

TR-386

Fixed Access Network Sharing - Access Network Sharing Interfaces

Issue:2

Issue Date: June 2024

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	Issues Editor	Changes
1	16 January 2019	16 January 2019	Peter Silverman, ASSIA Bruno Cornaglia, Vodafone	Original
2	10 June 2024	10 June 2024	Jan Diestelmans, Nokia Haomian Zheng, Huawei	Aligned with TR-370i2

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

Editor	Jan Diestelmans Haomian Zheng	Nokia Huawei
Work Area Director(s)	Bruno Cornaglia Mengmeng Li Haomian Zheng	Vodafone China Mobile Huawei
Project Stream Leader	Ken Kerpez	DZS

Table of Contents

Executive Summary	6
1 Purpose and Scope	7
1.1 Purpose	7
1.2 Scope	7
2 References and Terminology	8
2.1 Conventions	8
2.2 References	8
2.3 Definitions	10
2.4 Abbreviations	10
3 Technical Report Impact	13
3.1 Energy Efficiency	13
3.2 IPv6	13
3.3 Security	13
3.4 Privacy	13
4 System Overview	16
4.1 Centralized Management System (CMS)	17
4.2 VNO Management System	19
4.3 Virtual Access Node	21
4.4 InP Port Mapper	22
4.5 Virtual Switch	22
4.6 Physical Access Node	22
4.7 Server	22
4.8 Access SDN Manager & Controller	22
4.9 Slice Manager	23
4.10 Resource Mapper	23
5 Interface Definitions	24
5.1 Os-Ma-nfvo/Occo-Nf-sdn	24
5.2 Minf	25
5.3 Ve-Vnfm	26
5.3.1 Port Status and Alarms	26
6 FANS NETCONF/YANG interface definition	29
6.1 Basic principles	29
6.2 Achieving VNO access control	30
Annex A: FANS YANG Modules	31
Dependencies on related YANG modules and standards	31

List of Figures

Figure 1 – Management System Overview [1]	14
Figure 2 – FANS Models [1]:	15
Figure 3 – Centralized Management System	18
Figure 4 – Centralized Management System connections	19
Figure 5 – VNO Management System: High-Level Vision	20
Figure 6 – Provisioning: High-Level Vision	21
Figure 7 – Migration: High-Level Vision	21
Figure 8 – Virtual Port State Machine	26
Figure 9 – Virtual Port Alarm propagation in the xPON YANG Model	28

List of Tables

Table 1 – Applicability of Components in different models	16
Table 2 – FANS YANG Modules	31

Executive Summary

This Technical Report specifies the system interfaces associated with FANS. This document provides details and the information required to define these interfaces as well as the rules for communicating with them. The interfaces described are defined in TR-370i2 “FANS – Architecture and Nodal Requirements”. An overview of the interfaces required for TR-370i2 based systems is provided in section 4, while the interface definitions are provided in section 5. Section 6 provides an overview of how YANG models can be used to support these interfaces.

1 Purpose and Scope

1.1 Purpose

This Technical Report specifies the system interfaces associated with FANS. This document provides the information required to define these interfaces as well as rules for communicating with them.

The interfaces are those identified in TR-370i2 “FANS – Architecture and Nodal Requirements” [1].

This Technical Report covers:

- 1) Specification of the interfaces required by FANS.
- 2) Description of the capabilities exposed by FANS interfaces between the VNOs and InP.
- 3) Representation of the interfaces exposed by FANS systems, and the data exchanged across those interfaces.
- 4) Specification of the critical issues and operations pertaining to the delivery of information between FANS systems via the shared interfaces.

1.2 Scope

The scope of this Technical Report is to extend TR-370i2 *Fixed Access Network Sharing – Architecture and Nodal Requirements* [1] with details of the system interfaces involved in information exchange across FANS systems.

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 in RFC 2119 [9].

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

2.2 References

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

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

Document	Title	Source	Year
[1] TR-370i2	<i>Fixed Access Network Sharing – Architecture and Nodal Requirements</i>	BBF	2020
[2] TR-355a4	<i>YANG Modules for FTTdp Management</i>	BBF	2022
[3] TR-349	<i>DSL Data Sharing</i>	BBF	2016
[4] TR-298i2	<i>Management model for DSL line test</i>	BBF	2017

[5]	TR-252i3	<i>xDSL Protocol-Independent Management Model</i>	BBF	2013
[6]	TR-383a7	<i>Common YANG Modules</i>	BBF	2023
[7]	TR-371	<i>G.fast Vector of Profiles (VoP) Managed Object Structure</i>	BBF	2016
[8]	TR-413	<i>SDN Management and Control Interfaces for CloudCO Network Functions</i>	BBF	2018
[9]	RFC 2119	<i>Key words for use in RFCs to Indicate Requirement Levels</i>	IETF	Mar. 1997
[10]	RFC 6020	<i>YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF),</i>	IETF	Oct. 2010
[11]	RFC 6022	<i>YANG Module for NETCONF Monitoring</i>	IETF	Oct. 2010
[12]	RFC 6241	<i>Network Configuration Protocol (NETCONF</i>	IETF	Jun. 2011
[13]	RFC 8341	<i>Network Configuration Protocol (NETCONF) Access Control Model</i>	IETF	Mar. 2018
[14]	RFC 6991	<i>Common YANG Data Types</i>	IETF	Jul. 2013
[15]	RFC 7223	<i>A YANG Data Model for Interface Management</i>	IETF	May 2014
[16]	RFC 7224	<i>IANA Interface Type YANG Module</i>	IETF	May 2014
[17]	RFC 7317	<i>A YANG Data Model for System Management</i>	IETF	Aug. 2014
[18]	RFC 7950	<i>The YANG 1.1 Data Modeling Language</i>	IETF	Aug. 2016
[19]	RFC 8632	<i>A YANG Data Model for Alarm Management</i>	IETF	Sep 2019
[20]	G.988	<i>ONU management and control interface (OMCI) specification</i>	ITU-T	Oct 2012
[21]	802.1ag	<i>IEEE Standard for Local and <u>Metropolitan Area Networks</u> Virtual Bridged <u>Local Area Networks</u> Amendment 5: Connectivity Fault Management</i>	IEEE	2007
[22]	802.1ah	<i>IEEE Standard for Local and metropolitan area networks -- Virtual Bridged Local Area Networks Amendment 7: Provider Backbone Bridges</i>	IEEE	2008
[23]	G.8013/Y.1731	<i>Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks</i>	ITU-T	June 2023

- [24] BBF Published <https://github.com/BroadbandForum/yang> BBF 2017
YANG

2.3 Definitions

The following terminology is used in this Technical Report.

