFs is provided by the NFVI deployed in various NFVI Point of Presence (NFVI-PoPs).
An NFVI-PoP represents a single geographic location where a number of computing nodes of the NFVI infrastructure are located, and it supports the deployment of VNFs in a variety configurations. The FANS environment includes multiple VNFs of different network operators (VNOs) in a multi-tenant model at one or more NFVI-PoPs.
Figure 41 shows a comparison between the vAN model and ETSI NFV model, regarding the virtualised infrastructure.

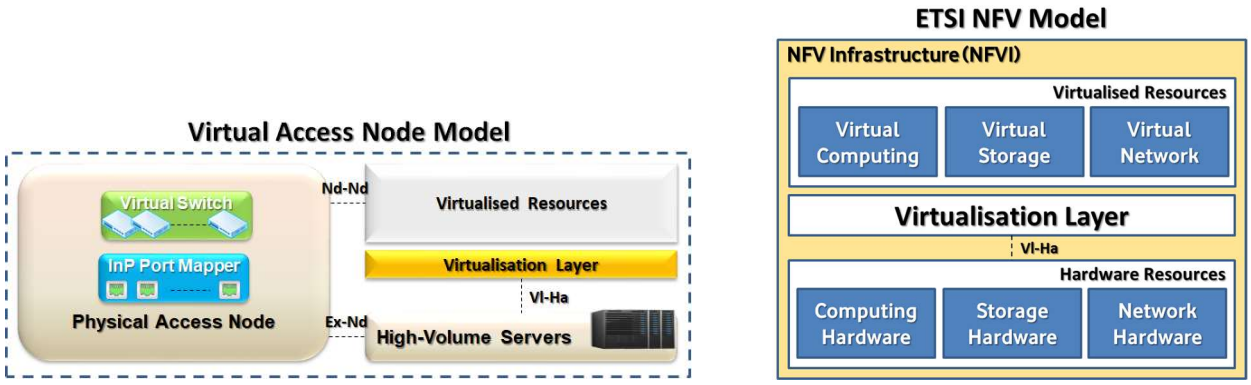


Figure 41 – Comparing Virtualised Network Infrastructure domains

Several elements are in common between the two models; the vAN model includes functionalities needed to host vANs, as well as software components common to many vANs. Moreover they provide functionality required to support deployment, interconnection, or management of vANs.
The virtualised infrastructure domain of the vAN model can be easily mapped into the NFVI of ETSI NFV Model.
The NFVI Infrastructure shown in Figure 41 includes:

- Hardware Resources
- Virtualisation Layer and Virtualised Resources

From the VNF's perspective, the virtualisation layer and the hardware resources look like a single entity providing the VNF with the desired virtualised resources.
More information on NFVI domains can be found be in:

- ETSI GS NFV 002 V1.2.1 [13]
- ETSI GS NFV-INF 001 V1.1.1 [12]
- ETSI GS NFV-INF 003 V1.1.1 [14]
- ETSI GS NFV-INF 004 V1.1.1 [15]

- ETSI GS NFV-INF 005 V1.1.1 [16]

6.1.2 Virtualised Network Functions (VNFs) Domain

A Virtualised Network Function (VNF) is a Network Function (NF) capable of running on an NFV Infrastructure (NFVI) and being orchestrated by a NFV Orchestrator (NFVO) and VNF Manager. In the NFV paradigm, the functional behaviour and the external operational interfaces of a Physical Network Function (PNF) and a VNF are the same.
In the Virtual Access Node model, the vAN functions match the VNFs of ETSI NFV model.

6.1.3 NFV Management and Orchestration (MANO) Domain

MANO stands for Management and Orchestration and it is the layer defined by ETSI to manage and orchestrate the virtual infrastructure and resources. NFV MANO includes three different managers:

- **Virtualised Infrastructure Manager (VIM)** – Controls and manages the NFVI compute, storage, and network resources
- **VNF Manager (VNFM)** – Oversees lifecycle management of VNF instances, coordination and adaptation role for configuration and event reporting between NFVI and E/NMS
- **NFV Orchestrator** – Responsible for on-boarding of Network Services (NS) and Virtual Network Functions (VNF), service lifecycle management, global resource management and so on

The VIM and VNFM layers together provide the VNF and resource lifecycle management capabilities. The NFVO provides the lifecycle management around the virtualised network service. Moreover, because the NFV MANO architecture is integrated in the existing legacy system using open APIs, this architecture works in a FANS scenario.
Figure 42 depicts the comparison between the Virtual Access Node model and ETSI NFV model regarding the management system infrastructure.

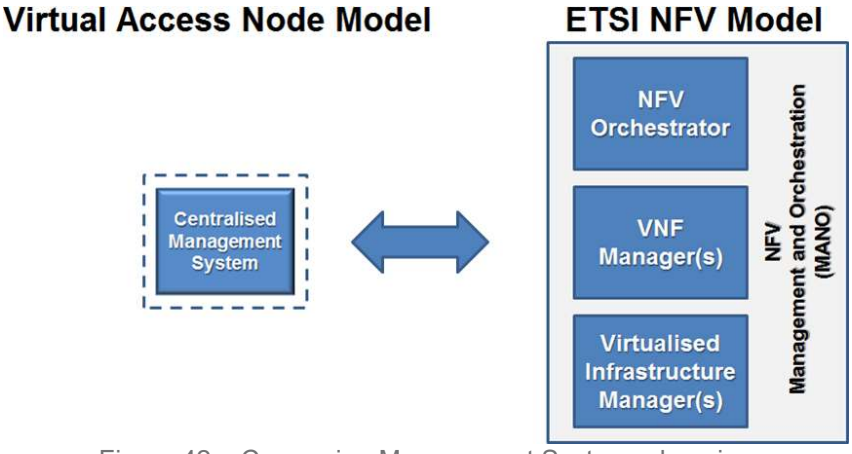


Figure 42 – Comparing Management Systems domains

In the FANS model, the InP is entirely in charge of managing the infrastructure and everything related to it. As shown in the previous Figure 42, NFV MANO decomposes the management and orchestration needs for the NFV architecture into three functional blocks, while the Centralised Management System (MS) is represented as a single block. At a high level, the Centralised Management System corresponds to the NFV MANO. This means that the Centralised MS in FANS model has the same behaviour as the NFV MANO in the ETSI NFV model, even though it is realized via a different management system model.

More detail on NFV MANO Architecture are described in the section 6.3 of this document.

6.2 Interfaces & Reference Points

An interface is a point of interaction between two entities that can be software services, hardware services and resources, while a reference point is an architectural concept that defines and exposes an external view of a function block.
The following Figure 43 depicts a reference point architecture, showing only the NFVI Network Domain and aligning these reference points with the NFV E2E Architecture [16].

Some of the reference points described in Figure 40 and Figure 43, have a 1:1 relation with those in Virtual Access Node model.
This section describes the main reference points between the functional blocks described in the previous section 6.1 and their relation with the FANS model. For the entire set of reference points, refer to the ETSI NFV and BBF documentation.

6.2.1 NFVI - Virtualised Infrastructure Manager (Nf-Vi)

In the vAN model, the Nf-Vi reference point is applied between the InP and the access infrastructure (physical access nodes, including virtual infrastructure, and servers in datacentres) as described in [17].

6.2.2 VNF/EM - VNF Manager (Ve-Vnfm)

The vAN model uses the Ve-Vnfm reference point to support communication between the virtual functions (vAN instances) and the Centralised Management System as described in [17].

