TECHNICAL REPORT

TR-386

Fixed Access Network Sharing - Access Network Sharing Interfaces

Issue: 1
Issue Date: January 2019

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 copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be 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 IS EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT.

Revision History

Issue Number	Issue Date	Publication Date	Issue Editor	Changes
1	16 January 2019	16 January 2019	Peter Silverman, ASSIA Bruno Cornaglia, Vodafone	Original

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

Editor	Peter Silverman	ASSIA
	Bruno Cornaglia	Vodafone
Work Area Director(s)	George Dobrowski	Huawei
	Christopher Croot	BT
Project Stream Leader	Bruno Cornaglia	Vodafone

Table of Contents

List of Figures

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-370 “FANS – Architecture and Nodal Requirements”. An overview of the interfaces required for TR-370 based systems is provided in section 4, while the interface definitions are provided in section 5. Section 6 provides an overview of how TR-370 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-370 "FANS – Architecture and Nodal Requirements" [1].

This WT 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-370 *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 be in RFC 2119 [10].

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-370	*Fixed Access Network Sharing – Architecture and Nodal Requirements*	BBF	2017
[2] TR-359	*A Framework for Virtualization*	BBF	2016
[3] TR-355i1	*YANG Modules for FTTdp Management*	BBF	2016
[4] TR-349	*DSL Data Sharing*	BBF	2016

[5]	TR-298	*Management model for DSL line test*	BBF	2013
[6]	TR-252i3	*xDSL Protocol-Independent Management Model*	BBF	2013
[7]	TR-383	*Common YANG Modules*	BBF	2017
[8]	TR-371	*G.fast Vector of Profiles (VoP) Managed Object Structure*	BBF	2016
[9]	TR-413	*SDN Management and Control Interfaces for CloudCO Network Functions*	BBF	2018
[10]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	Mar. 1997
[11]	RFC 6020	*YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF),*	IETF	Oct. 2010
[12]	RFC 6022	*YANG Module for NETCONF Monitoring*	IETF	Oct. 2010
[13]	RFC 6241	*Network Configuration Protocol (NETCONF*	IETF	Jun. 2011
[14]	RFC 6536	*Network Configuration Protocol (NETCONF) Access Control Mode*	IETF	Mar. 2012
[15]	RFC 699	*Common YANG Data Types*	IETF	Jul. 2013
[16]	RFC 7223	*A YANG Data Model for Interface Management*	IETF	May 2014
[17]	RFC 7224	*IANA Interface Type YANG Module*	IETF	May 2014
[18]	RFC 7317	*A YANG Data Model for System Management*	IETF	Aug. 2014
[19]	RFC 7950	*The YANG 1.1 Data Modeling Language*	IETF	Aug. 2016
[20]	G.988	*ONU management and control interface (OMCI) specification*	ITU-T	Oct 2012
[21]	802.1ag	*IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area NetworksAmendment 5:Connectivity Fault Management*	IEEE	2007
[22]	802.1ah	*IEEE Standard for Local and metropolitan area networks -- Virtual Bridged Local Area Networks Amendment 7: Provider Backbone Bridges*	IEEE	2008

[23]	G.8013/Y.1731	*Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*	ITU	August 2015
[24]	BBF Published YANG	https://github.com/BroadbandForum/yang	BBF	2017
[25]	draft-ietf-netmod-entity-00	*A YANG Data Model for Entity Management*	IETF	2016

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:

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.

The Virtual Access Node representation of the physical Access Node is exposed to VNOs for resource consumption.

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 an separate business entity within the InP.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AN	Access Node
BBF	Broadband Forum
CFM	Connectivity Fault Management
COTS	Commercial-Off-The-Shelf
FANS	Fixed Access Network Sharing
FCAPS	Fault, Configuration, Accounting, Performance, Security
GPON	Gigabit Passive Optical Network
IETF	Internet Engineering Task Force
InP	Infrastructure Provider
LOF	Loss of Frame
LOS	Loss of Signal
MS	Management System
NETCONF	Network Configuration Protocol
NFV	Network Function Virtualization
O-VLAN	Operator VLAN (Operator Virtual Local Area Network)
OAM	Operations, Adminstration, and Maintenance
ONU	Optical Network Unit
pAN	Physical Access Node
PNF	Physical Network Functions
QOS	Quality of Service
RTT	Round Trip Time
SDN	Software Defined Network
SLA	Service Level Agreement
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

WT-386 builds upon the architecture principles defined in TR-370, 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

WT-386 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.