Access Node (AN)	The Access Node is a device that 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 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.
Infrastructure Provider	The Infrastructure Provider (InP) typically owns and is responsible for the maintenance of the physical network resources of the network. In this Technical Report it is expected that the InP can make resources available to Virtual Network Operators (VNOs)
Virtual Access Node	<p>The abstraction of the Access Node element created as a process within the physical Access Node itself, a Centralized Management System or as a stand-alone VNF in the NFVI.</p> <p>The Virtual Access Node representation of the physical Access Node is exposed to VNOs for resource consumption.</p>
Virtual Network Operator	The Virtual Network Operator operates, controls, and manages the assigned portion of the Virtual Access Node and may do so over multiple Virtual Access Nodes". 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:

AN	Access Node
----	-------------

BAA	Broadband Access Abstraction
BBF	Broadband Forum
CFM	Connectivity Fault Management
CMS	Centralized Management System
COTS	Commercial-Off-The-Shelf
DSL	Digital Subscriber Line
EMS	Element Management System
FANS	Fixed Access Network Sharing
FCAPS	Fault, Configuration, Accounting, Performance, Security
GPON	Gigabit Passive Optical Network
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
InP	Infrastructure Provider
ITU-T	International Telecommunication Union – Telecommunication Standard Sector
LOF	Loss of Frame
LOS	Loss of Signal
MS	Management System
NACM	NETCONF Access Control Model
NETCONF	Network Configuration Protocol
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Interface
NIC	Network Interface Card
OAM	Operations, Administration, and Maintenance
OLT	Optical Line Terminals
ONU	Optical Network Unit
pAN	Physical Access Node
PNF	Physical Network Functions
PON	Passive Optical Network
RTT	Round Trip Time
SDAN	Software Defined Access Network
SDN	Software Defined Network
SDN M&C	Software Defined Network Management and Control
SLA	Service Level Agreement
TR	Technical Report
UNI	User Network Interface
vAN	Virtual Access Network

VNF	Virtualized Network Functions
VNO	Virtual Network Operator
YANG	Yet Another Next Generation (Data Model Language for NETCONF)

3 Technical Report Impact

3.1 Energy Efficiency

This Technical Report builds upon the architecture principles defined in TR-370i2, i.e., supporting multiple virtual access networks on one single fixed access network. Sharing network resources amongst several Virtual Network Operators (VNOs) avoids having to deploy multiple access network elements in parallel; this potentially reduces the overall network power consumption.

3.2 IPv6

This Technical Report references a variety of YANG modules defined by the Broadband Forum, notably TR-383 that include YANG modules that support IPv6 deployments. Hence this document also includes support for IPv6 deployments. It should be noted that as the actual network sharing methods are defined at Layer 2, each VNO can have its own specific IPv4 and/or IPv6 network.

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.

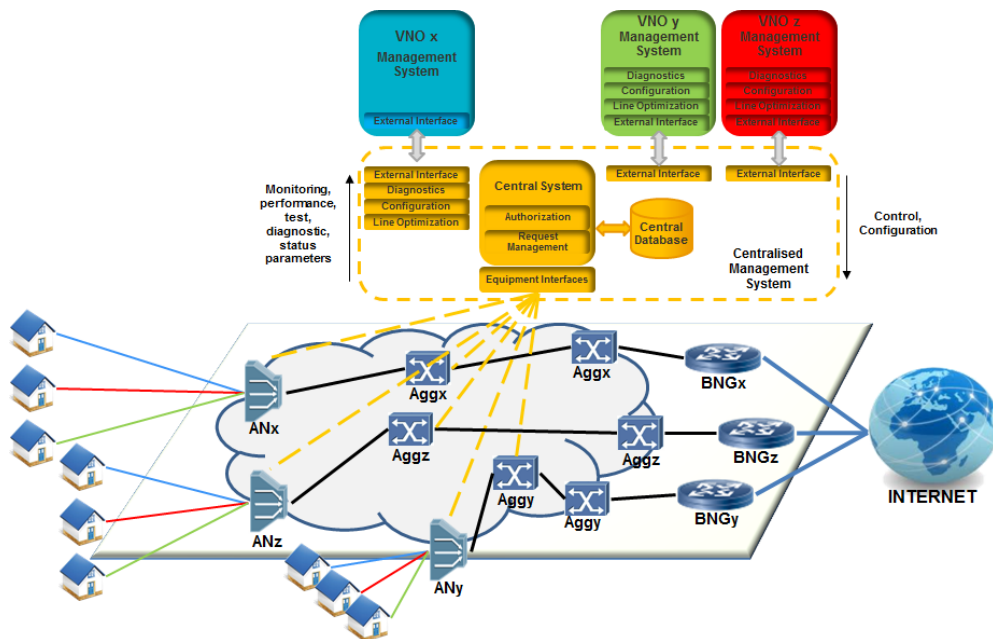


Figure 1 – Management System Overview [1]

