



Question(s): 19/13

Geneva, 16-27 July 2018

CONTRIBUTION**Source:** Ministry of Communications (India), Orange Polska S.A.**Title:** Proposal on new work item- "Cloud Computing - End to End Fault & Performance Management Framework of Multi-Cloud Virtual Network Services"**Purpose:** Proposal

Contact: Lav Gupta
DOT
India
Tel: + 13148250063
Fax: + 919868217055
E-mail: lavgupta@wustl.edu

Contact: Mahabir Parshad
TEC DOT
India
Tel: +919868217055
Fax: +91 11 23329088
E-mail: srddg.tec@gov.in

Contact: Arvind Chawla
TEC DOT
India
Tel: +91 9868512165
Fax: +91 11 23714866
E-mail: arvind.chawla@gov.in

Contact: Sridhar Sapparapu
TEC DOT
India
Tel: +919013133805
E-mail: diri.tec@nic.in

Contact: Emil Kowalczyk
Orange Polska S.A.
Poland
Tel: +48 502 397 809
E-mail: emil.kowalczyk@orange.com

Contact: Janusz Pieczerak
Orange Polska S.A.
Poland
Tel: +48 502 709 314
E-mail: janusz.pieczerak@orange.com**Keywords:** Multi cloud; fault management; performance management; virtual network service**Abstract:** This contribution proposes to start new work item related to End to End Fault & Performance Management Framework of Multi Cloud Virtual Network Services. NWI describes the deployment of Virtual Network Services (VNS) over multiple clouds based on Network Function Virtualization (NFV) paradigm using NFVIaaS and/or VNFaaS to provide VNSs. It proposes to establish a framework for end-to-end management of fault and performance issues, including detection and localization, in multi-cloud based virtual network services as a means to achieve carrier grade reliability and availability. The approach is generic in nature and is applicable to all member states.

Recommendation ITU-T <No.>

Cloud Computing - End to End Fault & Performance Management Framework of Multi Cloud Virtual Network Services

Summary

This recommendation describes the deployment of Virtual Network Services (VNS) over multiple clouds based on Network Function Virtualization (NFV) paradigm using NFVIaaS and/or VNFaaS to provide VNSs. It proposes to discuss establishment of a framework for end-to-end management of fault and performance issues, including detection and localization, in multi-cloud based virtual network services as a means to achieve carrier grade reliability and availability. The approach is generic in nature and is applicable to all member states.

Keywords: Multi-cloud, Multi-cloud Management Platform, Virtual Network Service, VNS, Virtual Network Functions, VNF, Service Function Chain, SFC, End-to-end Management, Fault, Performance, Availability, Reliability, Network Function Virtualization, NFV, Management and Orchestration, OSS

Introduction

Cloud computing is an essential ingredient of all modern telecommunications services, including 5G. A use case that service providers are globally interested in, is deployment of their service offerings as Virtual Network Services (VNS), using Network Function Virtualization (NFV), over multiple clouds. This gives them a number of advantages including freedom from proprietary solutions, reduced time to market, agility of service, proximity to customers and lower cost of deployment and operation. However, today the virtual deployments do not match the five nines (99.999%) availability, or the performance of the traditional physical networks based on dedicated and custom-built integrated hardware and software. A standards based Fault, Configuration, Accounting, Performance and Security (FCAPS) framework for VNS over multiple clouds would help attain the level of availability and performance that service providers and subscribers expect from the traditional networks. This recommendation focuses mainly on the Fault and Performance (FP) aspects of virtual network service deployments. For these aspects alone, ensuring proper operation of the VNS is more complex, as compared to traditional services, because of two main reasons: a) more layers of abstraction i.e. physical, virtual resources, virtual network functions, service function chains and virtual network services, and b) complex interaction of the involved management platforms, i.e., multi-cloud management platform (MCMP) of the cloud service provider, Operation Support Systems (OSS) of the service provider and Management and Orchestration platform (MANO) of NFV. These platforms together have the responsibility of managing the multi-cloud resources and the life cycles of virtual network services and their components. For this, the FP management functionality must collect and process all the alarms, notifications and performance metrics from different layers, e.g., VNS, SFC, VNF and EMS (**Note: somewhere in the description we may refer to criticality of the alarms as defined ITU X.733 Recommendations**). Four Critical aspects of end-to-end fault & performance management system are:

- i) Fault and Performance issues detection sub-system: carries out detection of fault & performance issues, both impending and manifest faults.. This is done in two steps: Step 1 involves classification of a situation as ‘fault’ or ‘no-fault’ and Step 2 involves further classification of fault problems as ‘manifest’ or ‘impending.
- ii) Fault and performance localization sub-system: carries out localization of manifest faults in two steps: coarse-grain and fine-grain localization. For impending faults it predicts the intensity and likely location of the problem.
- iii) Performance Management: Fix the fault that degrades network performance i.e. troubleshoot fault to restore network performance to original or improved condition;

- iv) Maintaining QoS (Quality of Service): Adhere to SLA (Service Level Agreement) for achieving 99.999% availability of network & business critical applications. (Availability requirement of service provider is five nines. Subscribers may have their own SLAs)

1 Scope

This document provides a framework and general requirements for

- NFVIaaS,
- VNFaaS,
- Virtual Network Services (VNS) in multi TSP domains / multi CSP Clouds
- End-to-End Fault and Performance Management of Multi Cloud Virtual Network Services.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.yyy] Recommendation ITU-T X.yyy (date), *Title*.

Sl. No.	Document No.	Title/Document Name
1 [ITU-T X.733]		Severity of Events & Alarms
2 [ITU-T Y.3500]	Recommendation ITU-T Y.3500 (2014) ISO/IEC 17788:2014,	Information technology – Cloud computing – Overview and vocabulary.
3 [ITU-T Y.3501]	Recommendation ITU-T Y.3501 (2013),	Cloud computing framework and high-level requirements.
4 [ITU-T Y.3502]	Recommendation ITU-T Y.3502 (2014) ISO/IEC 17789:2014,	Information technology – Cloud computing – Reference architecture.
5 [ITU-T Y.3503]	Recommendation ITU-T Y.3503 (2014)	Requirements for Desktop As A Service
6 [ITU-T Y.3510]	Recommendation ITU-T Y.3510 (2016),	Cloud computing infrastructure requirements
7 [ITU-T Y.3512]	Recommendation ITU-T Y.3512 (2014),	Cloud computing - functional requirements of Network As A Service
8 [ITU-T Y.3513]	Recommendation ITU-T Y.3513 (2014),	Cloud computing - functional requirements of Infrastructure As A Service

OTHER REFERENCES:

- 1 ETSI GS NFV-INF 001 V1.1.1 Network Functions Virtualisation (NFV); Infrastructure overview
- 2 ETSI GS NFV 002 v1.1.1 Network Functions Virtualisation (NFV); Architectural Framework.
- 3 ETSI GS NFV 003 v1.1.1 Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV.
- 4 ETSI GS NFV 004 v1.1.1 Network Functions Virtualisation (NFV); Virtualisation Requirements
- 5 ETSI GS NFV 001v010101 Network Functions Virtualisation (NFV); Use Cases

6	ETSI GS NFV-MAN 001v010101	NFV: Management and Orchestration
7	ETSI GS NFV-PER 001 v1.1.1	NFV Performance & Portability best practices
8	ETSI GS NFV-INF 010 v1.1.1	NFV Service quality metrics
9	ETSI GS NFV-SWA 001 v1.1.1	NFV: VNF Architecture

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Cloud Service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface. It may comprise the hardware & hypervisor layers delivering individual servers, border routers, firewalls, load balancers & switches.

3.1.2 Cloud Service Customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.3 Cloud Service Provider [ITU-T Y.3502]: party which makes cloud services available.

3.1.4 Hypervisor [ITU-T Y.3510]: A type of system software that allows multiple operating systems to share a single hardware host.

3.1.5 Party [ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.6 Virtual Machine [b-DMTF OVF]: The complete environment that supports the execution of guest software.