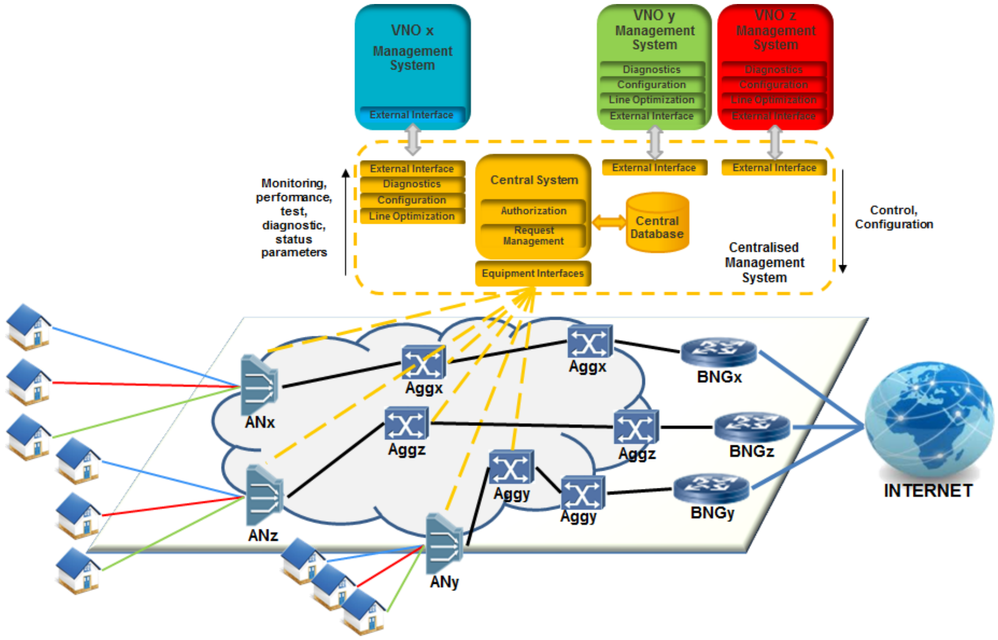
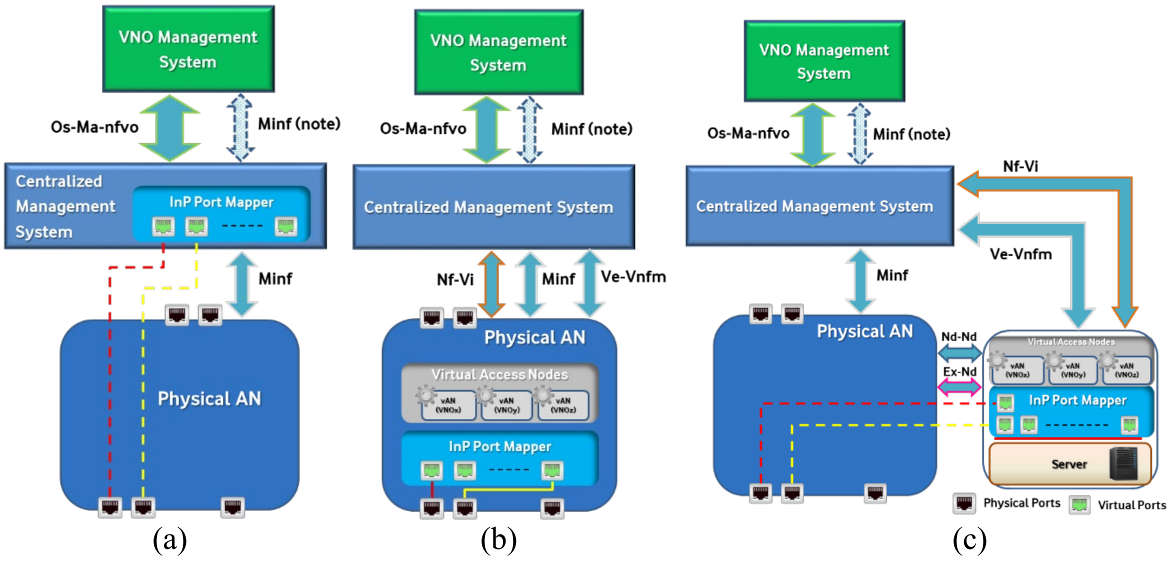