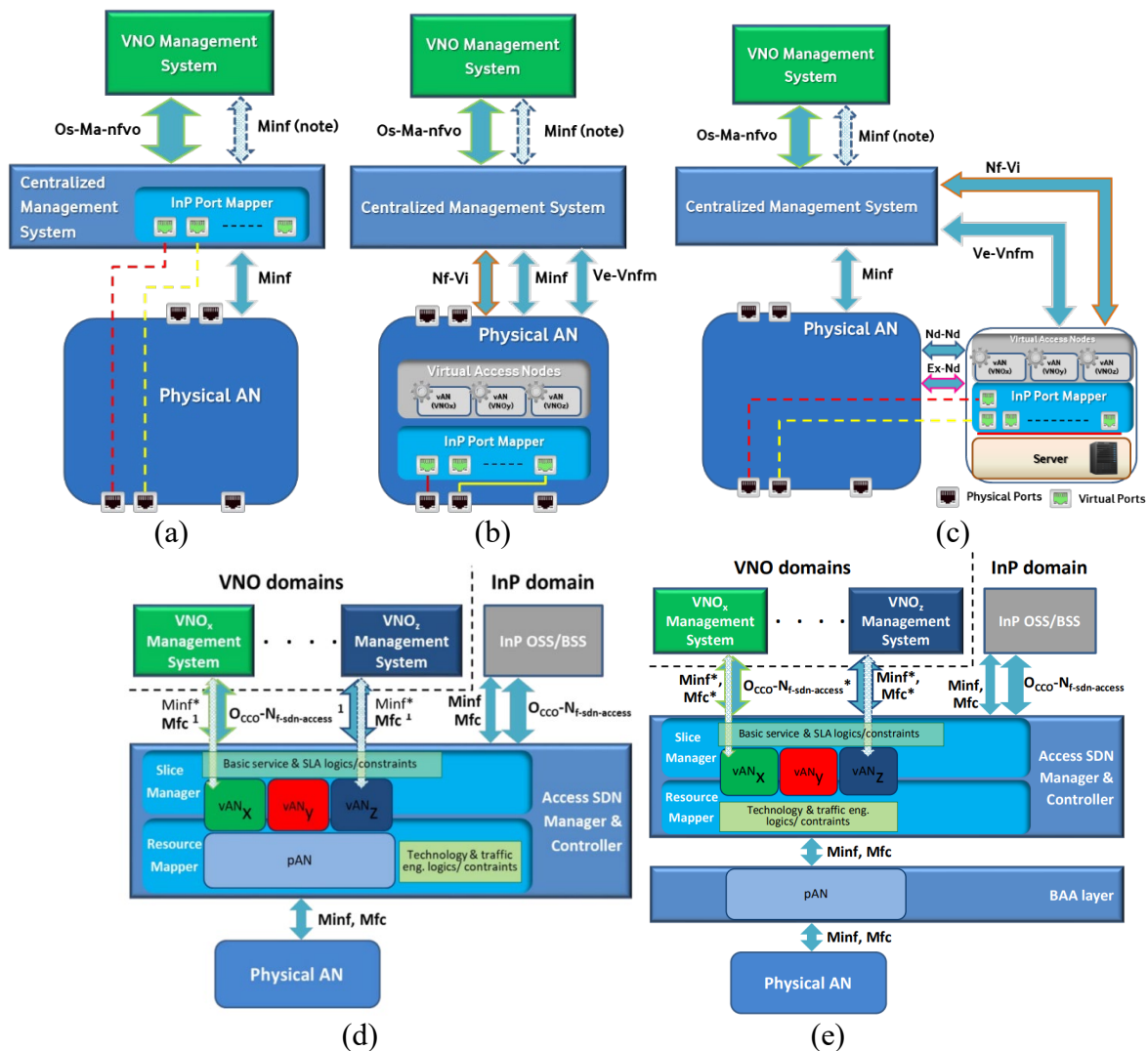


Figure 2 – FANS Models [1]:

- (a) Centralised Management System based FANS
- (b) vAN based FANS (vANs in physical OLT)
- (c) vAN based FANS (vANs in NFVI server)
- (d) SDN-based FANS with embedded BAA layer
- (e) SDN-based FANS with separate BAA layer

Note: Minf interface, i.e., FCAPS parameters, are exposed to VNOs as mediated by the Centralised MS.

4 System Overview

As defined in Section 5 of TR-370i2 [1] document, three models for network sharing can be deployed:

- Management System based (Figure 2(a))
- Virtual Access Node based (Figure 2 (b) and (c)) considering both cases with vAN inside the equipment (b) or in an external server (c)
- SDN-based (Figure 2(d) and (e)) considering both cases with BAA layer embedded (d) or as separate layer (e)

These three models depict a system capable of managing equipment from multiple vendors, and also maintaining backward compatibility. 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.

It is important to note that the solution based on the management system performs the network sharing at the management system level, not directly in the equipment itself. Table 1 reports the applicability of the components for each model:

- Sections 4.1 and 4.4 describe the Centralised management systems and InP Port Mapper for first and second solutions.
- Sections 4.2 and 4.6 describe the VNO management systems and Physical Access Node for all models.

Table 1 – Applicability of Components in different models

	Model 1: CMS-based	Model 2: vAN-based	Model 3: SDN-based
Centralised Management System	X	X	
VNO Management System	X	X	X
Virtual Access Node		X	
InP Port Mapper	X	X	
Virtual Switch		X	
Physical Access Node	X	X	X
Server		X	
Access SDN Manager & Controller			X
Slice Manager			X
Resource Mapper			X

- Sections 4.3, 4.5 and 4.7 sections apply only to the Virtual Access Node model.
- Sections 4.8, 4.9 and 4.10 section apply only to the SDN model.

TR-349 [3] defines interfaces for DSL data sharing that enable configuration, diagnostics and operational status information to be disseminated by an Infrastructure Provider (InP) to multiple VNOs, and which enable the VNO to manage the services they obtain from the InP. In the architectures shown in figures 1 and 2, the interface in TR-349 enables multiple VNOs to request changes in network configurations and to monitor their services across the physical DSL access network provided by an InP. TR-349 specifies the interface required to enable virtualization of the physical layer access in a shared network environment supporting DSL technologies.

TR-349 references the DSL management parameters in TR-252i3 [5], the DSL line test management parameters in TR-298 [4] and the G.fast management parameters in TR-371 [7]. The YANG modules defining all these parameters are in TR-355 [2].

4.1 Centralized Management System (CMS)

The CMS (as defined in Sections 5 and 6.3 of TR-370i2 [1]) is the main component of this model. It orchestrates services between the network and the datacentre, as well as resources across the end-to-end infrastructure. Moreover, it covers and performs centralised functions, providing automated data from network elements (via equipment interfaces) to VNOs (via external interfaces), including:

- Authentication
- Management of the network elements
- Configuration
- Diagnostics
- Line optimization
- Performance monitoring

A central supervisor component (Data Repository) can be placed within the Centralised Management system in order to enforce policies and avoid potential conflicts or discrepancies in resource sharing or line settings among VNOs.