3.1.7 Virtual Network Function (GS-NFV-003 V1.3.1):

3.1.8 Virtual Network Function Forwarding Graph (VNFFG) (GS-NFV-003 V1.3.1):

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Virtual Network Service: Virtual Network Service (VNS) can be described as an abstracted transport connectivity between two end points in a virtualised environment where the end points may be located in one or more clouds. A VNS utilises a Service Function Chain (SFC) or Virtual Network Function Forwarding Graph (VNFFG) for interconnecting virtual network resources end to end. An example of end-to-end Virtual Network Service is shown in fig. 5 & 6.

3.2.2 Service Function Chain:

3.2.3 Virtual container:

3.2.4 Docker: Docker is a type of virtual container.

3.2.5 Host Operating System:

3.2.6 Guest Operating System:

3.2.7 Cloud Service Types: cloud services are IaaS (bare metal, virtual compute, virtual storage and virtual links) PaaS (virtualized server with OS (s)), SaaS (IT services on the virtual infrastructure). These are accessible through the Internet.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CDN	Content Delivery Network
CPE	Customer Premises Equipment
DaaS	Desktop as a Service
DAS	Direct-Attached storage
DoT	Department of Telecommunications
EMS	Element Management System
FC	Fibre Channel
FCAPS	Fault, Configuration, Accounting, Performance and Security
IaaS	Infrastructure as a Service
IOT	Internet of Things
iSCSI	Internet Small Computer System Interface
IP	Internet Protocol
IPSEC	Internet Protocol Security
ITU-T	International Telecommunication Union – Telecom Standardization Sector
NaaS	Network as a Service
NFV	Network Function Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
OSS/BSS	Operations Support Systems/Business Support Systems
PaaS	Platform as a Service
P/PE router	Provider/Provider Edge router
PoP	Point of Presence
QoS	Quality of Service
SD-WAN	Software Defined Wide Area Network
SFC	Service Function Chain
SLA	Service Level Agreement
SSL	Secure Socket Layer
TEC	Telecommunication Engineering Centre
TSP	Telecom Service Provider
uCPE	Universal Customer Premises Equipment
vCPE	Virtual Customer Premises Equipment
VNF	Virtual Network Function
VNFaaS	VNF as a Service
VNPaaS	Virtual Network Platform as a Service
VNS	Virtual Network Service
VLAN	Virtual LAN

VM	Virtual Machine
VNFaaS	Virtual Network Function (VNF) as a Service
WAN	Wide Area Network

5 Conventions

In this Recommendation:

The keywords “**is required to**” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “**is prohibited from**” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “**is recommended**” indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords “**is not recommended**” indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords “**can optionally**” indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of management framework in multi-cloud environment

6.1 General

Network Function Virtualisation (NFV) enables faster deployment, simple configuration and ease of maintenance as compared with dedicated hardware based traditional network. The service provider can easily implement new innovative and customized services with NFV on customer demand. Various service models are included in the use cases of enterprise services, IOT services and mobile broadband. Examples of the high level use cases of NFV are IaaS, NaaS, VNFaaS, VNPaaS, Virtualisation of Mobile Core network and IMS, Virtualisation of mobile base station, Virtualisation of home environment, Virtualisation of CDNs, Virtualisation of P/PE routers, IOT, vCPE / uCPE, SD-WAN, WAN Optimization, Secure Internet Breakout, Secure Cloud Connect, Data Centre Interconnect. The high level NFV Framework containing three working domains, viz., VNFs, NFV Infrastructure and NFV Management & Orchestration (MANO) is as given below. Multi-cloud VNS deployments multiply the advantages of NFV.

6.1.1 Network functions virtualization management and orchestration architectural framework (NFV-MANO Architectural Framework) is the collection of all functional blocks, data repositories used by these blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFVI and VNFs. MANO consists of Virtual Infrastructure Manager, VNF manager and Orchestrator.

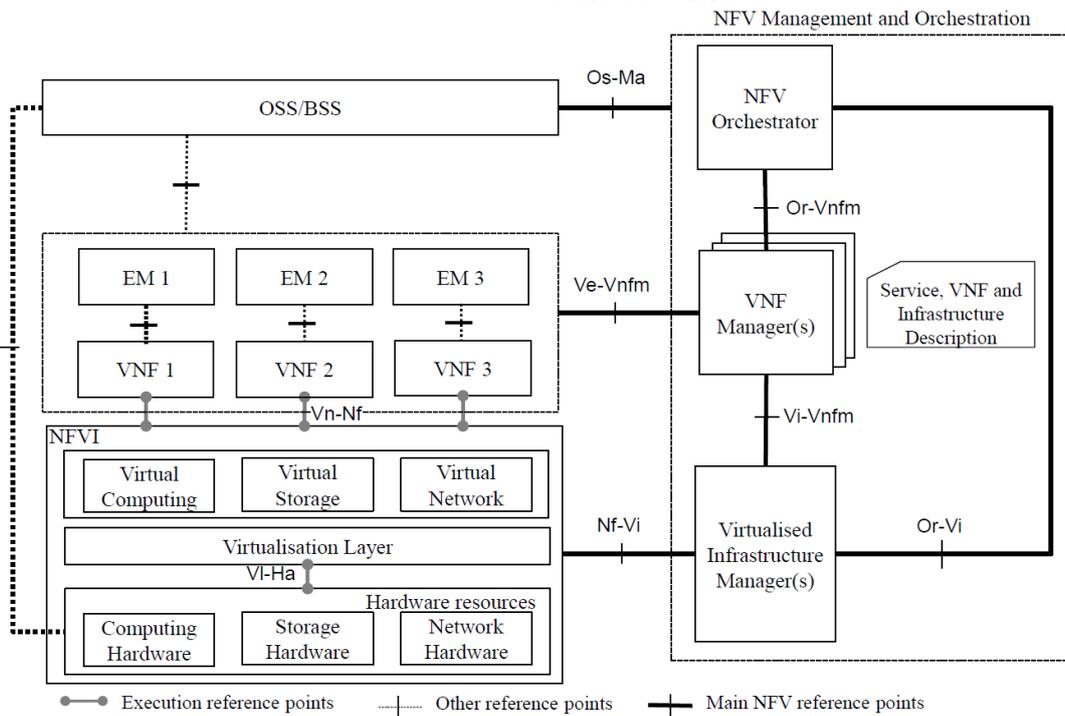


Figure-I NFV high level frame work

6.2 Network Function Virtualisation Infrastructure as a Service (NFVaaS)

6.2.1 Network Functions Virtualization Infrastructure (NFVI) is the foundation platform for Network Function Virtualisation (NFV) framework that contains the totality of hardware devices, operating system(s), hypervisors and other virtualization tools, virtual compute, virtual storage and virtual network elements that are used to instantiate virtual network functions. VIM is the resource management component of the NFVI. Network Function Virtualization (NFV) is a network architecture concept that uses the technologies of IT virtualization to virtualise entire classes of network node functions into building blocks that may connect, or chain together, to create communication services. The NFV framework may support either centralized or distributed architecture/environment depending on the use cases. The NFV infrastructure can span several locations. Network Functions Virtualization Infrastructure (NFVI) is the totality of all hardware and software components that build the environment where VNFs are deployed. The network providing connectivity within and between locations is considered as part of the NFV Infrastructure (NFVI).

6.2.2 The NFVI encompasses all hardware (compute, memory, storage), networking and software capabilities necessary to deliver a common platform that can support multiple use cases including network infrastructure workloads, such as mobile core and enterprise customer workloads such as firewalling or Wi-Fi control functions. NFVI capabilities must be agnostic to the underlying physical compute, storage and networking hardware requirements, types and vendor. The NFVI software must provide a consistent network virtualization and virtual hosting environment, which exposes a common northbound and southbound management layer that is independent of the underlying hardware or VNFs that are being supported.