Figure 1 – Management System Overview [1]



(a) (b) (c)

Figure 2 – FANS Models [1]:
(a) Centralized Management System based FANS
(b) vAN based FANS (vANs in physical OLT)
(c) vAN based FANS (vANs in NFVI server)
Note: Avatar 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-370 [1] document, two models for network sharing can be deployed:

- Management System based (Figure 1 and 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)

Both models include a system capable of managing equipment from multiple vendors, and also maintaining backward compatibility. The main difference between them is that the first manages existing (legacy) and/or new network equipment via the InP's management system, while the latter exploits the capabilities of a virtualized access node.

It is important to note that the solution based on the Management System (MS) performs the network sharing at the management system level, not directly in the equipment itself.
Sections 4.1 and 4.2 describe the Centralised and VNO management systems for both solutions while the subsequent sections apply only to the Virtual Access Node model.

TR-349 [4] 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.

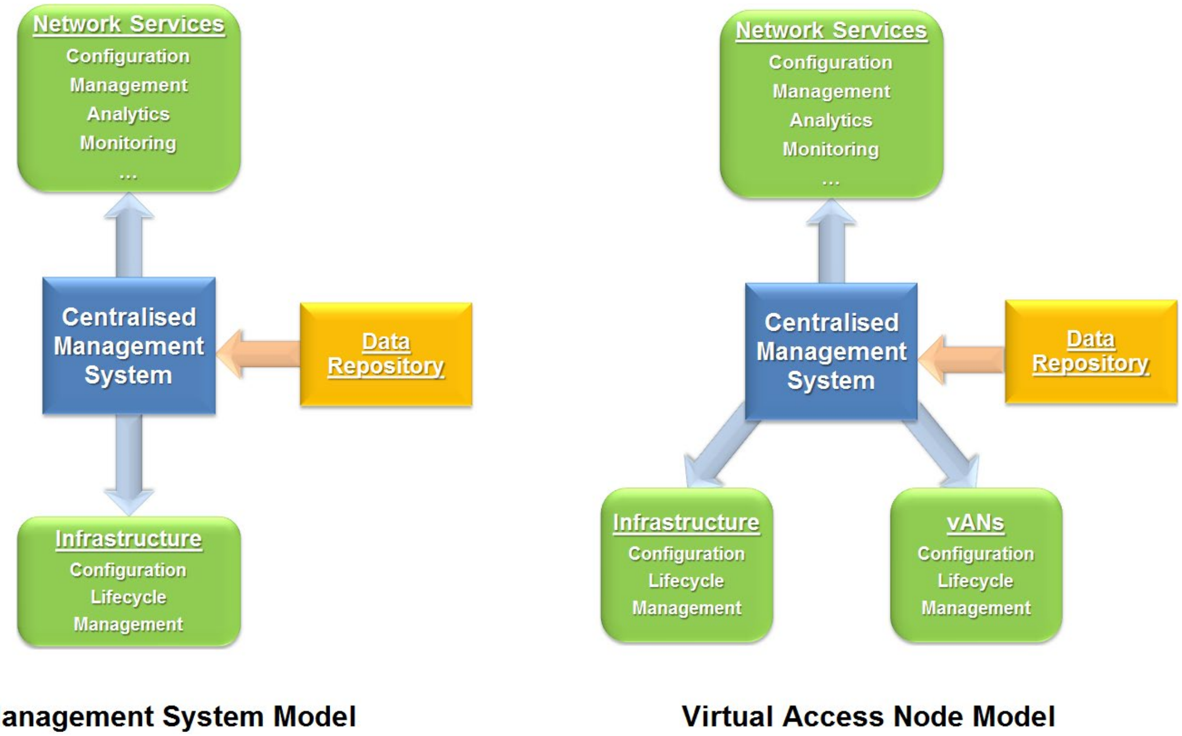
TR-349 references the DSL management parameters in TR-252i3 [6], the DSL line test management parameters in TR-298 [5] and the G.fast management parameters in TR-371 [8]. The YANG modules defining all these parameters are in TR-355 [3].