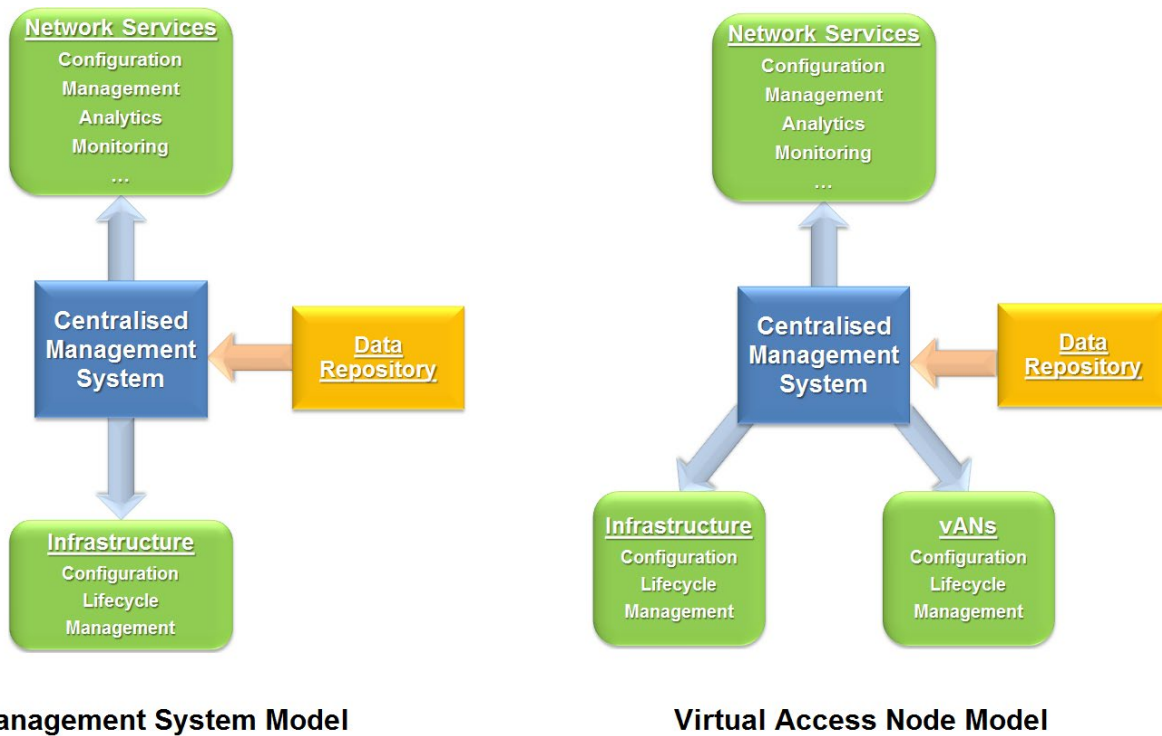


Figure 3 – Centralized Management System

In the Virtual Access Node model, the Centralised Management System is also in charge of coordinating the Virtual Access Node (vAN) instances, in particular to:

- Provide a global view of the network characteristics of the various logical links
- Management of virtual AN instances so as to meet the network requirements specified by InP-VNO agreements
- Manage dynamic changes of the network configuration (e.g., for scaling the capacity of the network services)
- Connectivity over a combination of Physical Network Functions (PNFs) and Virtualised Network Functions (VNFs)
- Support end-to-end network services involving both:
 - internal connectivity – between the components of a VNF making up each virtual Access Node
 - external connectivity – between the various locations of virtual Access Node instances and the PNFs
- Monitor utilisation, and compute paths for abstracted end-to-end network services, based on metrics such as jitter, RTT, delay and bandwidth

The Centralised Management System needs to guarantee service continuity and react to any event to maintain the requested SLA. Moreover, in a traditional environment, the monitoring system is able to collect data regarding the health and performance of application and hardware infrastructure. Since FANS introduces additional layers, the monitoring system also needs to monitor the virtual resources.

Alarms can be generated at the application, virtualization and hardware infrastructure level, and every issued alarm needs to be correlated with ones in others layer that are due to the same problem.

The Centralised Management System in the Virtual Access Node architecture exchanges information with the following entities (Figure 4):

- VNO Management System
- Virtual Access Node
- Physical Access Node
- Server

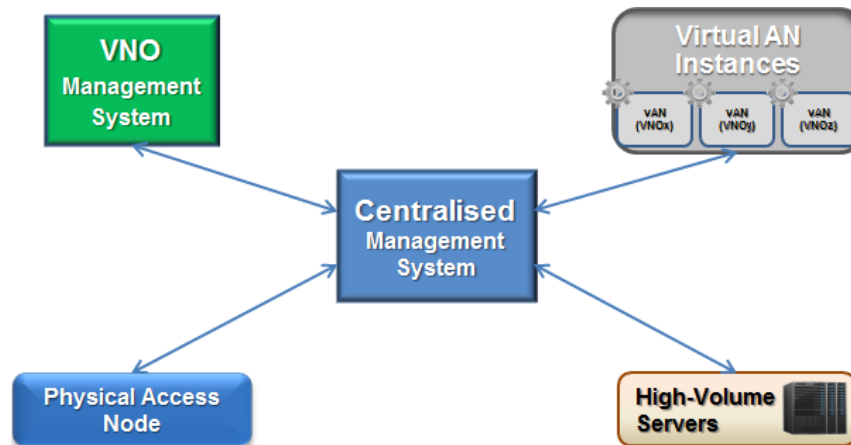


Figure 4 – Centralized Management System connections

More details are provided in Section 5.

4.2 VNO Management System

Since in the FANS model a VNO is more focused on providing commercial services, its Management System (VNO Management System) includes the set of operations and business support functions mainly used for service provisioning:

- Billing
- Order management
- Customer relationship management
- Service delivery
- Service fulfilment (including the network inventory, activation and provisioning)
- Service assurance
- Customer care

However, operations and business functions may also support the management and orchestration of legacy devices (via the Minf reference point exposed by the Centralised Management System, as defined in Section 6.2 of TR-370i2 [1] and TR-413 [8]).

In FANS, the VNO integrates its running virtualised functionalities on top of the InP infrastructure into an end-to-end network service instance. These functionalities and their supporting infrastructure need to be visible for configuration, diagnostic and troubleshooting purposes.

All the above are possible to be managed via the Centralised Management System, while the VNO Management System uses standard interfaces to communicate with Centralized Management System. It is important to note that each VNO maintains its own schema for service models and service management. However, certain operations are common to all VNOs and these are shown in Figure 5.