6.2.3 NFVI can also be defined to contain Hypervisor domain, Compute domain and Network domain as shown below.

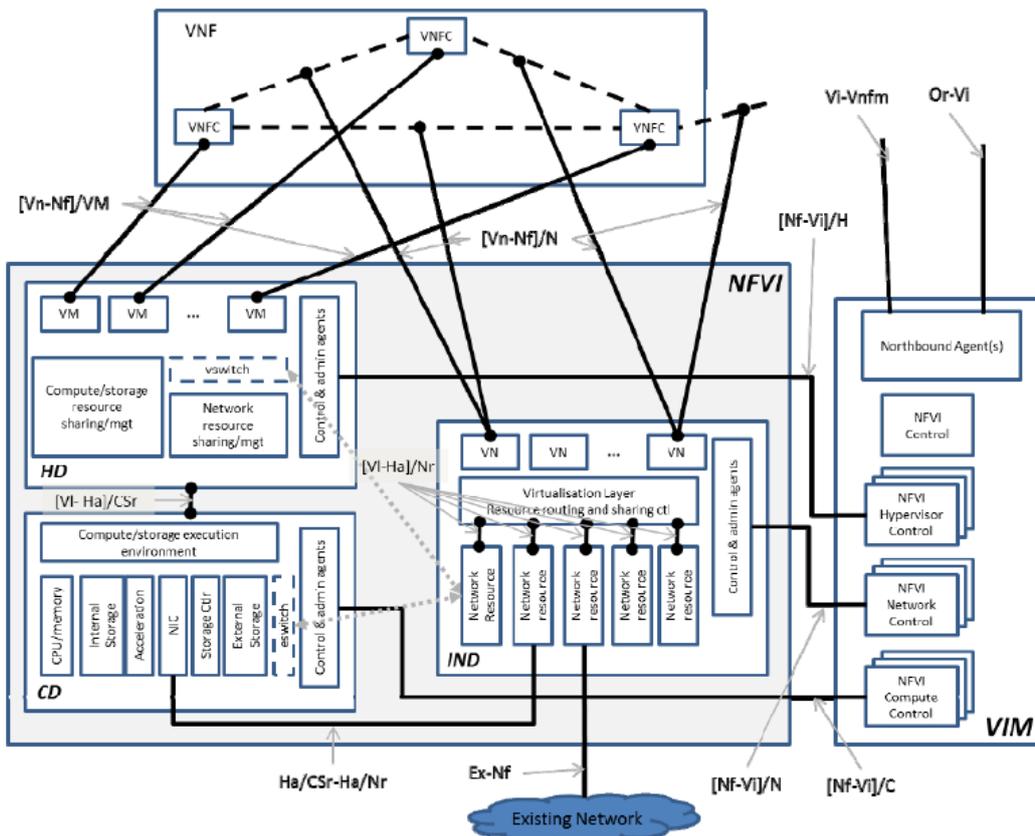


Figure-2 Domains of NFVI

6.2.4 The basic hardware consists of the general purpose commercially available off the shelf servers. The Hypervisor is directly installed on bare metal or on top of Host operating systems. The hypervisor must have a small footprint in the memory. It must support a shorter I/O path for maximum performance. The virtualization approach should support vertical and / or horizontal scaling depending upon the use cases for increasing capacity. The Hypervisor must allow prioritization of system resources e.g. CPU/Memory by defining the resource allocation to Virtual Machines (VMs). Hypervisor must support provisioning of the least possible CPU resources to the low critical virtual machines & reservation of CPU resources to high critical VMs. Non-Disruptive Virtual Machine migration must be supported. Virtualization software should have the ability to live migrate Virtual machines files from one storage array to another without any Virtual Machine downtime. It should also support the migration from one storage protocol to another (ex. FC, iSCSI, DAS etc) without any disruption.

6.2.5 Infrastructure domain provides the virtual resources that can be used to create virtual network functions in software. It may support creation and scaling of multiple types of Virtual Networking Functions (VNFs) decoupled from the underlying hardware. For instance, it may provide Logical Switching - Reproduce L2 and L3 switching functionality in a virtual environment, Logical Routing - Routing between logical switches, providing dynamic routing within different virtual networks. It may also host middle-box functionalities like Logical Firewall - Distributed firewall, kernel enabled line rate performance, virtualization and identity aware monitoring. It may provide Logical Load Balancer - Solution may provide a server load balancer with features like SSL offload. It may provide Logical VPN - The solution may provide L2VPN, SSLVPN, site-to-site IPSEC VPN services. The solution may support IPv6 native or Dual stack (IPV4/V6). It may support deployment of multiple instances of virtual networks independent of each other. The solution may offer to bridge VXLAN layer2 Networks and VLAN based networks

6.2.6 The Virtualised Infrastructure Manager (VIM) is responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator's Infrastructure

Domain (e.g. all resources within an NFVI-PoP, resources across multiple NFVI-POPs, or a subset of resources within an NFVI-PoP). A VIM may be specialized in handling a certain type of NFVI resource (e.g. compute-only, storage-only, networking-only), or may be capable of managing multiple types of NFVI resources (e.g. in NFVI-Nodes). The VIM controller function may be deployed in a centralized location (management data centre, central office, etc.) or distributed location in order to support multiple NFVI-Nodes representing a single cloud. VIM may support secure multi-tenancy. VIM may support carrier-grade availability. VIM may support policy based resource allocation, policy based workload placement, API based workload movement and tenant specific resource allocation policies. VIM orchestrates the allocation/upgrade/release/reclamation of NFVI resources (including the optimization of such resources usage), and manages the association of the virtualised resources to the physical compute, storage, networking resources. VIM along with NFV Orchestrator supports the management of VNF Forwarding Graphs (create, query, update, delete), e.g. by creating and maintaining Virtual Links, virtual networks, sub-nets, and ports, as well as the management of security group policies to ensure network/traffic access control. VIM may manage in a repository, the inventory related information of NFVI hardware resources (compute, storage, networking) and software resources (e.g. hypervisors), and manage the capabilities and features (e.g. related to usage optimization) of such resources. A service provider may obtain resources from more than one NFVI provider. Thus there may be more than one VIM in the picture. On the other hand, each VIM can manage more than one NFVI PoP.

6.2.7 The Virtual Network Function Manager (VNFM), which is part of MANO, is responsible for the lifecycle management of VNF instances eg: VNF Instantiation, VNF upgradation, Start and Stop VNFs, configure VNFs, VNF instance scaling out/in, monitor VNFs, VNF instance assisted or automated healing and VNF Termination. The VNF manager may have the capability to create and launch a new VNF based on specific template or VNF instantiation feasibility checking, if required. Each VNF instance is assumed to have an associated VNF Manager, A VNF manager may be assigned the management of a single VNF instance, or the management of multiple VNF instances of the same type or of different types. The VNF manager dynamically deploys a specific amount of compute/storage for a particular VNF based on a predefined template. The VNF manager solution may be fully multi-tenant and it may be shared across multiple customers.

6.2.8 The Network Orchestrator manages VNS deployment templates and VNF Packages (e.g. on-boarding new Network Services (NS) and VNF Packages). During on-boarding of VNS and VNF, a validation step may be done. To support subsequent instantiation of a VNF and a VNS respectively, the validation procedure needs to verify the integrity and authenticity of the provided deployment template, to ensure that all mandatory information is present and consistent. In addition, during the on-boarding of VNFs, software images provided in the VNF Package for the different VNF components are catalogued in one or more NFVI-PoPs, using the support of VIM. The orchestrator carries out network Service instantiation and Network Service instance lifecycle management, e.g. update, query, scaling, collecting performance measurement results, event collection and correlation, termination. Management of the instantiation of VNF Managers where applicable and management of the instantiation of VNFs, in coordination with 3rd party VNF Managers, is done by Orchestrator. The orchestrator validates & authorizes NFVI resource requests from VNF Managers, as those may impact Network Services (granting of the requested operation needs to be governed by policies).