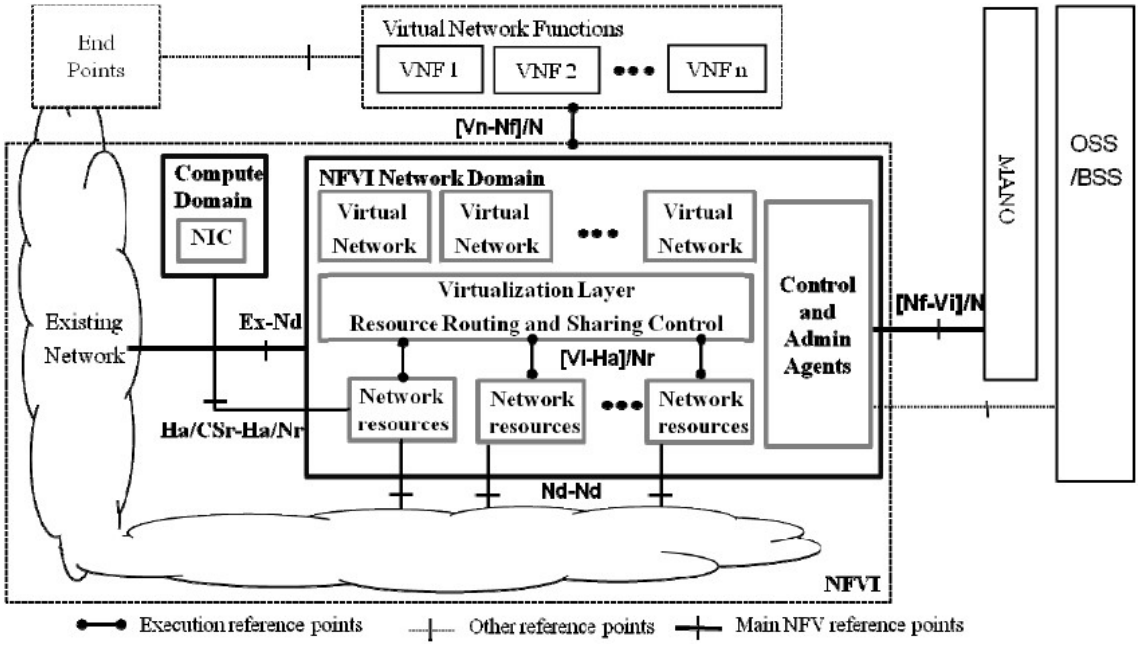


Figure 43 – Network Domain Reference Point Architecture [16]

6.2.3 OSS/BSS - NFV Management and Orchestration (Os-Ma)

Similar to the Os-Ma in [17] in the vAN model, the Os-Ma-nfvo reference point supports information transfer between VNO Management System and Centralised Management System.

6.2.4 OSS/BSS – Physical Infrastructure

A reference point is needed to support communication between VNO MS and the pAN.
In this scenario, NMS/EMS systems should be aware of virtualisation and collaborate with the Centralised MS (via Os-Ma-nfvo reference point) to perform functions that require exchange of information on resources lifecycle.
Note that this reference point is represented in the NFV reference Architectural Framework [13], but not yet specified, as shown in Figure 40. However, in BBF TR-359 [7] the “Minf” reference point is defined between OS/EM/WIM and the network elements within the physical infrastructure. This reference point has similar characteristics to the one needed in FANS architecture.

6.2.5 Virtualisation Layer - Hardware Resources (Vl-Ha)

The Virtualisation Layer is a key component in the ETSI NFV architectural framework. This layer abstracts and logically partitions physical hardware resources and provides anchors between the VNF and the underlying virtualised infrastructure.
The Vl-Ha described in [12] is an internal reference point that interfaces the Virtualisation Layer to hardware resources to create an execution environment for VNFs, and collect hardware resource state information for managing the VNFs independently from any hardware platform. This allows the decoupling of software from hardware.

6.2.6 VNF - NFV Infrastructure (Vn-Nf)

The Vn-Nf reference point described in [13] represents the execution environment used by VNFs to be executed on NFVI in ETSI NFV framework. It does not assume any specific control protocol, but in the FANS scenario, the Vn-Nf reference point uses a set of APIs to get access to the NFVI.

6.2.7 Infrastructure Network Domain - Existing Network (Ex-Nd)

The provision of connectivity between a vAN and a pAN in existing networks, requires the use of the Ex-Nd. More detail on Ex-Nd interface can be found be in [16].

6.2.8 NFV Infrastructure (Nd-Nd)

The Nd-Nd interface consists of protocols that are exposed between the NFVI-PoPs to provide connectivity between VNFs located in different NFVI-PoPs, regardless of the connectivity service provided. More detail on Nd-Nd interface can be found be in [16].

6.2.9 Management Interface (Minf)

Minf reference point is used by the Centralised Management Systems to communicate with the physical node and the virtual node for FCAPS functionalities (e.g. service parameters). More details about Minf interface can be found in TR-413 [25].

6.2.10 Control Flow Interface (Mfc)

Mfc reference point is used by the Centralised Management Systems to communicate with the physical node and the virtual node for flow control (e.g. forward table configuration).

6.3 NFV MANO

The vAN model does not impose any constraint (in terms of internal module numbers) on the Centralised Management System. The Centralised Management System could be a single point of management or it could have multiple internal management modules. In any case, it is important to note that Centralised Management System and NFV MANO have the same behaviour toward external systems or infrastructures.

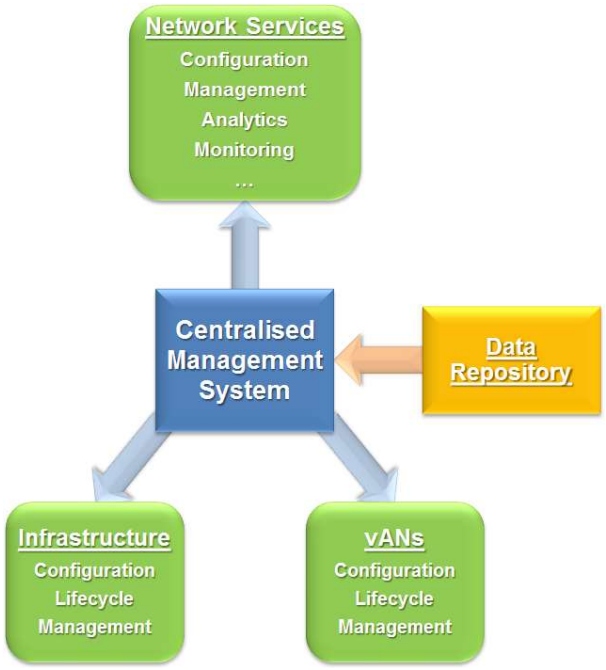


Figure 44 – Virtual Access Node model: Centralised Management System roles

In the FANS architecture the Centralised Management System is the main component of the models described in sections 5.1 and 5.2. It is in charge of the orchestration and management of both physical infrastructure and software resources, as well as governance of those vAN instances that share resources of the FANS infrastructure. Moreover, it is responsible for the lifecycle management of the vANs, including their creation, provisioning, and monitoring.

Finally, an internal data repository provides information for the vANs deployment and operational behaviour, such as vAN instantiation, lifecycle management and orchestration. The information elements to be handled by the Centralised Management System, need to support the flexible deployment and portability of vAN instances on multi-vendor environments.

The following is a non-exhaustive list of Centralised Management System functionalities:

- Resource Management
- Infrastructure Management
- Network Services Management
- Fault Management
- Capacity planning, monitoring and optimization information, performance measurement
- vAN instantiation and lifecycle management (software update/upgrade, scaling out/in and up/down)
- Network Service instantiation and lifecycle management
- Policy management
- Orchestration of both the virtual and physical infrastructure resources

More information on NFV MANO can be found be in [17].

7 Technical Requirements

The following sections describe technical requirements for the FANS model as extensions of the requirements specified in TR-101 [2] and TR-178 [3].

7.1 Network Requirements

A pure Ethernet Aggregation Network is still supported in FANS and it is mainly applicable to L2 access technologies. The following network requirements are needed to support the interconnection of network operators at Ethernet access node and aggregation node level.

7.1.1 Common Requirements

[R-01] The Access Node MUST support at least one of the encapsulation models described in section 5.2.6.
[R-02] The Aggregation Node MUST support at least one of the encapsulation models described in section 5.2.6.
[R-03] For the Virtual Node model, the virtual Access Node MUST support at least one of the encapsulation models described in section 5.2.6.
[R-04] For the Virtual Node model, the virtual Aggregation Node MUST support at least one of the encapsulation models described in section 5.2.6.

Note: the requirements above are fundamental to deploy a scalable and efficient FANS solution. For already deployed physical Access and Aggregation Nodes, [R-01] and [R-02] are to be considered optional although strongly recommended.

7.1.2 Access Node

The requirements specified in this section are incremental to TR-101 [2] and TR-178 [3]. All TR-101 [2] and TR-178 [3] Access Node requirements also apply to FANS-capable Access Nodes.

[R-05] The physical Access Node MUST be able to add the Operator Tag (O-Tag), the MPLS tag or the VXLAN encapsulation to the traffic flow received at the U interface when transmitting across the V-interface in the upstream direction.
[R-06] The physical Access Node MUST be able to remove the Operator Tag (O-Tag), the MPLS tag or the VXLAN encapsulation from the traffic flow transmitted at the U interface in the downstream direction.
[R-07] For the Virtual Node model, the physical Access Node MUST be able to associate physical ports with virtual ports for each VNO.
[R-08] For the Virtual Node model, the virtual ports MUST be identified through virtual port IDs. The logical/physical port ID and virtual port ID SHOULD be compatible with the syntax of access loop Identification defined in TR-101 [2].
[R-09] For the Virtual Access Node model, the InP Port Mapper MUST maintain a mapping between physical port IDs and virtual port IDs.