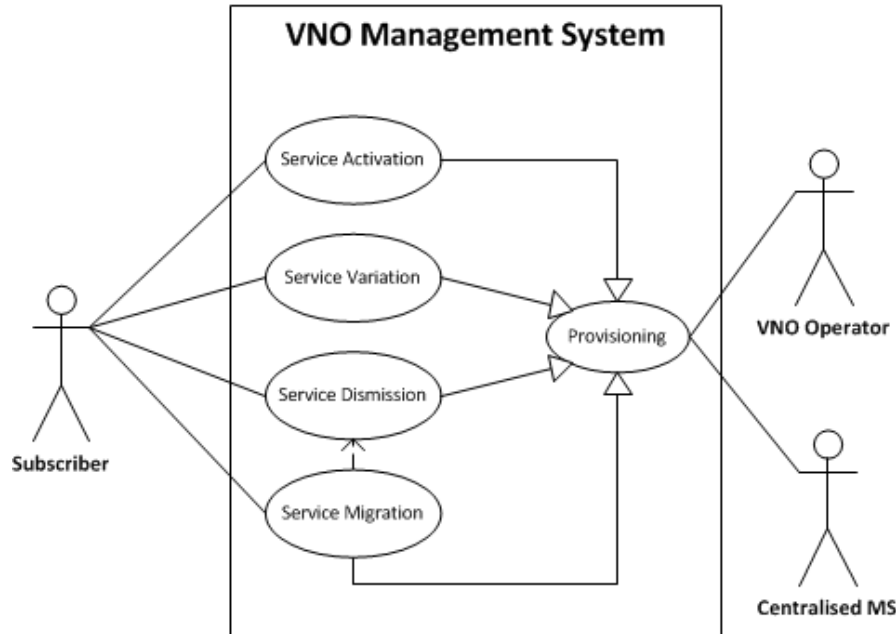


Figure 5 – VNO Management System: High-Level Vision

The main actor is represented by the VNO which can:

- Activate a new service
- Vary an existing service
- Divest an existing service
- Migrate an existing service toward another VNO

Each of the above actions can be interpreted as a “Service Provisioning” for the VNO and as a “Network Provisioning” for the Centralised Management System of FANS. The Service Provisioning is performed by internal VNO systems, while the latter is performed by the Centralised Management System by an exchange of information between it and the VNO MS at the Os-Ma-nfvo reference point.

As mentioned in section 4.1, the CMS is in charge of management of both the physical infrastructure and software resources, as well as the governance of vAN instances that share the resources of the FANS infrastructure. Thus, all tasks mentioned in Figure 6 and Figure 7 are performed by the CMS.

In summary:

- The Transport layer is the responsibility of the InP and thus the CMS
- The Service layer is the responsibility of the VNO via its VNO MS

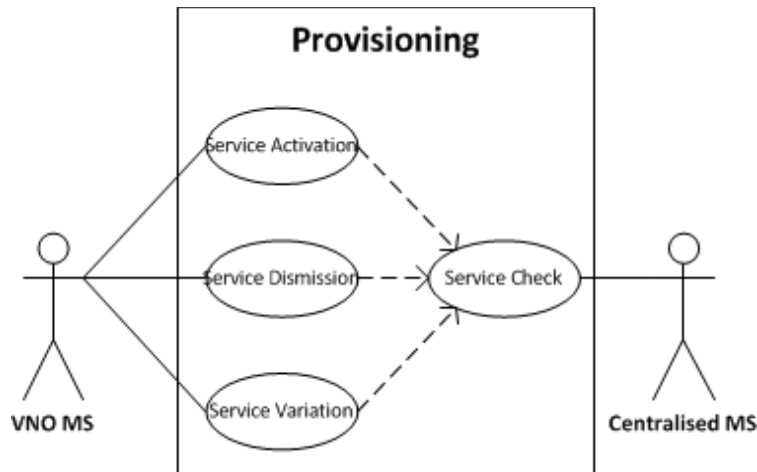


Figure 6 – Provisioning: High-Level Vision

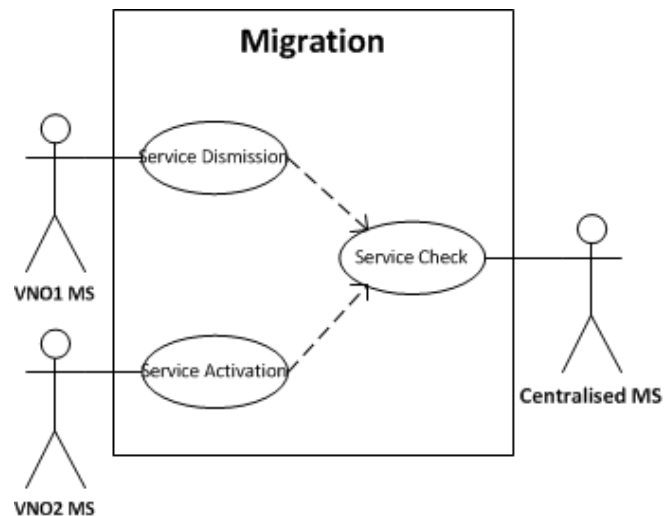


Figure 7 – Migration: High-Level Vision

4.3 Virtual Access Node

A virtual Access Node (vAN) (section 5.2.1 of TR-370i2 [1]) is a telco application that represents the whole set of characteristics of a traditional physical Access Node (NICs and other physical interfaces and cards are excluded).

A vAN is technology agnostic and either shares the physical resources of the Access Node with the other VNOs (section 4.6), or could be deployed on generic Servers (section 4.7) in the InP's data centres.

4.4 InP Port Mapper

The InP Port Mapper (section 5.2.3 of TR-370i2 [1]) is a virtual entity used to map logical ports to the host physical ports. For each VNO, it maps the logical port number used for a customer to that customer's physical port. It also facilitates customer migration between different VNOs terminating on the same physical access node.

4.5 Virtual Switch

A Virtual Switch (section 5.2.1 of TR-370i2 [1]) is a software program, located on a physical access node and responsible for forwarding customer traffic towards the InP Port Mapper (in the downstream). Details of the Virtual Switch are described in TR-370i2 [1].

4.6 Physical Access Node

The physical Access Node (pAN) is the starting point for the connection between the operator network and the customer. The main function of a Physical Access Node is to aggregate traffic from multiple subscribers, and different variants of Access Node can support all the widely deployed access technologies and services as well as the emerging ones.

4.7 Server

Servers can provide part of the physical resource layer needed for FANS. Together with storage, network and I/O interfaces they make up the physical compute domain which is analogous to the orchestration and management domain in an NFV scenario.

The hardware resource pool comprises:

- compute resources based on multi core processors and RAM
- storage resources, such as SSD, HDD or central storage.