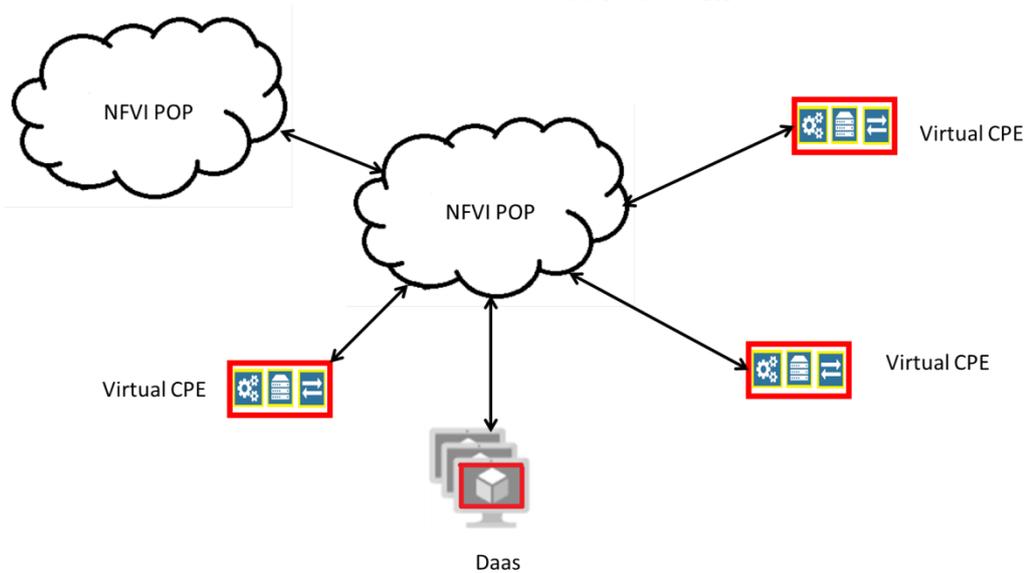


Figure-3 Use case with vCPE

6.3 VNF as a Service (VNFaaS):

6.3.1 Virtualized network functions (VNFs) are software implementations of network functions that can be deployed on Network Functions Virtualization Infrastructure (NFVI). The NFV solution may support service chaining of VNFs to create an end to end service. The solution may support real-time changes to deployed service chains.

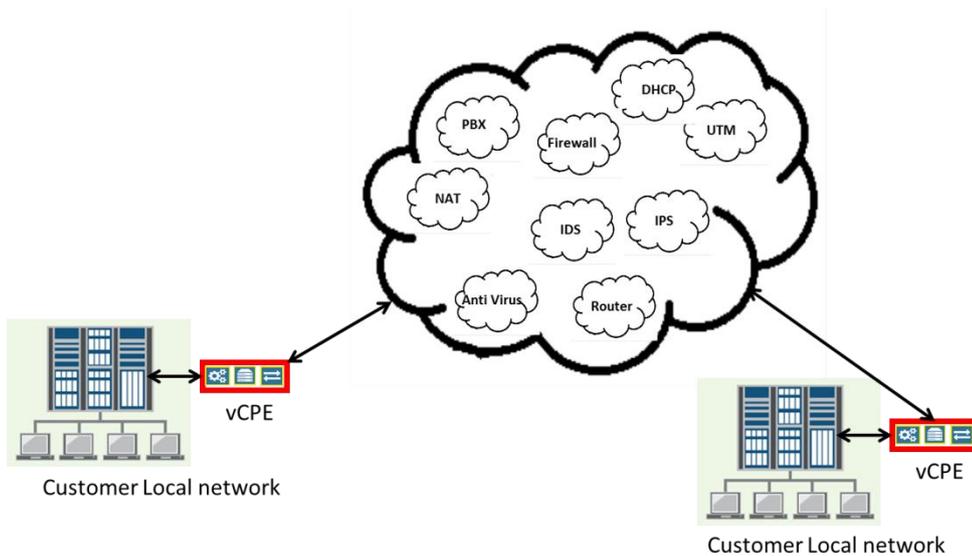


Figure-4 VNFaaS

VNFs are created in virtualized infrastructure as software applications and hosted on Virtual Machines (VMs) instantiated in NFVI PoPs of one or more clouds.

6.4 Virtual Network Services

6.4.1 Formation of VNS

A Virtual Network Service (VNS) can be formed between any two end points in one or more clouds. The abstracted transport connectivity between these two end points formed in a virtualised environment utilises a Service Function Chain (SFC) or Virtual Network Function Forwarding Graph (VNFFG), for interconnecting virtual network resources end to end.

6.4.2 VNS in a single cloud

A single cloud based on NFV frame work is depicted as below where only one NFVI node/PoP is shown in the figure-5.

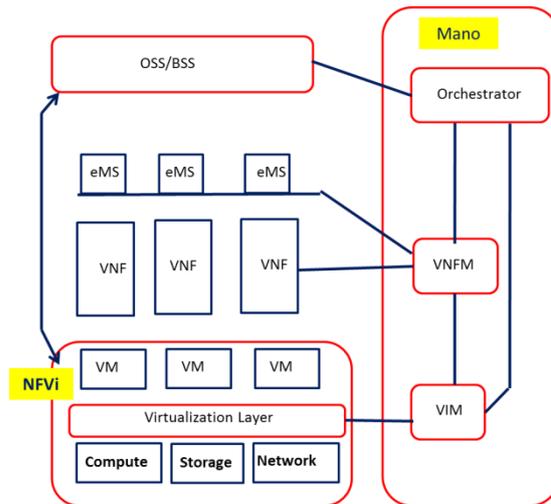


Figure-5 Single cloud with single NFVI-PoP

The figure-6 depicts the single cloud with multiple NFVI-PoPs. The multiple NFVI nodes/PoPs are controlled by the same VIM and OSS. The VNFs launched on all these NFVI nodes/PoPs are managed by the same VNFM.

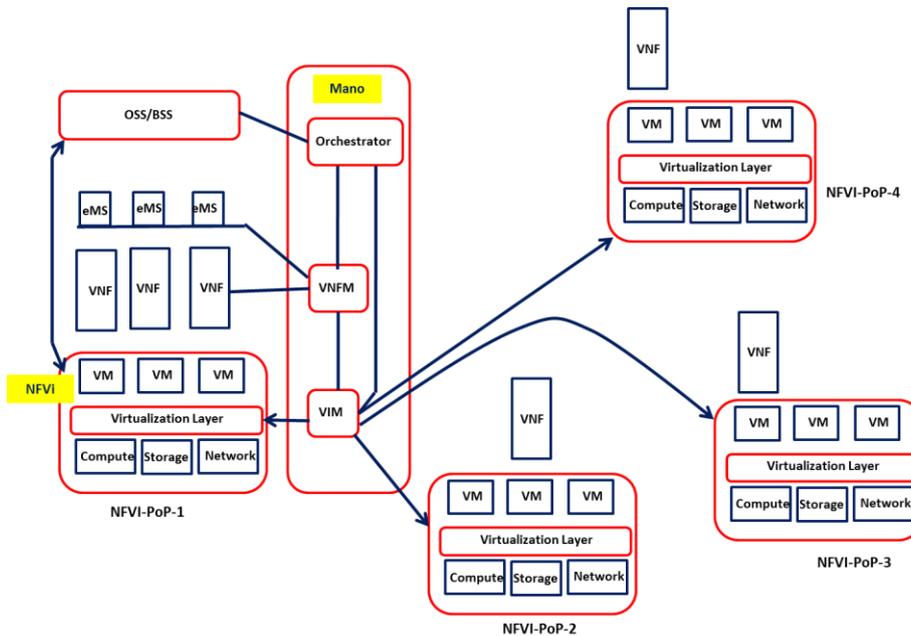


Figure-6 Single cloud with Multiple NFVI-PoPs

The following diagram (figure-7) depicts the virtual network service built between two virtual Customer Premises equipments (vCPEs) connected to the same as well as different NFVI-PoPs.