4.1 Centralized Management System

The Centralised Management System (CMS) (as defined in Sections 5 and 6.3 of TR-370 [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 centralized 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 Centralized Management system in order to enforce policies and avoid potential conflicts or discrepancies in resource sharing or line settings among VNOs.



Management System Model **Virtual Access Node Model**

Figure 3 – Centralised Management System

In the Virtual Access Node model, the Centralized 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 Centralized 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 Centralized 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

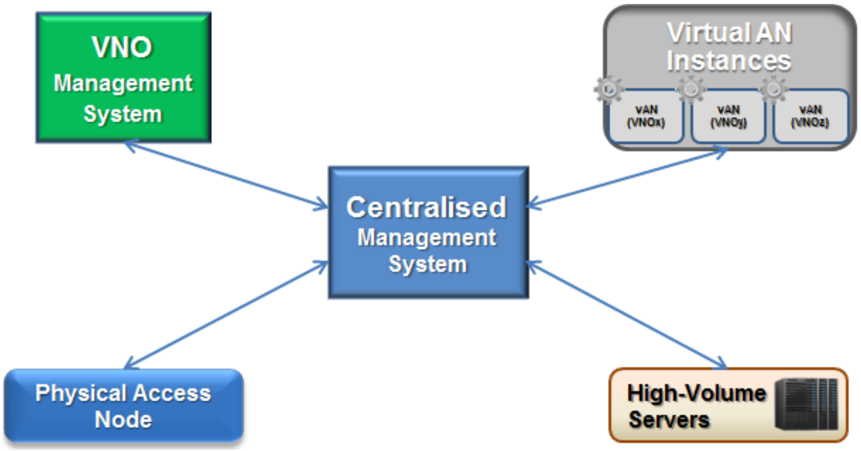


Figure 4 – Centralised Management System connections

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 and avatar version of the Minf reference point exposed by the Centralized Management System, as defined in Section 6.2 of TR-370 [1] and TR-413 [9]).

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 Centralized Management System, while the VNO Management System uses standard interfaces to communicate with Centralised 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.