Note: the requirements above are fundamental to deploy a scalable and efficient FANS solution. For already deployed physical Access Nodes, [R-05] and [R-06] are to be considered optional although strongly recommended.

7.1.3 Aggregation Node

All TR-101 [2] and TR-178 [3] Ethernet Aggregation Node requirements also apply to FANS-capable Aggregation Nodes.

[R-010] The physical Aggregation Node closest to A10 interface MUST be able to support add the Operator Tag (O-Tag), the MPLS Tag or the VXLAN encapsulation to the traffic flow received at the A10 interface in the downstream direction.

[R-011] The physical Aggregation Node closest to A10 interface MUST be able to support remove the Operator Tag (O-Tag), the MPLS Tag or the VXLAN encapsulation from the traffic flow transmitted at the A10 interface in the upstream direction.

Note: the requirements above are fundamental to deploy a scalable and efficient FANS solution. For already deployed physical Aggregation Nodes, [R-010] and [R-011] are to be considered optional although strongly recommended.

7.2 Virtual Access Node model Requirements

This section provides a set of requirements to support the FANS architecture defined in section . Unless stated otherwise, the requirements presented in TR-101 [2] and TR-178 [3] remain applicable and they are now extended with FANS specific requirements.

7.2.1 Common Requirements

[R-012] When virtual Access Nodes are deployed inside physical Access Node by running on virtual machines, the physical Access Node MUST support the Nf-Vi interface to the Centralised Management System.

[R-013] The virtual Access Node MUST support Ve-Vnfm interface to the Management System.

[R-014] When virtual Aggregation Nodes are deployed inside physical Aggregation Node by running on virtual machines, the physical Aggregation Node MUST support the Nf-Vi interface to the Centralised Management System.

[R-015] The virtual Aggregation Node MUST support Ve-Vnfm interface to the Management System.

[R-016] The Access Node, the Aggregation Node, the virtual Access Node and the virtual Aggregation Node MUST support bulk pre-configuration including line-specific settings and VLAN associations, based on Operator Tag, as defined by Centralised Management System configuration.

[R-017] The Access Node and the Aggregation Node MUST support the transmission of diagnostics, status, and performance data to the Centralised Management System via Minf interface.

[R-018] The virtual Access Node and the virtual Aggregation Node MUST support the transmission of diagnostics, status, and performance data to the Centralised Management System via Minf interface.

[R-019] The Access Node and the Aggregation Node MUST trigger the appropriate alarms, including, but not limited to alarms for continuity loss, packet loss, latency and jitter, by informing the Centralised Management System using the Minf interface.

[R-020] The virtual Access Node and the virtual Aggregation Node MUST trigger the appropriate alarms, including, but not limited to alarms for continuity loss, packet loss, latency and jitter, by informing the Centralised Management System using the Minf interface.

7.2.2 Access Node

[R-021] The FANS system MUST allow the InP to maintain and abstract the mapping of the physical nodes and physical ports in the InP's access network into multiple virtual Access Nodes.

[R-022] The FANS system MUST restrict the scope of a VNO's control to the VNO's allocated virtual Access Node and its own virtual ports.

[R-023] The FANS system MUST allow the InP to allocate a subset of access network functions to a virtual Access Node based on the exposed functions from the InP crossed with the VNO's requirements. The subset of access network functions and corresponding protocols can be either instantiated on demand during virtual Access Node allocation, or be pre-configured in the physical Access Nodes.

[R-024] The FANS system MUST allow different services (e.g. mobile backhaul, residential, IPTV) to be provisioned using different virtual Access Nodes with different subsets of network functions in the same physical Access Node.

[R-025] The Centralised Management System MUST allow a VNO to retrieve, control and manage the state of a virtual port allocated to that VNO. The state definitions are listed below:
- a) “LINKUP” MUST be valid when the physical port has no alarm/defect.
- b) “LINKDOWN” MUST be valid when the physical port has an alarm/defect.
- c) “PORTUP” MUST be valid when the physical port is administratively up.
- d) “PORTUP” is the default state when the physical port is added, and MUST transit to LINKUP/LINKDOWN/PORTDOWN state after system power-up.
- e) “PORTDOWN” MUST be valid when the physical port is administratively down and replaced with LINKUP/LINKDOWN/PORTUP as the state changes.

[R-026] The Centralised Management System MUST allow reporting of the following transient status:
- a) “ADD” MUST be valid when VNO adds a virtual port.
- b) “DELETE” MUST be valid when VNO deletes a virtual port.
- c) “MODIFY” MUST be valid when VNO modifies a virtual port administratively up or down.

[R-027] The Centralised Management System MUST allow the following transient status to be captured by the system log:
- a) “ADD”,
- b) “DELETE”,
- c) “MODIFY”.

[R-028] The Centralised Management System MUST synchronize the add/delete operations of virtual port mapping with the InP Port Mapper table and vice versa,.

[R-029] The Centralised Management System MUST allow a VNO to delete a virtual port if and only if the virtual port is administratively PORTDOWN.

7.2.3 Aggregation Node

[R-030] The virtual Aggregation Node MUST be able to switch based on the MPLS tag as specified in TR-101 [2] and TR-178 [3]or the operator O-VLAN tag or the VXLAN encapsulation.

7.3 Centralised Management System Requirements

[R-031] In the case of the virtual Access Node deployment model, the Centralised Management System MUST support a standardised interface from the Centralised Management System in order to retrieve and to send messages autonomously to the InP Port Mapper. Specify which interface has to be mentioned.

[R-032] In the case of the Virtual Access Network deployment model, the Centralised Management System or other systems SHOULD provide proactive management of network performance issues to avoid bandwidth starvation. This management SHOULD be based on virtual Access Node and virtual Aggregation Node traffic usage.

[R-033] In the case of the Virtual Access Network deployment model, the Centralised Management System MUST provide the capability of proactive management, in order not to exceed the equipment computational and physical resources of the virtual Access Node and virtual Aggregation Node instances.

[R-034] In order to support FANS, Os-Ma-nfvo SHOULD implement the following function and related Data Model: (bbf-fans-vno) [23].

[R-035] The Minf interface SHOULD be specified according to TR-413 [25], including also Mfc interface requirements for controlling packet flows on physical ANs.

7.4 SDN-based FANS Requirements

This section provides a set of requirements to support the SDN-based FANS architecture defined in section 5.3. Unless stated otherwise, the requirements presented in TR-101 [2] and TR-178 [3] remain applicable and they are now extended with FANS specific requirements.

7.4.1 Access Node

[R-036] The physical Access Node $M_{inf\text{-}AN\text{-}type}$ and $M_{fc\text{-}AN\text{-}type}$ interfaces MUST comply with section 5.1 of TR-413 [25].

7.4.2 Aggregation Node

Note: The NETCONF/YANG interfaces for Aggregation Nodes (or the switch fabric) are not yet defined.

7.4.3 SDN Manager and Controller Requirements

For the SDN-based FANS solution represented in Figure 36 and Figure 37 the following requirements apply:

[R-037] The Access SDN Manager and Controller MUST maintain an abstracted representation (pAN) of the physical Access Node and keep this representation aligned with the physical Access Node itself in terms of configuration, alarms and events.

[R-038] The Access SDN Manager and Controller MUST implement slicing mechanisms (functionally represented by the Slice Manager block in Figure 36 and Figure 37) to allocate InP network resources to VNOs based on requests and tasks received from VNO Management Systems.

VNOs have access to the allocated network resources via their own vAN representation (vAN_n).
The Slice Manager MUST expose InP network resources to VNOs via a programmable FANS API (O_{CCO}-$N_{f\text{-}sdn\text{-}access}$ in Figure 36 and Figure 37).

[R-039] The Slice Manager MUST expose full control of the InP network resources to the InP via an unconstrained FANS API.

[R-040] The InP unconstrained FANS API SHOULD comply, as a superset of service elements and parameters, with the O_{CCO}-$N_{f\text{-}sdn\text{-}access}$ interface specified in the relevant section of WT-411 [31].

[R-041] It SHOULD be possible to tailor the FANS API exposed to each VNO via programmable logics/constraints to implement:

- basic FANS service(s) characteristics based on VNOs/InP collective service agreements and, if applicable, regulatory provisions
- VNO specific FANS SLA agreed with the InP but not conflicting with the above basic FANS service(s) characteristics

[R-042] The FANS API towards VNOs SHOULD at least expose the service elements and parameters and comply with the requirements of the Os-Ma-ccodo interface specified in the relevant section of WT-411 [31].[1]

Note: the support of O-VLAN parameters is fundamental to deploy a scalable and efficient FANS solution. For already deployed physical Access Nodes, such support is to be considered optional although strongly recommended.