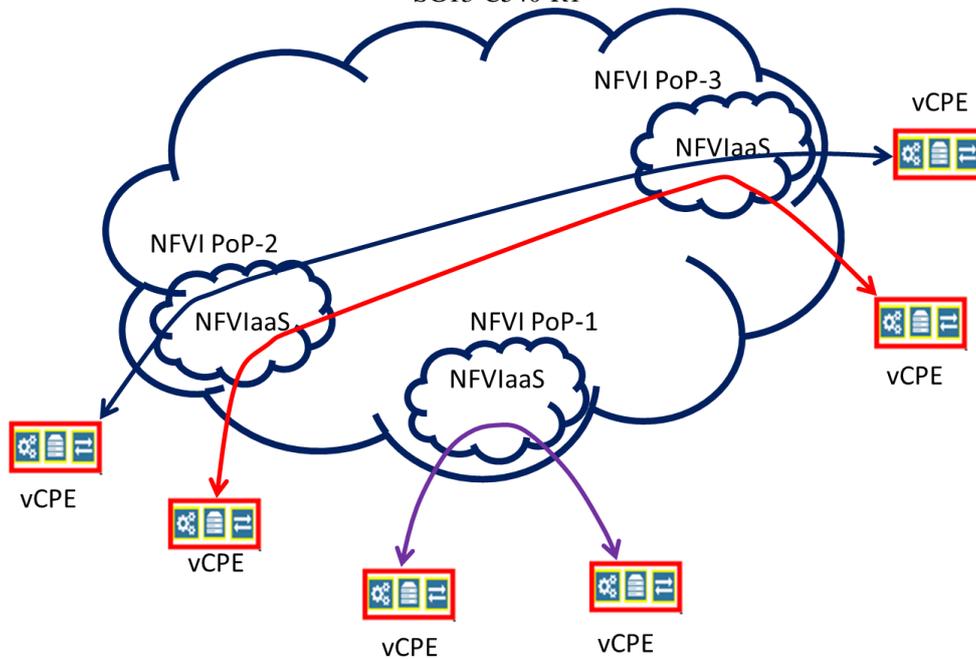


Figure-7 – Virtual network services in a single cloud

6.4.2 VNS in multi cloud

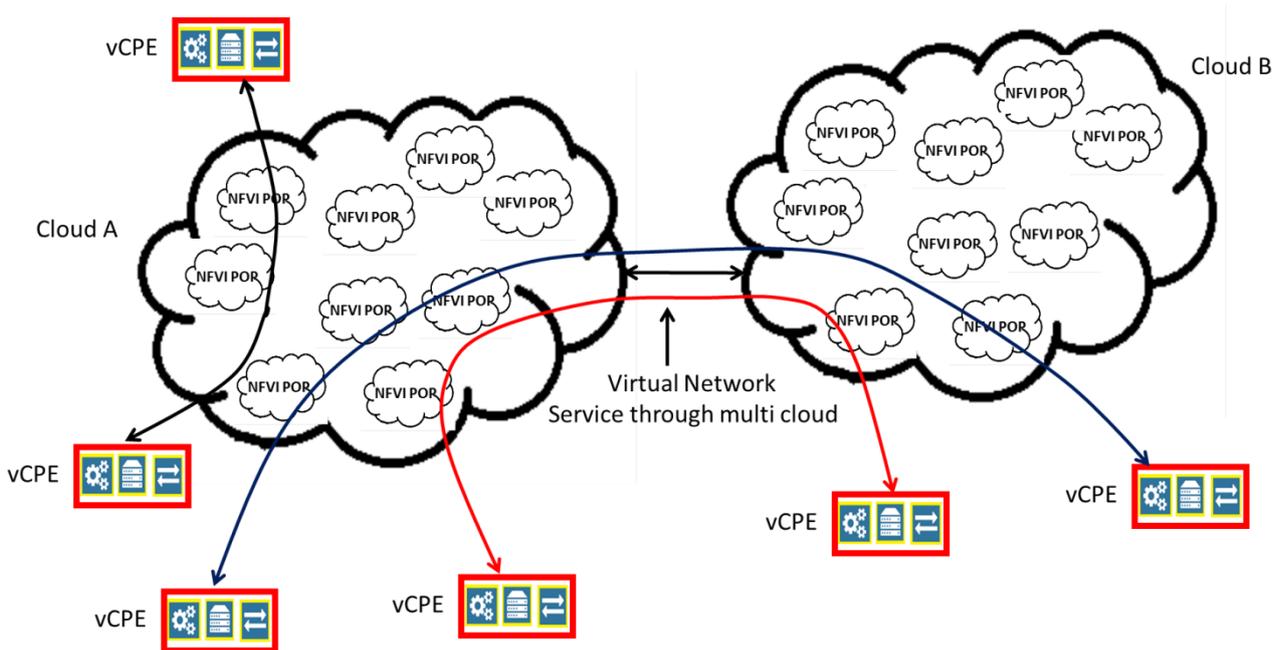


Figure-8 VNS in Multi Cloud scenario – Different administrative domains

The interconnectivity between two different clouds using the NFV framework is as shown below in figure-9.

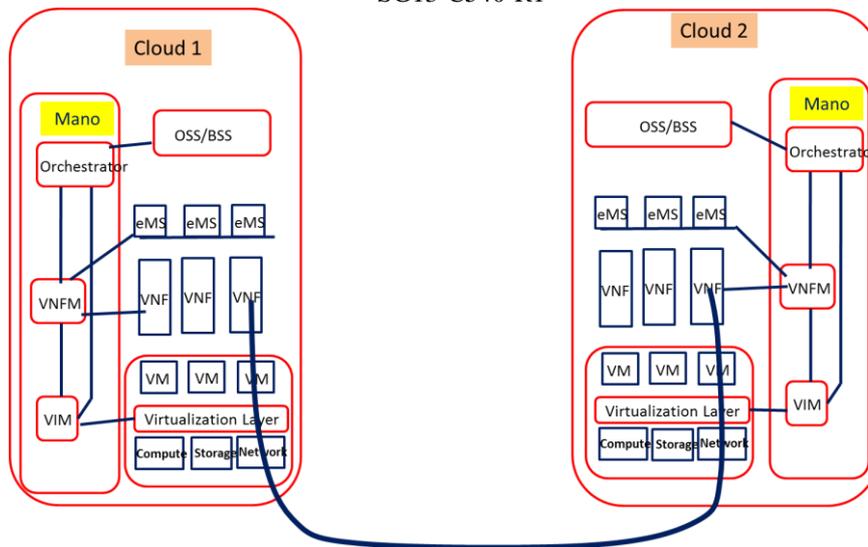


Figure-9 Interconnectivity in Multi Cloud scenario – Different administrative domains

Virtual Network Service (VNS) is delivered through an ordered set of Virtual Network Functions (VNFs) chained into Service Function Chains (SFCs) or VNF graphs interconnecting the virtual network resources to handle the traffic in a desired way. Such VNFs are created in software and hosted on Virtual Machines (VMs) instantiated in NFVI PoPs of one or more clouds. Effective coordination amongst Management & Control Platform(s) (MCPs) of Cloud Service Provider(s), BSS/OSS of Telecom Service Provider and NFV-MANO (NFV Management Orchestrator) is the key to successful Virtual Network Service (VNS) delivery over multiple clouds.

7 Management Framework for End to End Fault and Performance issues in Multi Cloud Virtual Network Services

7.1. Background

7.1.1 The approach described here is generic in nature and applicable to all member states interested in ushering state-of-the-art cloud based telecommunications network deployment in their countries. Such deployments are expected to give a number of benefits over traditional deployments using physical appliances. Some of the benefits are: flexibility of obtaining resources, ease of scaling and descaling, freedom from proprietary hardware and software, ease of redeploying resources, risk mitigation, ease of deploying new services and reduced total cost of operation.

7.1.2 Traditional Practice

The traditional practice largely involves use of physical network appliances like routers, switches, broadband remote access servers, and middle-boxes like firewalls, deep packet inspectors or load balancers. These integrated hardware and software solutions are normally closed and proprietary leading to vendor lock-in, thereby making expansions and deployment of new services difficult and time consuming. Such equipment are also not amenable to easy scaling or redeployment of resources. The power and space requirements as well as the total cost of operation are higher in physical element based networks.

In traditional networks, time-tested standards relating to fault, configuration, accounting, performance and security (FCAPS) are embodied in ISO Common Management Information Protocol (CMIP) and ITU TMN M.3010 and M.3400 recommendations. Network management based on relevant standards provides five nines availability and carrier grade reliability.