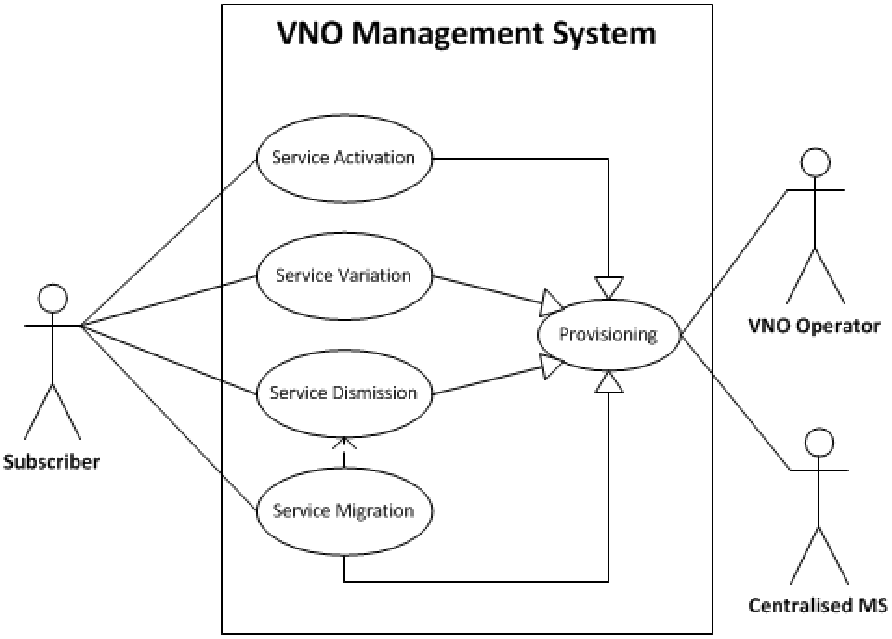


Figure 5 – VNO Management System: High-Level Vision

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

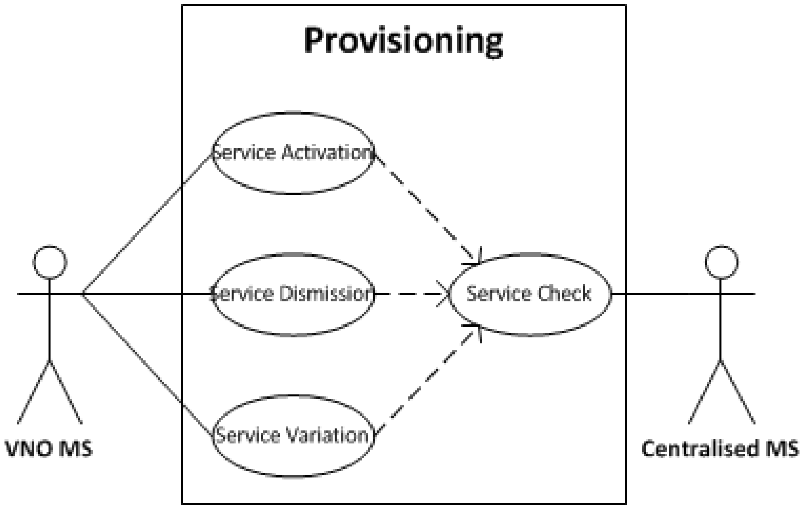


Figure 6 – Provisioning: High-Level Vision

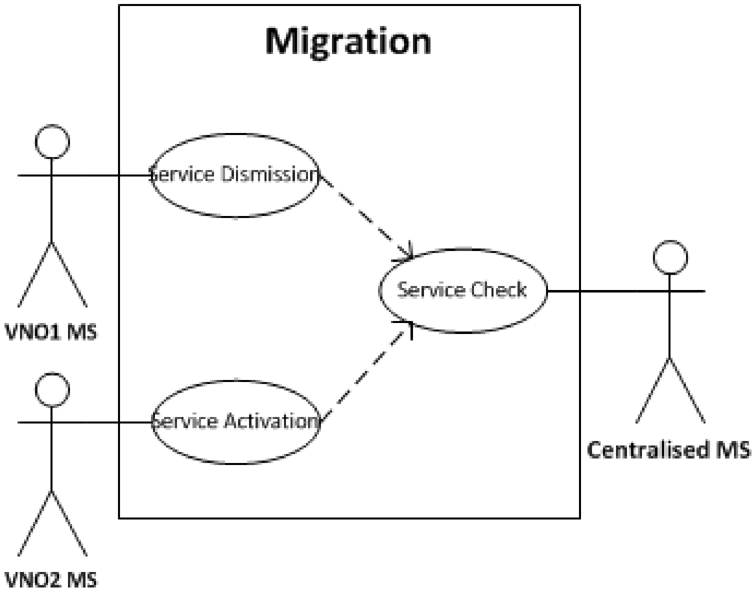


Figure 7 – Migration: High-Level Vision

4.3 Virtual Access Node

A virtual Access Node (vAN) (section 5.2.1 of TR-370 [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-370 [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-370 [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). This is done using the Operator VLAN (O-VLAN) Tag and well-known forwarding rules. O-VLAN tag information is agreed between the VNO and InP and is added to the Ethernet frame at the interconnection point. The Virtual Switch can intelligently forward customer data by inspecting packets before passing them on, ensuring traffic isolation. O-VLAN is a third VLAN tag added to identify the operator. Details of the O-VLAN are described in TR-370 [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. These resources are all managed by the virtualization layer.

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.

The following sections provide a list of functional modules for the Os-Ma-nfvo and Minf interfaces via YANG [11] modelling and NETCONF [13].

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 configuration models.
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 modelling 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

As depicted in Figure 2, the Os-Ma-nfvo interface is the true FANS API as it enables the exchange of requests and data between each VNO Management System and the Centralized Management System 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 Centralized Management System), 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 Centralized Management System:

- Assignment of VNO characteristics:
  - O-VLAN identifier for the Q-in-Q-in-Q schema (as defined in TR-370 [1])
  - Access Node/Access Ports
  - Bandwidth quota
- Backup/Restore of the vAN
- Equipment Inventory
- Common NMS/EMS related procedures that cannot be managed via the Minf interface (via ETSI standard interfaces in the CMS and NETCONF):
  - 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 interface is based on the following modules, already specified in BBF and IETF documents ([7],[18]):

- **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.