The hardware resource pool is based on Commercial-Off-The-Shelf (COTS) hardware, or be provided by physical access nodes. These resources are all managed by the virtualization layer.

4.8 Access SDN Manager & Controller

The Access SDN Manager and Controller (section 5.3 of TR-370i2 [1]) 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 of the Access Nodes, e.g., in the form of a YANG Data Store;

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:

- device share of the access network based on resource requests from VNO domain
- mapping of the device shares (e.g., device share X, Y, Z) to the pAN representation

These tasks are fulfilled respectively by the Slice Manager and the Resource Mapper

4.9 Slice Manager

The slice manager (section 5.3 of TR-370i2 [1]) is responsible for implementing a sharing mechanism for allocating InP network resources to the VNO based on requests and tasks received from the VNO management system.

It is 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

The Slice Manager accepts VNO requests only if compliant with the basic service and SLA logics/constraints and pass them to the Resource Mapper.

4.10 Resource Mapper

The Resource Mapper (section 5.3 of TR-370i2 [1]) ultimately accepts/rejects a VNO request based on resource availability, bandwidth allocation strategies and the overall overbooking agreed with all VNOs.

The Resource Mapper maintains the correspondence between the physical/logical resources in the pAN representation and those allocated to the VNOs in their own network representations.

The Resource Mapper guarantees separation of VNO domains by appropriate segregation of VNO access to their own vAN representations.

5 Interface Definitions

The following sections focus on the Os-Ma-nfvo and Minf interfaces, since the other interfaces that complete the FANS architecture, shown in Section 4, are already defined in the ETSI NFV standard documents. According to TR-370i2 Fig. 29, Minf interface is in charge of the configuration of Access Nodes instead of Os-Ma-nfvo. The following sections focus on the Minf interface between VNO Management System and InP 's Centralized Management System or Access SDN Manager & Controller and Minf interface between InP 's Centralized Management System or Access SDN Manager & Controller and InP's Access Nodes.

The following sections provide a list of functional modules for the Os-Ma-nfvo and Minf interfaces via YANG [10] modeling and NETCONF [12].

YANG allows different VNOs to have different configuration models as follow.

The use of a YANG based interface allows the InP to expose different VNOs to have different configurations.

In a regulated environment it seems more likely that the same interface (in terms of superset, depth and granularity of accessible parameters) is exposed to VNOs for a reason of equivalence of treatment. Then each VNO, in the context of the parameters superset exposed, may agree with the InP to hide and/or abstract certain parameters to customize the FANS interface to its own service models and needs. Again YANG modeling is very suitable for that.

From the operators' perspective it is necessary to separate the handling of configuration data, operational state data, and statistics from network devices, and to make a clear distinction between these entities.

5.1 Os-Ma-nfvo/Occo-Nf-sdn

As depicted in Figure 2, the Os-Ma-nfvo/Occo-Nf-sdn interfaces are the true FANS API as they enable the exchange of requests and data between each VNO Management System and the Centralised Management System or the SDN Controller respectively to allow the configuration of Access Nodes (both Physical and Virtual). The VNO MS is generally not involved in the initial planning and configuration of the access nodes (this being provided by the Centralised Management System or by the SDN controller) but is involved in the activation and ongoing management of subscriber services.

This bidirectional interface can be used for the following purposes, with the understanding that any VNO request is always subject to the brokerage and mediation of the Centralised Management System or of the SDN Controller:

- Assignment of VNO characteristics:
 - Virtual Access Node including access ports and network ports
 - Bandwidth quota on network port or access port, if shared with other VNO
 - Backhaul traffic encapsulation configuration
- Backup/Restore of the vAN
- Equipment Inventory
- Common NMS/EMS related procedures that cannot be managed via the Minf interface:

- Configuration management for the creation/deletion of network links that connect subnetworks
- Configuration management for the creation, modification and deletion of the customer line parameters
- Fault management for assessing the impact of customer line failures
- Security management for partitioning the element layer view and control
- Applying, checking and if necessary rejecting a configuration request

An initial list of YANG modules for the Os-Ma-nfvo/Occo-Nf-sdn interfaces is based on the following modules, already specified in BBF and IETF documents ([6],[17]):

- **ietf-system**: YANG definitions for the configuration and identification of the management system of a device
- **bbf-interfaces-performance-management**: management objects for the reporting of performance management of statistics defined by the IETF interfaces data model “ietf-interfaces”

NOTE: This list is accurate as of the time of publication of this document but is subject to modification when the BBF releases new or modified YANG modules.

[R-1] In order to support FANS, Os-Ma-nfvo SHOULD implement the following function and related Data Model: (bbf-fans-vno)

5.2 Minf

The Minf interfaces is used by the Centralised Management System to interact with the physical ANs. More specifically the Minf interface is used for both FCAPS functionalities and flow control, i.e., the forwarding of flows across the physical node.

Regardless of the FANS architectural options shown in Figure 1 and Figure 2 the VNO Management Systems access to the network resources via the mediation, through the FANS API (Os-Ma-Nfvo), of the Centralised Management System that verifies and reconciles the requests from all the VNOs. Furthermore, the SDN-based solution would also require FANS API (OCCO-Nf-sdn-access interface).

The VNOs requests on the access resources rely on the Os-Ma-Nfvo interface, while the Minf interfaces and the ETSI interfaces are accessible and used only by the Centralised Access SDN Management and Control to access physical resources (Minf) and, when applicable, access virtualized resources (Ve-Vnfm, Nf-Vi).

[R-2] The Minf interface SHOULD comply with TR-413 [8]. In order to support FANS, the following YANG files SHOULD be supported on Minf if not listed in TR-413:

- bbf-fans-vno
- bbf-fans-resource-sharing-descriptor
- bbf-fans-resource-sharing

The Minf interface model consists of a few functional modules, including a generic bbf-fans which can be used in different functionalities, a pair of management modules and a pair of resource modules.

Note: TR-413 [8] also specifies an Mfc interface for controlling packet flows on physical ANs.

This is not yet captured in this Technical Report nor defined in TR-370i2 [1].

5.3 Ve-Vnfm

This interface is applicable only to the Virtual Access Node model and provides lifecycle management of the vANs, implemented as VNFs, managed by the Centralised Management System which for this model is required to support VNF Manager functionalities in addition to those of Access Manager & Controller which are common to both FANS models.