7.1.3 Benefits of multi cloud environments

Multi-cloud computing, coupled with Network function virtualization (NFV), provides numerous advantages to the service providers including ease of deployment, ease of scaling, ease of introducing and switching off services and reduced cost of operation. This may increase viability of telecommunications business and lead to thriving telecommunication sectors in the -countries. However, there are a number of reasons as to why the combination of multi-cloud & NFV i.e. VNS over multiple clouds needs a strong fault & performance management system to be a viable replacement for traditional networks. For carrier grade availability & reliability of up-to five nines (99.999%) for multi-cloud VNS, there is a need for standardization of techniques for fault and performance detection and localization to deal with complexity in such networks as the anomalous behaviour could be in the hardware, virtual machines, VNFs, SFCs or at the service levels.

7.1.4 Multi-Cloud challenges

Nowadays, the telecommunication's networks have traditionally been designed to provide high availability and standards-based quality of service. In virtual network, services deployment over multiple clouds identifies new challenging to equip multi-cloud management systems to deal with performance issues. Especially, that virtual network services relay over underlying physical network and "software" infrastructure (NFV-based infrastructure). Therefore, the end to end management are related to physical, virtual layer or the virtual network functions of multi-cloud environments where virtual machines hosted particular NFV are hosted.

In fact, the traditional deterministic methods fail to deliver in virtual environments in which virtual resources can be dynamically scaled, migrated or destroyed. It is important to propose to use predictive techniques to be able to identify management issues before or after they have occurred.

In hybrid telecommunication networks with physical appliances and "software" infrastructures, the deterministic methods ensure carrier grade availability and reliability. On the other side, the service function chains using virtual resources over multiple clouds provide a number of complex factors and make it imperative to use predictive methods for assuring carrier grade availability.

The "software" infrastructure provides the advantages of breaking free from proprietary network appliances and brings in ease of scaling. Implementation of "software" infrastructure over multiple clouds adds new advantages, leveraging greater flexibility in obtaining resources, avoiding total outages, proximity to customers and lower total cost of operation.

The one of the main challenges identified in NFV-based systems are related to change management (including single or cascade faults) and performance issues, which have strong impact on whole environment. The precise detection of source of fault and area affected by faults are key aspects in telecommunication's software infrastructure, whose performance starts to be comparable to performance achieved over traditional networks.

Some of the key challenges in Multi-Cloud VNS are as follows:

- Absence of an FCAPS framework
- Non-applicability of traditional rule based techniques when used in today's networks
- Multiple layers of implementation: physical infrastructure, NFVI (Virtual Machines), Virtual Network Functions (VNF) and Virtual Network Services.
- Massive distribution of network functions over disparate clouds.
- Multiple control centres: cloud management systems, operators' OSS/BSS and NFV-MANO (Management and Orchestration) and multi-cloud management platforms.

7.1.6 Change management in multi-cloud

The change management in multi cloud-based network services would be a collaborative process among the elements constituting the service and the management systems involved. Modern communication systems produce large volumes of high-dimensional operational data. In such a case, analysing the data to get an actionable understanding of the situation becomes difficult. The fault, configuration and performance system should be able to identify potential performance

hazards or may result in a fault that would require resources to rectify. In particular, the key challenges of change management in virtualized environments are related to:

1. Fault detection to notify impending or actual fault and performance issues
2. Determination of the root cause of the problem by identifying the resources that are malfunctioning or the severity with which they may malfunction in the future

7.1.7 Performance management in multi-cloud

The problem of detection and diagnostic given conditions that degrade network performance deals with the detection of any condition that has already led to or could lead to degraded performance or failure as well as identification and localization of manifest and impending faults. The performance management is part of pre-validation, with simulated traffic, as well as can be done on live environment to check the real behaviour of the network. The performance management is based on Quality of Service (QoS) metrics, which measure if the network behaves according to expectations, or Quality of Experience (QoE) metrics, which ensure the user perception of the network and service quality.

7.2 Description of framework

7.2.1 Introduction:

Telecommunications networks have traditionally been designed to provide five nines/high availability and standards based quality of service. In virtual network services deployment over multiple clouds, it is challenging to equip multi-cloud management systems to deal with fault and performance issues. Virtual network services have underlying physical and network function virtualization infrastructure. The telecommunications network functions in the virtualized form go into the virtual machines provided by the NFVI. When performance deviates from normal or a fault occurs, there is no access to the physical hardware for telecom operators to test. The root cause of the problem could be in the physical, virtual layer or the virtual network functions. The traditional deterministic methods fail to deliver in virtual environments in which virtual resources can be constantly scaled, migrated or destroyed. It is proposed to make use of predictive techniques to be able to identify fault or performance issues before or after they have occurred.

7.2.2 Framework scope

The framework is intended to facilitate effective end-to-end fault and performance management in multi-cloud virtual network services. In telecommunication networks with physical appliances, deterministic, methods ensure carrier grade availability and reliability. However, when telecom service providers' service function chains are using virtual resources over multiple clouds, a number of complex factors make it imperative to use predictive methods for assuring carrier grade availability. This recommendation discusses open source non-discriminatory procedure to ensure this objective.

7.2.3 Ecosystem Description

Network Function Virtualization (NFV) provides the advantages of breaking free from proprietary network appliances and brings in ease of scaling. When NFV is deployed over multiple clouds then there are added advantages like greater flexibility in obtaining resources, avoiding total outages,

proximity to customers and lower total cost of operation. Cloud technology can multiply the benefits of NFV. It could provide greater flexibility in obtaining resources, bring Network Service Provider's (NSP's) points of presence close to customers, provide an opportunity to optimize performance and control cost. However, NFV over multiple clouds has not yet attained the level of performance to be a viable replacement for traditional networks. One of the main reasons is the absence of a standard based Fault, Configuration, Accounting, Performance and Security (FCAPS) framework for the virtual network services.

Traditional networks have time-tested standards relating to fault, configuration, accounting, performance and security (FCAPS) as embodied in ISO Common Management Information Protocol (CMIP) and ITU TMN M.3010 and M.3400 recommendations. In combination of NFV & multiple clouds i.e. in Multi-Cloud VNS, the concerns regarding five nines availability, carrier grade reliability and quality of service parameters, like latency and packet loss, need address.

In NFV, faults and performance issues can have complex geneses within virtual resources, compute, storage and networking, as well as virtual network functions and cannot be effectively handled by traditional rule-based systems. To be able to make use of the multi-cloud paradigm effectively, it is more important that to fix Fault and Performance issues. Without a robust mechanism for handling Fault and Performance, service providers would find meeting service level agreements (SLAs) difficult and growth of the promising technology of NFV might get hampered. The framework should contain mechanisms for handling both manifest and latent fault and performance issues.

7.2.4 Network Service Structure

A Virtual Network Service (VNS) can be described as an end to end implementation using service function chain (SFC) or virtual network function forwarding graph (VNFFG), interconnecting the virtual network resources. SFC or VNFFG is an ordered set of VNFs in the virtual environment that represent functions like routers and broadband network gateways or middle-boxes like load balancers and firewalls, which act on the traffic in the sequence they appear in the chain. Such VNFs are hosted on virtual machines (VMs) instantiated over physical data centre and network resources. An example of end-to-end Multi-Cloud VNS is shown on the left side of Figure-10 below.