[R-043] The Slice Manager MUST accept VNO requests only if compliant with the basic service and SLA logics/constraints and pass them to the Resource Mapper.

[R-044] The Resource Mapper MUST ultimately accept/reject a VNO request based on resource availability, bandwidth allocation strategies and the overall overbooking agreed with all VNOs. This MAY be implemented via (programmable) traffic engineering logics/contraints in the Resource Mapper.

[1] This requirement is intended to become mandatory once the referenced specification is published.

[R-045] The Access SDN Manager and Controller MUST send a notification to the VNO Management Systems whether a request was accepted or not.

[R-046] The Access SDN Manager and Controller MUST support roll-back on partially executed VNO requests.

[R-047] The Resource Mapper MUST maintain the correspondence between the physical/logical resources in the pAN representation and those allocated to the VNOs in their own network representations (vAN_n).

[R-048] The Resource Mapper MUST guarantee separation of VNO domains by appropriate segregation of VNOs' access to their own vAN representations.

For the SDN-based FANS solution represented in Figure 38 the following requirements apply:

[R-049] The Access and the Aggregation SDN Manager and Controller elements MUST maintain abstracted representations (pAN and pAggN respectively) of the physical Access Nodes and the Aggregation Nodes and keep these representations aligned with the physical Access Nodes and the Aggregation Nodes themselves in terms of configuration, alarms and events.

[R-050] The Network Orchestrator MUST implement slicing mechanisms (functionally represented by the Slice Manager block in Figure 38) to allocate InP network resources to VNOs based on requests and tasks received from VNO Management Systems

VNOs have access to the allocated network resources via their own virtual network representation ($Slice_n$) which combines the VNOs access and aggregation network representations (vAN_n and $vAggN_n$).

[R-051] The Slice Manager MUST guarantee separation of VNO domains by appropriate segregation of VNOs' access to their own Slice representations.

[R-052] The Slice Manager MUST expose InP network resources to VNOs via a programmable FANS API (Os-Ma-ccodo in Figure 38).

[R-053] The Slice Manager MUST expose full control of the InP network resources to the InP via an unconstrained FANS API.

[R-054] The InP unconstrained FANS API SHOULD comply, as a superset of service elements and parameters, with:

- the O_{CCO}-$N_{f\text{-}sdn\text{-}access}$ interface specified in the relevant section of WT-411 [31] for the Access domain.[2]

Note: The interfaces for the Aggregation domain are not yet defined in WT-411 [31].

[R-055] The FANS API SHOULD be tailored to each VNO via programmable logics/constraints to implement:

- basic FANS service(s) characteristics based on VNOs/InP collective service agreements and, if applicable, regulatory provisions
- VNO specific FANS SLA agreed with the InP but not conflicting with the above basic FANS service(s) characteristics

[R-056] The FANS API towards VNOs SHOULD at least expose the service elements and parameters and comply with the requirements of the Os-Ma-ccodo interface specified in the relevant section of WT-411 [30].[3]

Note: the support of O-VLAN parameters is fundamental to deploy a scalable and efficient FANS solution. For already deployed physical Access Nodes, such support is to be considered optional although strongly recommended.

[R-057] The Slice Manager MUST accept VNO requests only if compliant with the basic service and SLA logics/constraints, translate them into domain-scoped requests before passing them to the Access and the Aggregation Resource Mappers.

[2] This requirement is intended to become mandatory once the referenced specification is published.
[3] This requirement is intended to become mandatory once the referenced specification is published.

[R-058] The Access and the Aggregation Resource Mappers MUST ultimately accept/reject a VNO request based on resource availability, bandwidth allocation strategies and the overall overbooking agreed with all VNOs. This MAY be implemented via (programmable) traffic engineering logics/constraints in the Resource Mappers.

[R-059] The Network Orchestrator MUST send a notification to the VNO Management Systems whether a request was accepted or not. This is based on whether or not the Access and the Aggregation SDN Manager and Controller accepted the corresponding requests.

[R-060] The Network Orchestrator, the Access and the Aggregation SDN Manager and Controller MUST support roll-back on partially executed VNO requests.

[R-061] The Access and the Aggregation Resource Mappers MUST maintain the correspondence between the physical/logical resources in the pAN and pAggN representations respectively and those allocated to the VNOs in their own network representations ($vAN_n$and $vAggN_n$ respectively).

7.4.4 BAA Layer Requirements

If the FANS management and control architecture includes a BAA Layer separate from the Access SDN Manager and Controller, the following requirements apply:

[R-062] The BAA Layer NAI and SAI MUST comply with section 5.2 of TR-413 [25].

8 OAM and Other Operational Aspects

As shown in section 5, FANS clearly needs a Management Systems to provide the necessary controls to support the underlying service building blocks.

Management is defined as the set of mechanisms for provisioning new subscribers and operators, controlling network feature delivery, detecting and addressing networking and application troubles.

Many of the management and policy functions that a network operator (InP) has to perform in providing their services are also useful functions that can be exposed to other operators (VNOs) which have business relationships with the InP.

Current OSS/BSS systems need to be assessed with respect to their capability to move from current to dynamic operations. In case of OSS, this includes OSS service fulfilment, inventory and assurance stacks and can be done by consolidating and automating where possible, and by ensuring OSS readiness for dynamic process support. These steps are required in order to play a part in the target OSS for NFV and SDN and to be ready for dynamic operations.

The introduction of the virtualisation concept requires a mix of new and existing solutions for management and security with common interfaces and mechanisms. Based on this, functions can be virtualised when and where it makes sense without affecting the overall framework or processes.

The following sections describe the OAM and other operational aspects as applied to FANS.

8.1 Ethernet OAM

Supporting new services and their underlying network features requires a new set of network management and control interfaces, since each VNO in the FANS architecture has the possibility of choosing their own OAM scheme based on the capabilities of the InP equipment.

In an Ethernet aggregation network, ITU-T Rec. G.8013/Y.1731 [18] and IEEE 802.1ag [19] (so-called CFM: Connectivity Fault Management) standards enable end-to-end service OAM functions to one or more operators networks:

- *ITU-T Rec. G.8013/Y.1731* [18] monitors the performance of Ethernet services on both Ethernet Virtual Connection (EVC) and Class of Service (CoS) basis for the Service Level Agreement (SLA) assurance
- *IEEE 802.1ag* [19] improves reliability with OAM tools for instant fault notification and rapid fault isolation

End-to-end Service OAM spans the entire Ethernet network between demarcation points at each customer location (UNI to UNI). Ethernet OAM frames are forwarded on the same route as the user Ethernet flow.

It should be noted that no new requirement is needed for the Residential Gateway (RG) or MS-BNG in the FANS architecture because these nodes already support existing requirements for OAM.
Furthermore, the Ethernet OAM model for FANS has to be compliant with the multiple maintenance levels already leveraged in both TR-101 [2], TR-178 [3] and later architectures, to support the ability for each operator to handle their own OAM scheme, independently of the underlying transport and/or virtualisation technology.

The Management System model (5.1), does not introduce any change in the existing OAM, while for the virtual Access Node model (5.2) the OAM has to support the introduction of virtual Access Node (vAN) and virtual Aggregation Node (vAggN).

Figure 45 and Figure 46 depict the OAM model in the case of InP and VNO management respectively for the FANS architecture.