5.3.1 Port Status and Alarms

As described in TR-370i2[1], the Port State of a virtual port is retrievable and settable on a CMS. The states represent the physical link connection of the port, the port's operational and administrative state, and state suppression exists when several states are valid simultaneously.

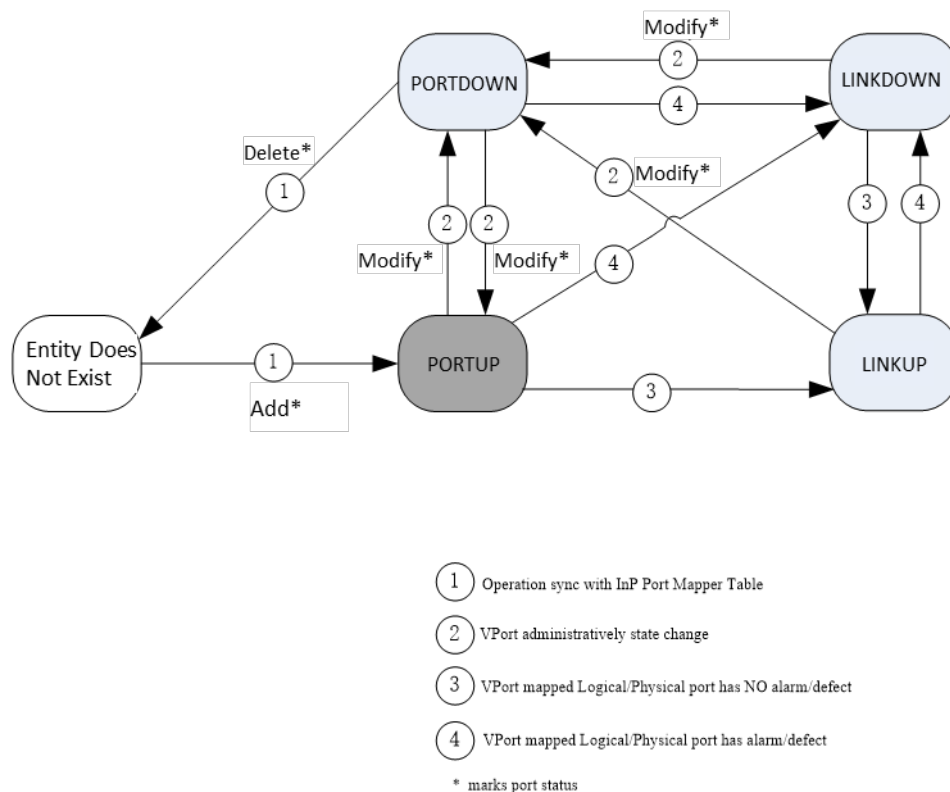


Figure 8 – Virtual Port State Machine

Figure 8 demonstrates the virtual port state machine and associated status.

Alarms on the Logical/Physical port are raised on a given physical AN when problems are detected at different network layers. They can be used to correlate the state of the virtual port for a virtual AN. The alarms that can be raised include:

- ITU-T Rec. G.988 [20] fault management alarms for ONU management.
- On a specific physical AN, the failure conditions incorporated for Physical Port are as follows:
 - Ethernet Physical Layer:
 - LAN-LOS of Physical port (e.g., ONU UNI)
 - GPON TC layer:
 - LOS, LOF, SF, SD of ONU ANI

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks. The VNO MS supports IEEE 802.1ag [21] Connectivity Fault Management (CFM) and IEEE 802.3ah [22] Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback.

The IEEE 802.3ah [22] standards enable link monitoring and remote fault detection on a specific physical AN, the failure conditions incorporated for Physical Port are as follows:

- Data Link Layer:
- The error events defined for Link Monitoring: Errored Frame Event, Errored Frame Period, Errored Frame Seconds Summary Event;
- The remote failure indication: Link Fault, Dying Gasp, Critical link events.

The ITU-T Rec. G.8013/Y.1731[23] and IEEE 802.1ag [22] standards enable end-to-end service OAM functions to one or more VNO networks. On a specific physical AN, the failure conditions incorporated for specific Physical Port are as follows:

- Data Link Layer:
- ETH-AIS, Eth-RDI

The alarms and operation actions of a virtual port will be reflected at Virtual Access Node, CMS and VNO MS.

- On a specific virtual AN, the failure conditions incorporated for a Virtual Port are:
- LINKDOWN, PORTDOWN
- Operator actions: ADD, DELETE, MODIFY

The VNO MS exchanges alarm information with physical AN through Minf Interface. The Minf interface supports retrieving FCAPS data from the physical AN. The CMS has a global view of the underlay resources, link connections etc, and can retrieve alarms on both physical and virtual ANs. The Centralized Management System and Virtual Access Node have knowledge of the alarms raised on both physical AN and virtual ANs; so alarms, notifications and events can also be logged on the CMS for future analysis.

At the time of publication of this document, YANG modules for PON management were being developed by the Broadband Forum. RFC8632 from IETF applies for functionalities about alarm management. Alarms should propagate into both InP and VNO management systems as appropriate.

As shown in Figure 9 below, the alarm definition for virtual port correlation follows the xPON YANG model defined in TR-385 [1].