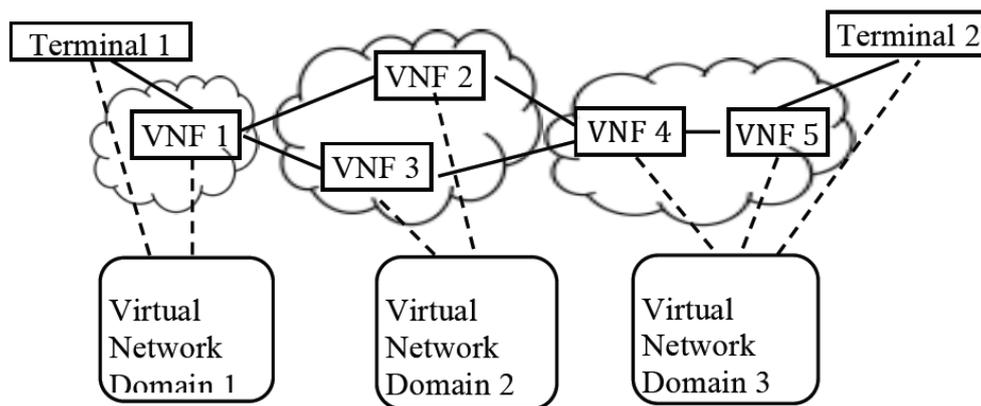


Figure-10 Multi domain end to end virtual network service

The detailed network and VNF connectivity diagram in multi cloud scenario is depicted below. In this diagram, two VNFs in first cloud, two VNFs in second cloud and three VNFs in third cloud are connected as per the VNF Graph to provide the end to end network service.

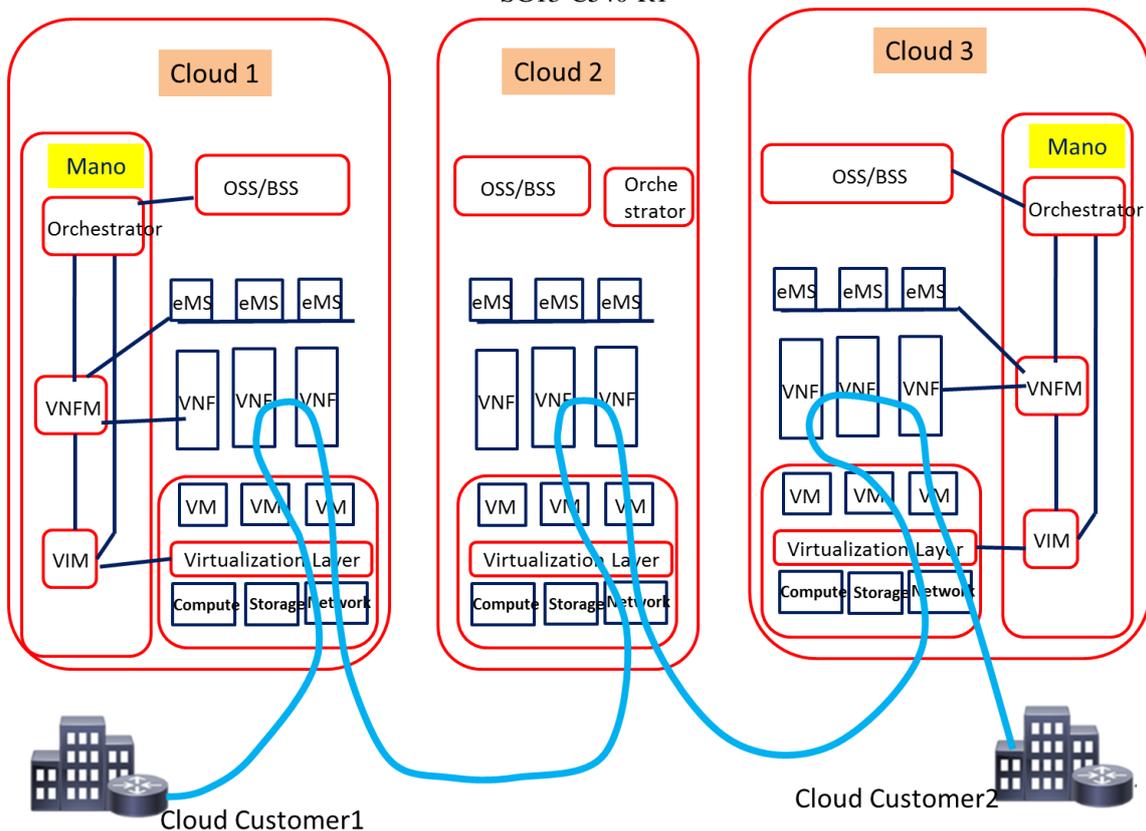


Figure-11 VNF Forwarding Graph for Multi domain end to end service

Faults happen due to physical or algorithmic causes. Faults may occur for a number of reasons, prominent amongst which are malfunctioning or failed devices because of hardware or software failures in VMs or VNFs, failure of links and configuration errors. There could be other reasons like cyber-attacks, disasters or environment factors. Faults appear as errors. Errors in turn are deviations of a system from normal operations. Errors are reported through system alarms. Alarms are notifications about specific events that may or may not be errors. The degradation of a service can be detected through notifications, counters or meters. The Fault detection and Performance Management system should be able to identify which issues are potential performance hazards or may result in a fault that would require resources to rectify. Four levels of severity of events & alarms have been defined in ITU standard X.733: Critical, Major, Minor, and Warning [ITU92]. The critical alarm comes when the service can no longer be provided to the user. Major alarm indicates the service affected condition while minor means no current degradation is there, but if not corrected may develop into a major fault. A warning is an impending service affecting fault or performance issue. It is for the predictive capabilities of the Fault detection and Performance Management system to predict what faults will develop and with what severity levels.

Communication networks are widely distributed and are complex. The variety of FCAPS issues that can afflict them is large. The system to detect, diagnose and localize any condition that degrades network performance requires:

- Detection of any condition that has already led to or could lead to degraded performance or failure. The reasons could be manifest faults, hidden faults or inconspicuous deviations. The goal of such detection would be to sense and notify impending or actual fault and performance issues.

- Identification and localization of manifest and impending faults as well as performance problems. The goal of such localization would be to determine the root cause of the problem by identifying the resources that are malfunctioning or the severity with which they may malfunction in the future.

Any end-to-end fault and performance management system should take into account all the markers including alarms, notifications, warnings, observed behaviour, counter readings and measured values of performance indicators to carry out the above functions.

7.2.5 Approaches for End-to-End Fault & Performance Management

End-to-end Fault and Performance Management in multiple cloud based Virtual Network Services is a collaborative process among the elements constituting the service and the management systems involved. Modern communication systems produce large volumes of high-dimensional operational data. In such a case, analyzing the data to get an actionable understanding of the situation becomes difficult. In general, predictive approach is recommended that takes a learning route to solve the problem of the complex interaction of features of fault detection and localization. More specifically, however, a model based on a judicious combination of shallow as well as deep structures / architectures in machine learning, can be used for prediction of fault & performance issues along-with the severity levels of impending faults with a high level of accuracy.

A. Model for Fault Detection and Localisation

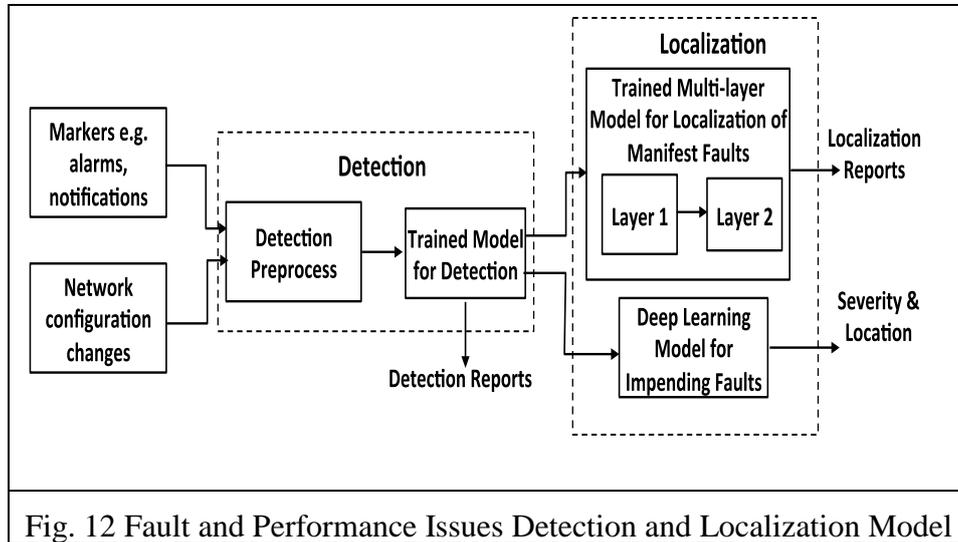


Fig. 12 Fault and Performance Issues Detection and Localization Model

The proposed model approach has predictive and deductive properties to meet the Fault and Performance Management requirements. Run time monitoring and measurements, alarms, notifications and warnings, configuration changes, measurements and environmental factors are all used along with the models trained with historical data to draw inferences about the manifest performance and fault issues. Additionally, decision about impending faults is taken using these inputs and the predictive properties of machine learning models. The detection system first decides whether there is a manifest or an impending fault or a performance issue. Based on this, the system will launch into identification and localization. Detection is essentially a two-stage binary classification problem that first classifies the outcome into ‘normal performance’ and ‘abnormal performance’ or ‘faulty’ and ‘not faulty’ classes. Then for the ‘faulty’ or ‘abnormal’ cases, it decides whether the problem is manifest or impending. Failure prediction needs to be accompanied with a high probability of correctness as actions following such a prediction involve cost. For localization, the model uses a multi-layered strategy. First, the broad category of the fault is determined (Layer 1). The system then does fine grain localisation (Layer 2) within the broad category and identifies the actual device(s) having a fault or suffering from performance degradation as well as their severity levels. Location & Severity of impending faults need deeper predictive structures.