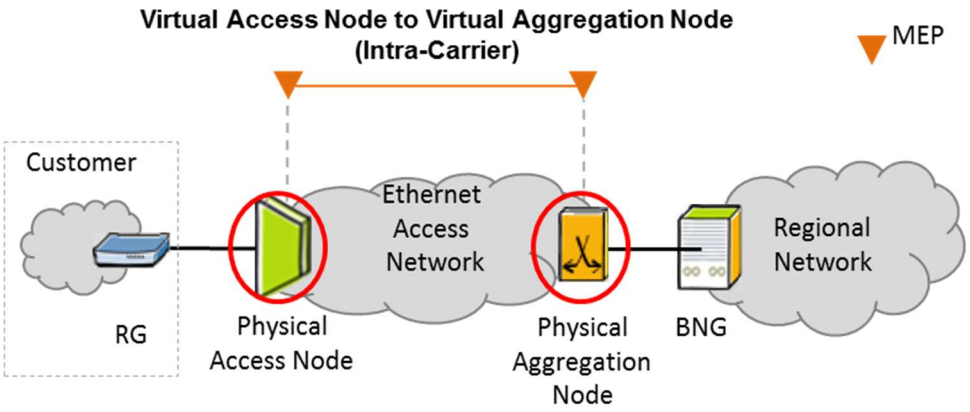


Figure 45 – Extension of TR-101 [2] to FANS: InP OAM

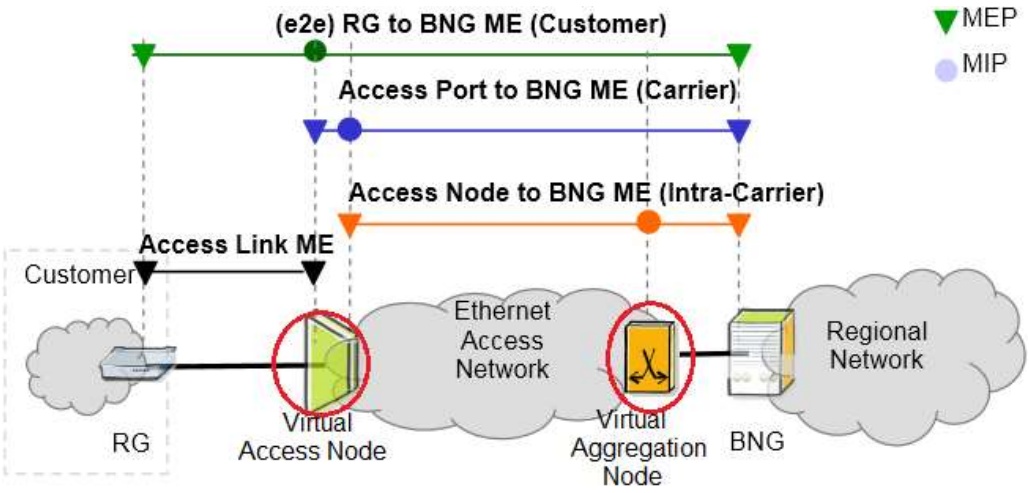


Figure 46 – Extension of TR-101 [2] to FANS: VNO OAM

As shown in the above figures, each stakeholder in FANS has its own set of OAM functionality.
InP supports Maintenance Points (MPs) only at Intra-Carrier level, between physical Access Node and physical Aggregation Node, while the VNO at Customer, Carrier, Intra-Carrier and Access Link levels, on a per VLAN basis. Thus, a VNO is in charge of monitoring the end-to-end service while InP provides the monitoring of the service transport across its network.

8.2 Other Operational Aspects

The relationship between InP and VNO is a business to business relationship and eTOM model is described in [21].

8.2.1 Customer Relationship Management

Customer Relationship Management (CRM) systems allow operators to manage business relationships, data and information associated with them. In general, CRM processes (Figure 47) regard customer service and support, whether storefront, telephone, web or field service. They are also concerned with retention management, cross-selling, up-selling and direct marketing for the purpose of selling to customers.

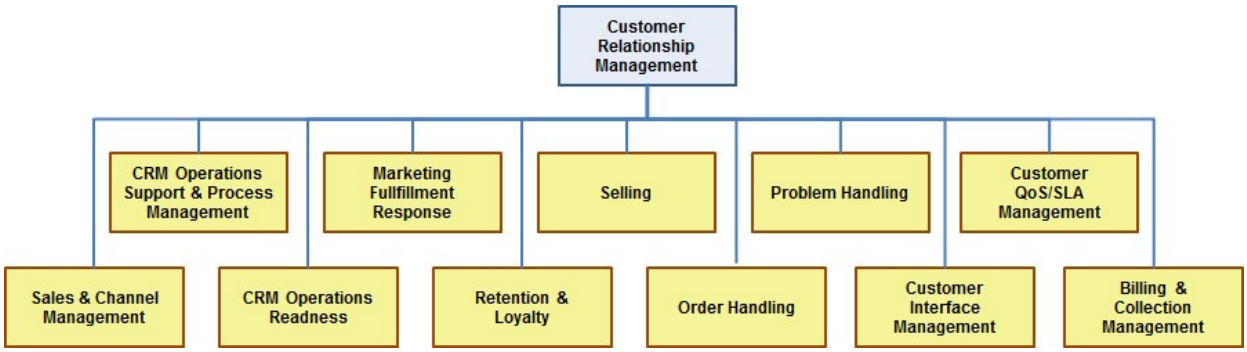


Figure 47 – eTOM CRM Processes

Actors & Involved Processes - CRM	
InP	**VNO**
CRM Operations Support & Process Management	CRM Operations Support & Process Management
	Marketing Fulfillment Response
	Selling
Problem handling	Problem handling
Customer QoS/SLA Management	Customer QoS/SLA Management
	Sales & Channel Management
CRM Operations Readiness	CRM Operations Readiness
	Retention & Loyalty
Order Handling	Order Handling
	Customer Interface Management
Billing & Collections Management	Billing & Collections Management

Table 1 – Actors & Involved Processes: CRM

Table 1 shows the processes in which InP and VNO are involved. Note that some of these processes involve both parties, this means that an operator has to expose at least an interface toward the other one, to communicate information or operating instructions.

8.2.2 Service Management and Operations

Service Management & Operations (SM&O) focus on the knowledge of services (Access, Connectivity, Content, etc.) and include all the functionalities needed for the management and operation of communications and information services required by customers.
The scope is service delivery and management as opposed to the management of the underlying network and information technology.
These processes are accountable to the business management layer function of product management (the profit and loss accountability) to meet, at a minimum, targets set for Service Quality, including process performance and customer satisfaction at a service level, as well as Service Cost.

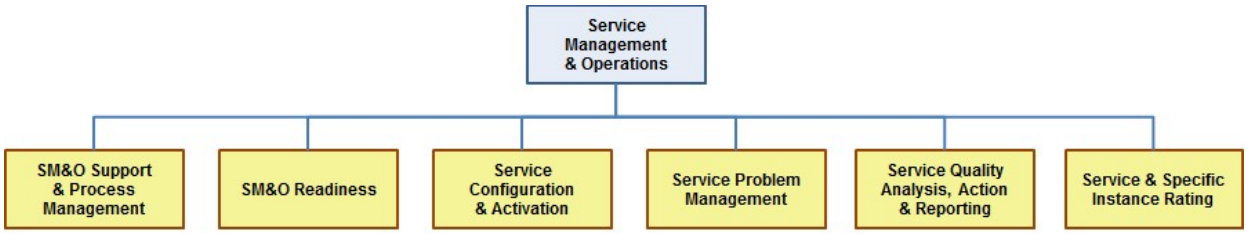


Figure 48 – eTOM SM&O Processes

Table 2 shows the processes in which InP and VNO are involved as actors. Note that some of these processes involve both parties, this means that an operator has to expose at least an interface toward the other one, to communicate information or operating instructions.

Actors & Involved Processes - SM&O	
InP	**VNO**
SM&O Support & Process Management	SM&O Support & Process Management
SM&O Readiness	SM&O Readiness
	Service Configuration & Activation
Service Problem Management	Service Problem Management
	Service Quality Analysis, Action & Reporting
	Service & Specific Instance Rating

Table 2 – Actors & Involved Processes: SM&O

8.2.3 Resource Management and Operations

Resource Management & Operations (RM&O) maintains knowledge of resources (application, computing and network infrastructures) and is responsible for the direct management of all these resources (e.g., networks, IT systems, servers, routers, etc.) used to deliver and support services required by customers. It is also responsible for ensuring that the network and information technologies infrastructure supports the end-to-end delivery of the required services.

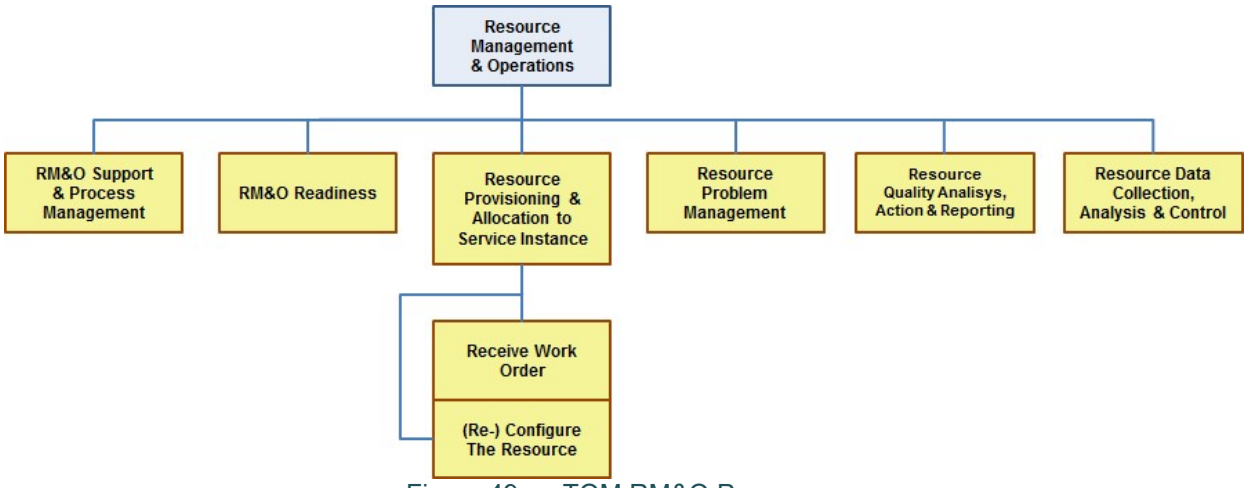


Figure 49 – eTOM RM&O Processes

Table 3 shows the processes in which InP and VNO are involved as actors. Note that some of these processes involve both parties, this means that an operator has to expose at least an interface toward the other one, to communicate information or operating instructions.