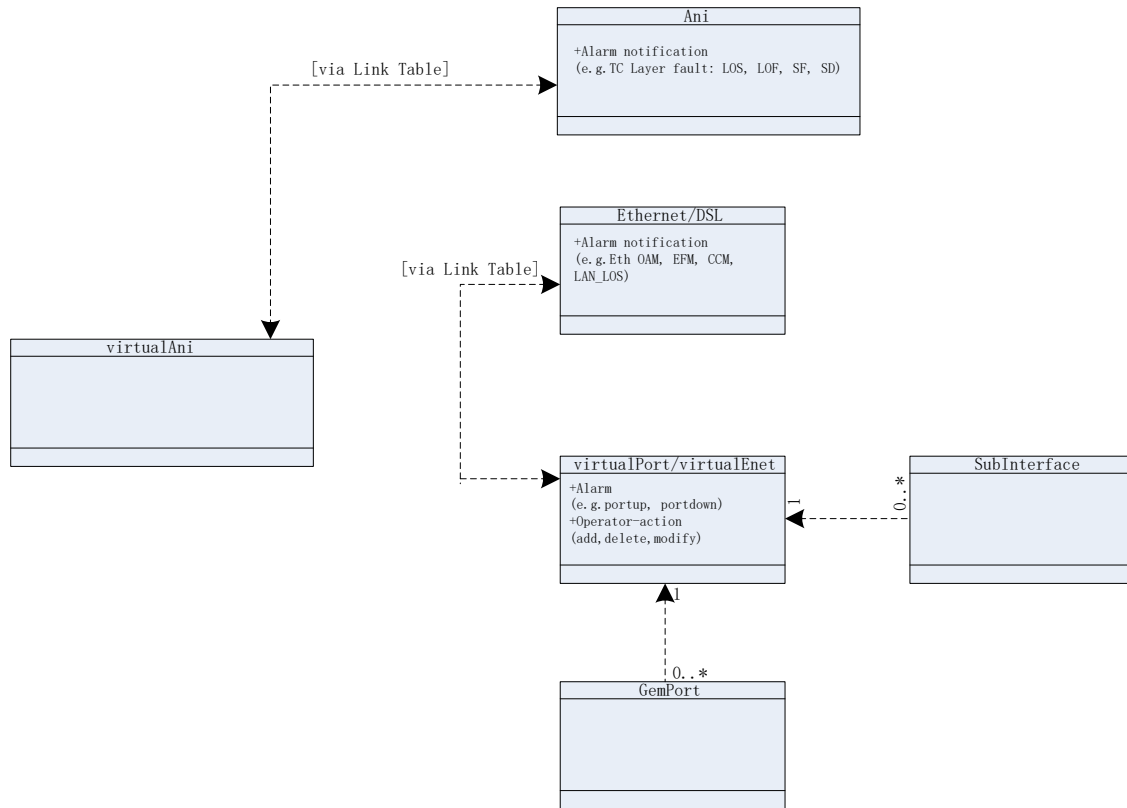


Figure 9 – Virtual Port Alarm propagation in the xPON YANG Model

6 FANS NETCONF/YANG interface definition

6.1 Basic principles

As described in TR-370i2, the principles of NETCONF/YANG can be adopted to achieve FANS in combination with the concept of a “Device Share”. This section describes the new YANG module required to achieve FANS, and how to apply it for multiple VNOs. The descriptions in this section can be applied to a variety of YANG modules and interfaces.

To allow different parties to manage a part of the network, it is necessary to model the different “network partition” that they will use. For this purpose, a new YANG module has been defined by the Broadband Forum, called the Infrastructure Provider YANG module. This module allows the definition of the set of VNOs that will access the Access Node and defines resource segmentation between the different VNOs. Each network partition consists of a list of objects with the following characteristics:

- The name allocated to this VNO
- The VNO credentials, i.e., identification of the VNO when opening a NETCONF session to the device. NETCONF session and user info is defined in `ietf-netconf-monitoring.yang` in RFC6022[11]
- A traffic tag specific to this VNO for segregating the traffic of a specific VNO
- The bandwidth allocated to the operator on this device

The Infrastructure Provider is responsible for creating a network partition for each VNO in the network, using the Nf-Vi interface. The name allocated to each VNO needs to be unique.

Once the VNO network partitions are created, each VNO will need to manage their own using the set of interfaces and resources which are exposed to them (see Section 0). Both configuration and operational data (e.g., performance counters) will be managed by each VNO separately.

Each VNO needs to use NETCONF/YANG to perform configuration actions within the bounds of their virtual access network. Security, mediation and privacy can be ensured using the approaches defined in TR-370i2.

It is necessary to support a query function via Os-Ma-nfvo to obtain the detailed information of network resource shared by authorized VNOs. The Infrastructure Provider can use this function to check whether there is enough resource while creating a new Virtual Network, as well as avoid potential conflicts. This function is also useful for global administrative operations, such as diagnostics, performance monitoring, and fault management etc. It should be noted that this query function does not conflict with the concept of isolation between different VNOs, because only the administrator (e.g., the InP) has access to this function.

There are however some concerns with scalability of NACM whose original purpose is to provide control access of multiple users to the same Data Store of resources.

The restrictions imposed by these base YANG modules also apply to the VNOs. For example, when a module allows defining several profiles, these are usually stored in a list where the name of the profile must be unique. If VNOs were able to define their own profiles, they might use a name

already in use. Consequently, some mechanism is required to ensure uniqueness of a name in a list. This is not explicitly modeled in the YANG modules, but needs to be done through either the physical device or through the Infrastructure Provider. This should be further studied. Potential options could go towards enhancements of NACM.

6.2 Achieving VNO access control

Using the set of YANG modules referenced in this document, the next step is to control how different VNOs can perform configuration actions and access state information to those objects that are under its control. Likewise, there is a need to ensure that a VNO is unable to change the configuration data or retrieve state data that is associated with another VNO.

An option that was initially considered consisted of a solution at the protocol level; IETF defines Network Configuration Access Control Model in RFC 8341[13]. With this model, rules can be defined that allow or deny access to a specific data node. So, in principle this model could be used to ensure different VNOs won't be able to interfere with each other. This could be achieved by adding a rule for every data node that is "owned" by a specific VNO to allow access or not.

There are however concerns with this method. Specifically, the NACM data tree would need to be configured by the InP separately for each VNO, which has scaling difficulties.

This document therefore provides a different approach of resource sharing and control. Specifically, this document assumes that standard YANG modules (ietf-interface, bbf-l2-fwd...) are maintained and that VNO segregation is generally achieved through means that do not require YANG module changes. As defined in TR-370i2, this can either be ensured through the physical device or through the Infrastructure Provider and Centralised Management System.

Annex A: FANS YANG Modules

This section describes the YANG modules to be used in the context of FANS deployment for the purposes of this Technical Report.

Dependencies on related YANG modules and standards

The YANG modules in this Technical Report are based on YANG 1.1 (RFC 7950) and are used for:

- Construct FANS instance from VNO perspective
- Construct FANS instance in SDN-based model via SDN M&C and BAA. The sharing over the following entities are supported:
 - Resource sharing based on ports
 - Resource sharing based on VLAN

This Technical Report uses the YANG modules defined in the following table.

The YANG modules related to the Minf Interface are included in the following Table 2.

Table 2 – FANS YANG Modules

Function	YANG Module(s)	Source	Integrations/Gaps
FANS	bbf-yang-types bbf-dot1q-types	TR-383	Imported by bbf-fans-vno.yang
	bbf-yang-types bbf-dot1q-types	TR-383	Imported by bbf-fans-resource-sharing & bbf-resource-sharing-descriptor

End of Broadband Forum Technical Report TR-386