Other functionalities are candidated for being modelled in FANS:

- **bbf-fans-vno**: YANG definitions for configuration and identification of the Virtual Network Operator; it defines the network partition as a list of objects with the following characteristics:
  - Operator VLAN (O-VLAN) identifier (Note: O-VLAN can be configured by using a new YANG module or by expanding the current one)
  - Name (Identifier) of the VNO accessing the access node
  - Bandwidth Quota allocated to the VNO
  - Name (Identifier) of the Access Node
  - Access Ports

[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 Centralized 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**Error! Reference source not found.**, the VNO Management Systems access to the network resources via the mediation, through the FANS API (Os-Ma-Nfvo), of the Centralized Management System that verifies and reconciles the requests from all the VNOs.

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 Centralized 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 SHALL be specified according with TR-413 [9].

Note: TR-413 [9] 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-370 [1].

The generic BBF modules for frame classification, sub-interface, and sub-interface tagging, reported in TR-413 [9], should be extended to handle the triple VLAN tagging schema, as per BBF TR-370 [1] . The new modules can be derived from the above modules and named as follows:

- **bbf-fans-frame-classification**
- **bbf-fans-sub-interfaces**
- **bbf-fans-sub-interface-tagging**

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 Centralized 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-370[1][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.

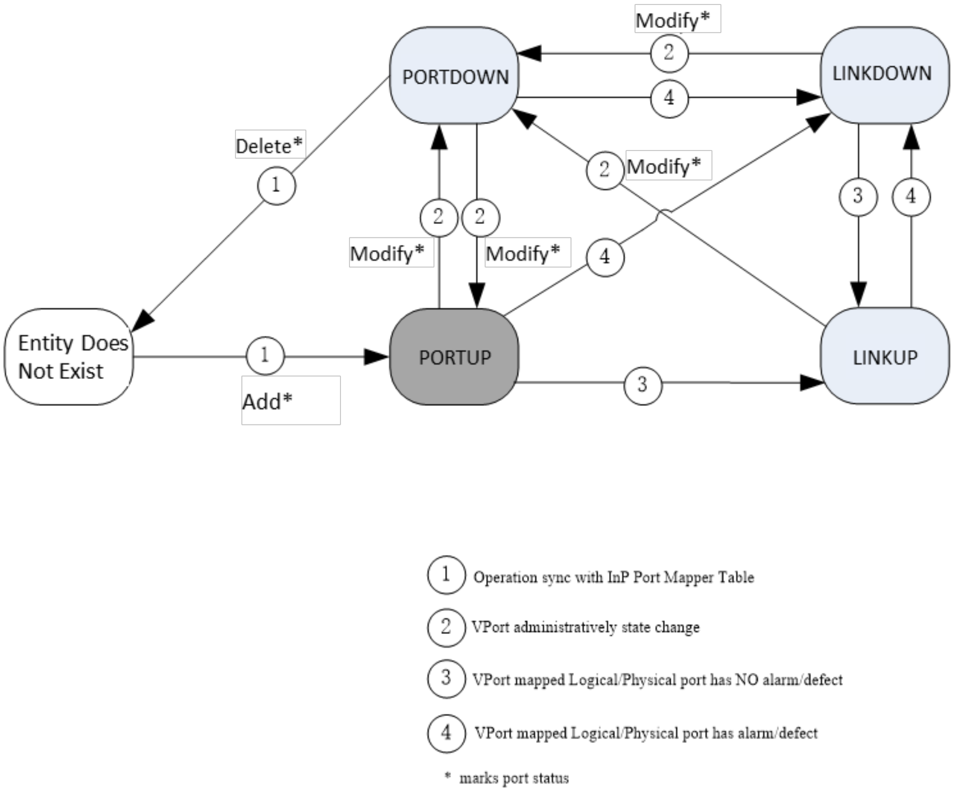

Modify*
2
PORTDOWN
LINKDOWN
4
Delete*
1
2
Modify*
3
4
2
2
Modify*
Modify*
4
Entity Does Not Exist
1
PORTUP
LINKUP
Add*
3
1 Operation sync with InP Port Mapper Table
2 VPort administratively state change
3 VPort mapped Logical/Physical port has NO alarm/defect
4 VPort mapped Logical/Physical port has alarm/defect
* marks port status

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][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; soso 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 and YANG modules for alarm management were being developed by IETF CCAMP. 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 PON YANG model defined in TR-385 [1], and bbf-alarm-management defined in TR-383 [7].