Actors & Involved Processes - RM&O	
InP	**VNO**
RM&O Support & Process Management	RM&O Support & Process Management
RM&O Readiness	RM&O Readiness
Resource Provisioning & Allocation to Service Instance	Resource Provisioning & Allocation to Service Instance
Resource Problem Management	Resource Problem Management
Resource Data Collection, Analysis & Control	Resource Data Collection, Analysis & Control
	Receive Work Order
Re/Configure the Resource	Re/Configure the Resource

Table 3 – Actors & Involved Processes: RM&O

9 Privacy and Security

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. In general, two ways to ensure privacy can be recognized:

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

Security is a complex issue but many threats can be easily identified. They are based on a risk assessment of the network, history of attacks against similar networks, or a combination of both. The overall security solution should include measures for physical security that include anti-theft, anti-physical-damage, and anti-data-snooping/stealing measures.

In FANS, privacy mainly involves the isolation of end users' networks and VNOs' networks. This means that each end user network and VNO network is isolated from all other networks that are deployed using the same physical network. InP and VNOs have to adapt their operating procedures and systems to guarantee the end users' isolation and to prevent access to an end user network by unauthorized users. The InP as the owner of the shared infrastructure, must meet the following requirements:

- guarantee the isolation of the entire infrastructure, preventing access by unauthorized users
- respect the VLAN isolation for the VNOs

This document does not define any specific mechanisms to support lawful intercept, but this feature is not precluded since FANS maintains backward compatibility with existing architectures.

In Ethernet-based access networks, network security plays a significant role for the network operators. The FANS architecture does not introduce any additional vulnerabilities over those of standard Ethernet bridging, at least regarding the physical architecture. The FANS architecture runs on the physical infrastructure and thus, security relies on the mechanisms used for physical infrastructure, as defined in TR-101 [2] and TR-178 [3]. Hardware and physical environment security is essential. If physical security cannot be ensured, attackers may get access to sensitive data by exploiting vulnerabilities in physical security.

On the other hand, in the FANS virtual Access Node model (5.2.1), the introduction of virtualisation leads to complex security implications, but it can also provide a better isolation of both end users, VNOs and operators networks.

In practice network virtual partitions have limited vulnerability to outside attacks, since outsiders cannot inspect or inject packets within a virtual network partition from the outside.

Being based on Ethernet access network, a first level of privacy and security in the FANS architecture can be established through three approaches, according to what is described in section 5.2.6:

- Operator VLAN (O-VLAN) tunnels
- MPLS tunnels
- VXLAN tunnels

These techniques support isolation of the traffic from different VNOs. A VNO can thus maintain its existing VLAN mapping for its own customer base, solving both privacy and security issues.

It is important to note that in the FANS virtual Access Node model (5.2.1), security aspects have to be evaluated in a different way compared with traditional networks, since a virtualised environment could be exposed to external attacks that are not expected within the traditional network architectures.

The introduction of virtualisation requires a mix of new and existing solutions for management and security with common interfaces and mechanisms:

- Network Security – including anti DDoS for vAN, security transport, etc.
- Virtualisation System Security – including CPU/memory/disk/IO isolation, hypervisor scheduling mechanisms, anti-virus system, etc.

- Application Security – including data storage security, login security, management security, etc.

Security of the Centralised Management System is an important part of the overall security solution in FANS. To protect it against unauthorized intrusion and misuse, it is essential to restrict user access to the management interface and enforce access security policies like setting up password restrictions.

Best practise would be to divide into different domains. Domains are defined based on different service levels for easy management of network security, which shows a clearer structure of the network. When an attack occurs, it will be isolated in the domain.

Moreover, it is important to cover the security of interfaces. The information exchanged through the northbound or the southbound interfaces are important and thus should be secured properly.
For this reason, the following aspects need to be considered:

- Authentication
- Authorization (how access rights are determined and managed)
- Privacy
- Auditing (how valid and denied accesses are logged and how these records are made available to those entitled to access them)

In general, the security of the infrastructure network domain, hypervisor domain, compute domain and network application domain should leverage the applicable security guidelines outlined in the existing standards development organizations and industry forums.

Appendix I.Access Technologies (Informative)

The scope of this annex is to give some information on how to implement the FANS architecture in different access technologies, like FTTC/B/dp/H. This helps developers to better understand the impact of FANS in the different components of the access architecture.

Fibre to the x (FTTx) is a term which represents various optical fibre delivery topologies that are categorized according to where the fibre terminates in the connection of Subtending Access Nodes.
FTTx specifies the level of penetration of Optical Network Unit (ONU) in the last-mile access networks. For the scope of the FANS, the following technologies will be considered:

- **FTTC (Fibre To The Curb/Cabinet)** – It extends the optical infrastructure from the office, which is typically at the site of the MDF (Main Distribution Frame), to the Street Cabinet (SC) or to a cluster of them.
- **FTTdp (Fibre To The distribution point)** – It is very similar to FTTC but in this scenario the fibre infrastructure terminates closer to the boundary of the customer premise, [30].
- **FTTB (Fibre To The Building)** – Also this architecture is very similar to FTTC and FTTdp, where the fibre infrastructure terminates at the basement of a multi-dwelling unit and each apartment is connected by using existing copper infrastructure.
- **FTTH (Fibre To The Home)** – It is realised when the fibre network is available directly to the customer site (e.g., fibre is terminated within the customers apartment or office space). In this case the ONU is called Optical Network Termination (ONT).

The following Figure 50 depicts a typical legacy access architecture with different FTTx options, such as FTTCab, FTTB/C and FTTH.

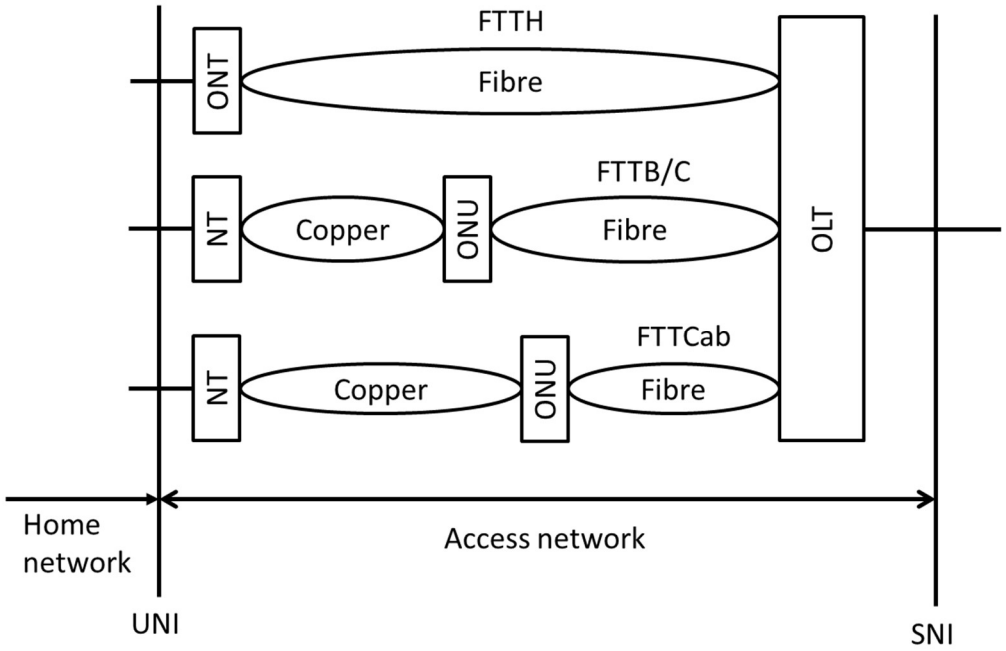


Figure 50 – FTTx Access Network Architecture

A Passive Optical Network (PON) Optical Line Terminator (OLT) provides termination of multiple customer broadband and telecommunications endpoints and serves as a first-level aggregation point. Multiple OLTs could be aggregated together by an Ethernet aggregation switch, which in turn forwards the traffic to a broadband network gateway.