B. Markers and Metrics for Fault Detection and Localisation

There are events relating to communication, quality of service, processing, equipment and environment that produce alarms, notifications, warning or error messages, measurements, counter values and conditions. Of course, many of the markers will appear in more than one type of fault or performance issue. Once, trained, detection and localisation algorithms would be able to pick out relevant markers and use them to predict the type of condition that may have arisen. Some of the markers related to mobile, fixed and broadband networks are given in Table 1 below.

TABLE 1 ILLUSTRATIVE LIST OF MARKERS

Mobile Network	Fixed Network	Broadband
Carrier/Interference Ratio	No Dial Tone	Intermittent Connection
Radio Link Time Out	Channel Noisy	Low Data Rate
Time Slot Shortage	MDF Jumper Disconnection	Phone Works Broadband Down
Occupied Bandwidth	Line Card Port Faulty	Repeated Training
RX Noise Floor	Primary Cable Fault	LAN Lamp Off
Radio Power	Distribution Cable Fault	Line Noisy
Frequency Error	DP Fault	DSLAM Port Mismatch
Antenna Tilt	House Wiring	No Ping
Signal Strength	MDF Fuse Blown	ADSL Lamp Flashes/Off
BTS Down	Customer Instrument Faulty	No Line Sync
Handover Failure	Dis in One Limb	Browsing Issues
Roaming Failure	Earth Contact	Micro-Filter Faulty
Packet Loss	Drop Wire Fault	No Comms
Hypervisor Alarm	Ring Tone Fault	Dropouts
Registration Failure	Message Fault	No Authentication
Low CSSR	Delayed Dial Tone	

TABLE II EXAMPLE SHOWING MANY-TO-MANY RELATIONSHIP BETWEEN FAULTS AND MARKERS

	Phase Error	Power	EVM	Rx Noise Floor	Origin Offset	Occupied BW	Frequency Error	C/I Ratio
Call Drop*	Y	Y	Y	Y	Y		Y	Y
Call Blocked**		Y	Y	Y	Y	Y		

*Radio link timeout; **Time Slot Short; EVM: Error Vector Magnitude; Rx: Receiver; C/I: Carrier to Interference Ratio; Y: Marker Present

It is important to have an objective and quantitative metrics for good service to the consumers, fault localisation and identification of the root cause of performance deviations.

C. Training Datasets

The quality & quantity of the datasets affect the learning and prediction performance of machine learning algorithms. Information about faults, observations and restoration details in the telecommunication networks is contained in the fault dockets, test reports, central office system logs, outdoor maintenance staff logs, cable maintenance staff diaries and docket closure reports. Fault severity has three categories with 0 indicating no faults, 1 indicating a few faults and 2 indicating many faults. There are datasets for event type, the features logged, the resource affected and the severity type. The severity type is different from fault severity and classifies the warning given by the system.

D. Shallow and Deep Learning Methods

Shallow structures are simpler with one stage of non-linear operation, e.g., one hidden layer in neural networks. Here, the Support Vector Machine (SVM) Learning Method is a supervised learning method that analyses data and recognizes patterns. However, Deep learning architectures through stacked auto encoders would have more than one level of the composition of non-linear operations in the function learned. One of the key advantages of deep learning is the automatic extraction of high-level features from the given dataset. This is a distinct advantage over the difficult feature engineering in shallow structures that require human intervention. In deep learning, higher-level features are learned as a composite of lower level features. In this way, features are learned at many levels of abstraction, making it easier to grasp complex functions that map the input to the output directly from data.

E. Detection of Fault and Performance Conditions

Fault and Performance issues may range from simple single point failures to multiple correlated or uncorrelated events. A fault presents itself in the form of system malfunction and notifications from faulty and other connected devices. The failure detection mechanism should be able to filter out dependent and routine operational events so that resources are not wasted in localizing these problems. In NFV, the faults in VM, VNF & Virtual Network cause Virtual Network Services (VNS) to behave abnormally. For example, failure of a Gigabit Ethernet interface on the core router may cause some or all of the virtual private network (VPN) links of many customers to be non-functional. In this context, the goal of the Fault & Performance detection mechanism is to correlate alarms, notifications, measurements and other markers generated by events to infer manifest or predict impending performance and fault conditions. Some errors may be cleared by the system, others may produce warnings that may signal impending problems while still another may produce faults that bring down functionalities and make themselves evident. The trained shallow machine learning models learn from the past events relating to faults and their resolutions. The models work in two stages: the first stage just makes a decision between 'fault' and 'no-fault' conditions, while the second stage does a more detailed examination of the markers to choose between 'manifest' and 'impending' faults. Minor faults & warnings would be the main contributors to the impending faults and need to be analysed to make this decision. With correct segregation, the localization stage would be able to carry out its functions properly.

F. Localization of Fault and Performance Conditions

The severity level of the faults indicates whether they are warnings, minor, major or critical. In the case of major & critical faults, devices degrade performance or stop working and need immediate action. Minor faults do not affect service and can be scheduled for localization accordingly. Warnings, along with the state information, provide insight into the degrading health of devices and could signal a major impending fault. In multi-layer fault identification and localization system, at Layer I, it detects the brand category of fault and then at Layer 2,

does a fine grain classification. In the case of impending faults, the system predicts the locations and severity levels of the developing faults.

7.3 Conclusive Analysis of Framework

Deployment of Virtual Network Services on multiple clouds is the key to successful provision of large real time and distributed services. However, for this scenario, concerns about five nines/high availability (99.999%) and quality of services parameters like latency and packet loss still remain.

Based on study of the markers and metrics related to fault & performance management of communication networks, handling fault & performance anomalies when they occur is crucial for the success of NFV deployments over clouds. In the proposed model for detection & localization of manifest & impending fault & performance issues, some of the aspects of detection and localization of faults have been implemented using shallow and deep structures respectively. It may be observed that SVM for classification performs well for detection of faults / no-faults or manifest / impending fault situations. This information can then be used with localization function for deeper analysis of the warnings to predict impending faults and their severity. Deep structure of stacked auto-encoder may be used for careful examination of 'warning' cases to predict the severity of faults.

Hence, it can be reasonably concluded that a fault detection and localization system based on a combination of shallow and deep machine learning architectures/structures would be useful in handling voluminous operational data of high dimension for detection and localization of Fault and Performance issues. While simpler detection can effectively be handled by, shallow machine learning structures like Support Vector Machine (SVM), however deeper structure i.e. the stacked auto encoder can be useful for a more complex localization function where a large amount of information needs to be worked through to get to the root cause of the problem.

Annex A

<Annex Title>

(This annex forms an integral part of this Recommendation.)

<Body of annex A>

<Appendix Title>

(This appendix does not form an integral part of this Recommendation.)

<Body of appendix I>

Bibliography

[b-DMTF OVF]

DMTF Standard DSP0243 Version 1.0.0 (2009), Open virtualization format specification.