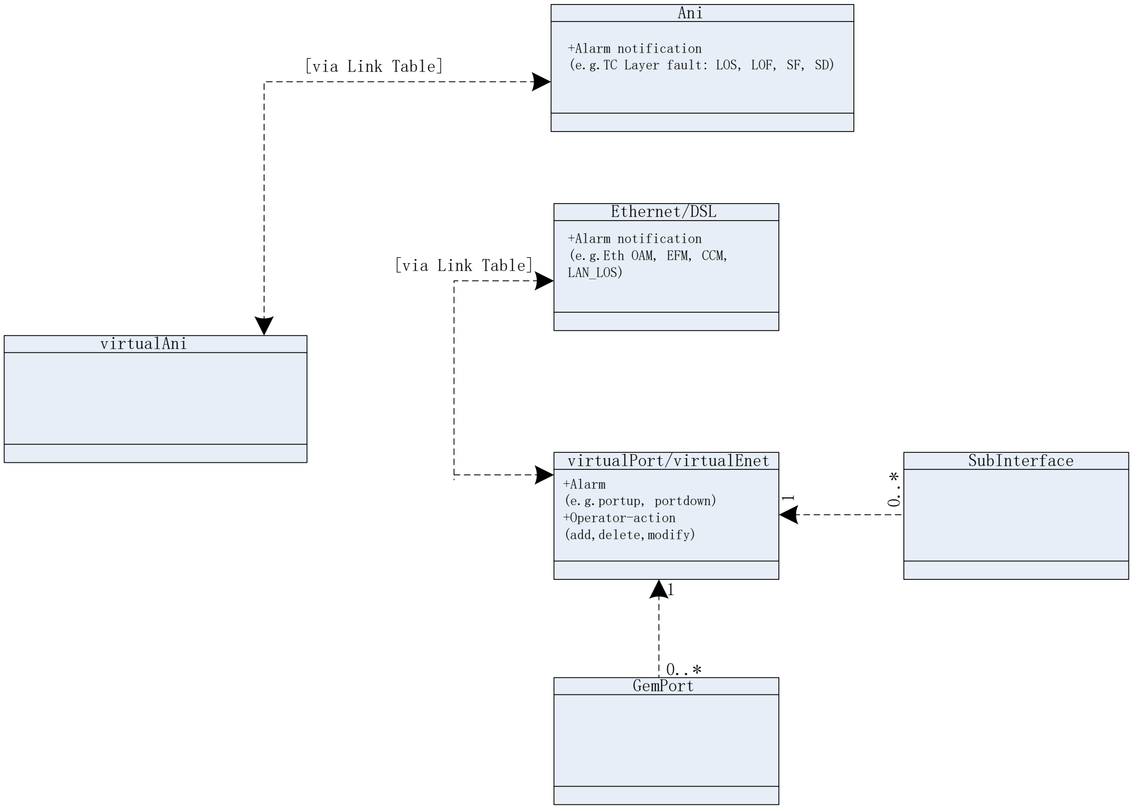


Figure 9 – Virtual Port Alarm propagation in the xPON YANG Model

6 FANS NETCONF/YANG interface definition

6.1 Basic principles

As described in TR-370, the principles of NETCONF/YANG can be adopted to achieve FANS in combination with the concept of a “Virtual Access Node”. 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
- 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 5). 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-370.

It is necessary to support a query function via Os-Ma-nfvo to obtain the detailed information of network resource shared by all existing 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; NETCONF defines an Access Control Model "NACM", defined in IETF RFC 6536). 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-370, this can either be ensured through the physical device or through the Infrastructure Provider and Centralized Management System.

End of Broadband Forum Technical Report TR-386