In the figure, the reach indicated as “Fibre” represents the Optical Access Network (OAN) and shows that both ONT/NT and OLT have an interface (respectively UNI and SNI) that depends on which services are provided by the operator.
The OLT and ONU share the responsibility for Access Node VLAN requirements as specified in TR-101 [2] and TR-178 [3]. In detail:

- ONU assumes the responsibility of ingress traffic classification for the U interface. ONUs potentially terminate multiple services and may have different types of U interfaces
- OLT assumes the responsibility of ingress traffic classification for the V interface. The OLT is the first aggregation point in a PON access scenarios

TR-101 [2]specifies 3 different VLAN architectures:

- Residential/Business 1:1
- Residential/Business N:1
- Business TLS

These models are also supported in FANS scenario. Examples are shown in the following Figure 51, Figure 52 and Figure 53 in the case of a GPON network.

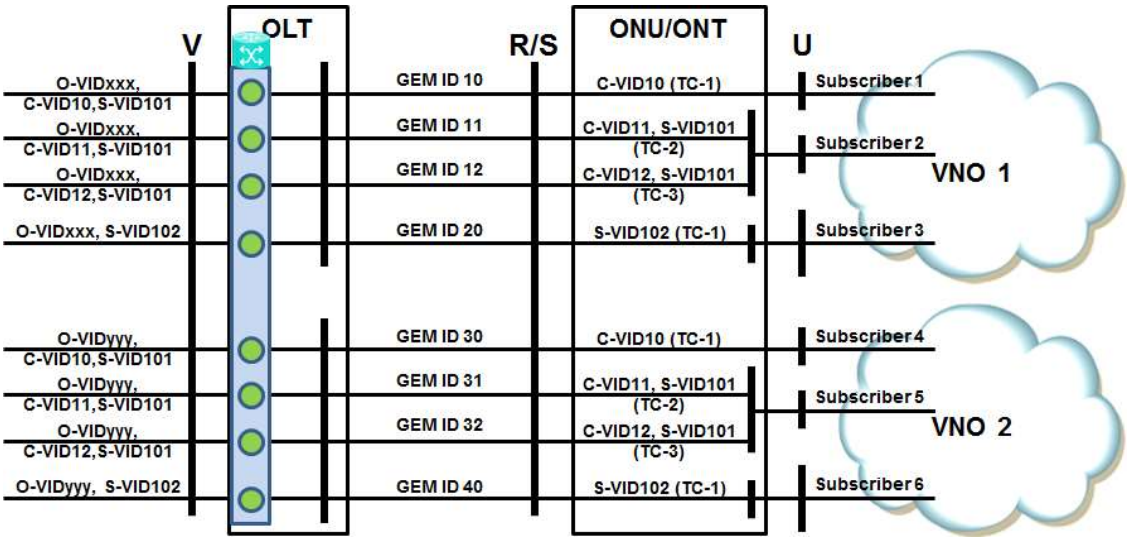


Figure 51 – FANS 1:1 VLAN Architecture Example

The above Figure 51 depicts a 1:1 VLAN architecture. The ONT maps each 1:1 VLAN into a unique U interface. The traffic at V interface in upstream direction could be double-tagged or single-tagged:

- For double-tagged VLANs, the ONT:
  - can either assign a C-VLAN ID or translate a C-VLAN ID, while the OLT adds the S-VLAN ID and the O-VLAN ID (Subscriber 1 and Subscriber 4)
  - can assign S-C VLAN IDs to incoming traffic, while the OLT adds the O-VLAN ID and passes through the traffic (Subscriber 2 and Subscriber 5)
- For single-tagged VLAN, the ONT adds the S-VLAN ID or translates an incoming tag to S-VLAN ID, while the OLT adds the O-VLAN ID and passes through the traffic (Subscriber 3 and Subscriber 6)

In the downstream direction, the OLT removes the outer tags or passes through the traffic to proper GEM port (based on the S-tag value and priority bits). The ONT removes the tags and forwards frames from the GEM port to its associated U interface.

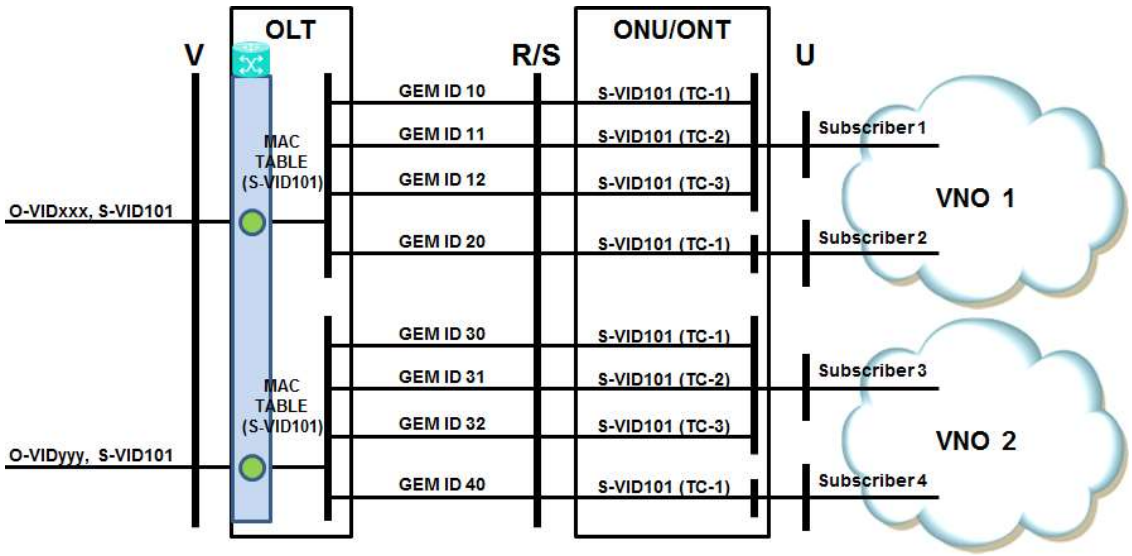


Figure 52 – FANS N:1 VLAN Architecture Example

For N:1 model, the ONT adds the S-VLAN ID or translate an incoming tag to S-VLAN ID for upstream traffic. The OLT adds the O-VLAN ID and will pass-through any upstream traffic with S-VLAN ID on them.

In the downstream direction, the OLT passes through the traffic with O-VLAN ID and S-VLAN ID to the ONT by determining GEM Port (based on MAC address and priority bits). The ONT will remove the S-tag and forward frames from the GEM Port to appropriate U interface.

For TLS VLAN model, the ONU maps each U interface into one or more unique S-VLANs. In this model there are two mutually exclusive methods of subscriber tag assignment:

- Single-tagged, priority-tagged or untagged subscriber packets
- Double-tagged subscriber packets

In the first method a S-Tag is added at the ONU for upstream traffic and is passed through at the OLT, in addition to the O-VLAN ID added by OLT. In the downstream direction, the OLT passes the packet through again, and the S-Tag is removed at the ONU before forwarding traffic to the U interface. For this method, the subscriber can identify optional non-TLS VLANs with specific Q-Tags.

In the second method, frames with valid S-Tags are accepted and may be translated to new values at the ONU. Frames with invalid S-Tags are silently discarded. In both directions the frames are passed through the OLT, in addition to the O-VLAN ID added by OLT.

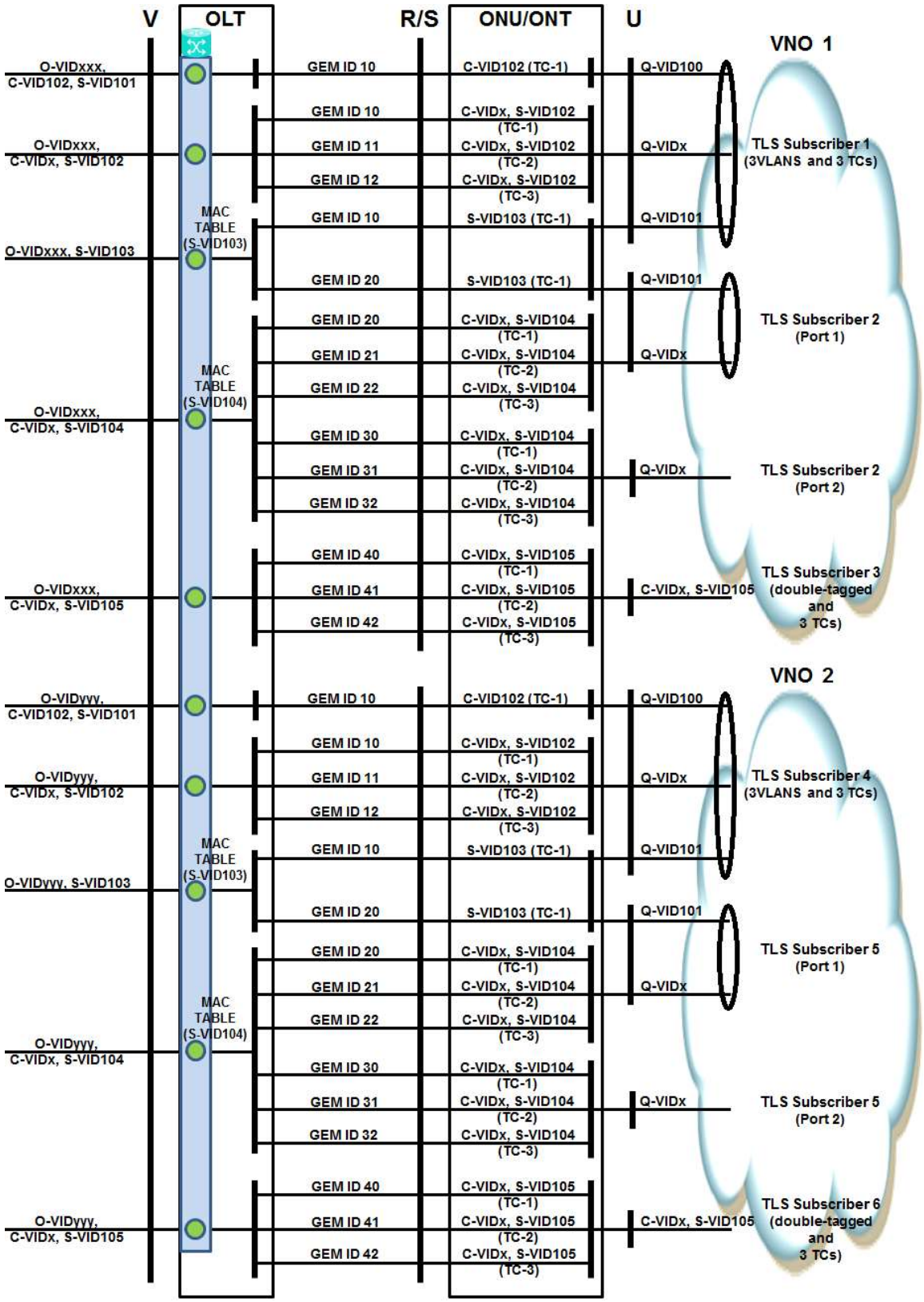


Figure 53 – FANS TLS VLAN Architecture Example

Figure 54 describes the mapping of physical ports to virtual ports in case of FTTC/FTTdp/FTTB. It can be noted that in this case the approach is based on Shared ONU as the same ONU includes connections of multiple virtual operators.

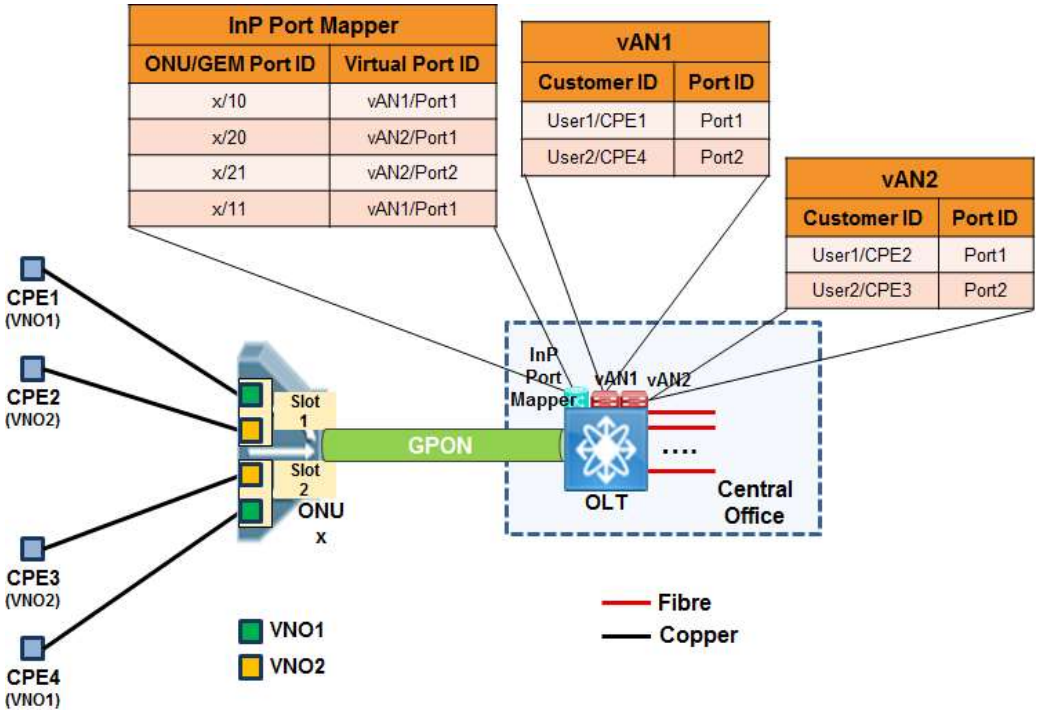


Figure 54 – Customers management in FANS FTTC/FTTdp/FTTB architectures

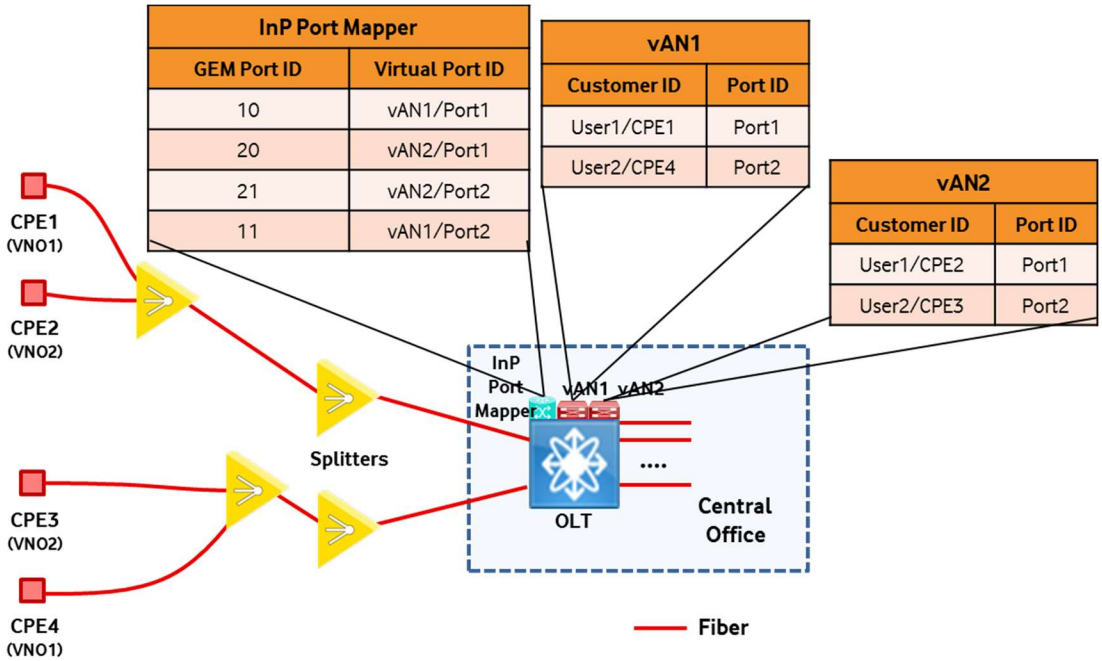


Figure 55 – Customers management in FANS FTTH architecture

As shown in Figure 54, the InP Port Mapper Table contains one-to-one relationships between physical port IDs and virtual port IDs, while each vAN instance, as mentioned in section 5.2.1, provides similar functions to

those of a physical AN (pAN), thus maintaining information on the customer connected and the port (virtual) on which the customer is terminated.

Figure 55 describes the mapping of physical ports to virtual ports in case of FTTH. It can be noted that in this case the approach is based on Dedicated ONU as the each ONU is owned and managed by a single virtual operator. Thus, the InP Port Mapper Table contains one-to-one relationships between GEM Port IDs and Virtual Port IDs, while the relationship table for each vAN instance is similar to the previous case (Shared ONU).

End of Broadband Forum Technical Report TR-370