INTERNATIONAL INTERCONNECTION FORUM

FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

Operational Impacts of NFV on Int. Carriers networks

This document provides the i3 forum's perspective on operational impact of NFV on carrier networks. It does not intend to duplicate other existing specifications or documents on the same issue, but to complement these documents with the perspective of the international carrier members of i3 forum.

Table of Contents

1. Editorial Team

Company	Name	Role
Metaswitch	Micaela Giuhat	Project co-leader and Chief editor,main contributor
TI Sparkle	Alessandro Forcina	Project co-leader and Chief editor
Tata	Alan Tai	Contributor
Telenor	Jay Gupta	Contributor

2. Scope and Objective of the Document

The development of new technologies, such as network function virtualization, while bringing much needed OPEX and CAPEX savings to networks, have significant operational impacts when they are first introduced.

This document intends to identify the operational impacts associated with the introduction of NFV in an international carrier environment, and in some instances provide the industry consensus on how best to integrate the new technology. This document is not intended to have a comprehensive list of operational impacts, rather to highlight the most important ones, and raise awareness these impacts.

3. Acronyms

BSS	Business Support System
FCAPS	Fault, Configuration, Accounting, Performance, Security
NBI	North Bound Interface
NFV	Network Functions Virtualization
OSS	Operations Support System
SDN	Software Defined Network
SLA	Service Level Agreement
MANO	Network Functions Virtualization Management and Orchestration
NFVI	NFV Infrastructure
NFVO	Network Functions Virtualization Orchestrator
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Function
VNFM	Virtualized Network Function Manager
EMS	Element Management System NMS Network Management System

4. Introduction

Migration to any new architecture, including NFV, impacts most operations functions, from initial requirements and testing to final implementation and billing, therefore these impacts need to be well understood by Int. Carriers looking to implement NFV.

According to Deloitte Consulting, key considerations for effective operations in NFV/SDN networks include:

- Service strategy and design needs to maintain status quo in terms of operational performance for traditional services being migrated to NFV/SDN.
- Carrier grade performance needs to be ensured by leveraging features such as dynamic creation and migration of virtual network functions to meet availability requirements.
- Operations needs to migrate to “management by exception” wherein most common errors and performance degradations are addressed via automated self-healing and self-optimization rules.
- Critical functions such as fault, outage, and performance management need to be supported with smooth handoffs across different teams which maintain physical and virtual network resources.
- The skillset of operations teams needs to be expanded to include scripting capabilities (or their equivalent via GUI-based tools) to be able to effectively create “recipes” for managing software VNFs.
- A DevOps-based model which drives closer coordination between operations and development teams needs to be introduced to improve service agility and quality.

The role of operations spans across the entire service lifecycle, and each of these stages is impacted by the introduction of NFV and SDN based networks. The entire operations model including processes, tools and technology, as well as people and organization needs to be redesigned for each functional area within Service Design and Fulfillment, Service Operations and Readiness, as well as Service Assurance.

As a result, i3 forum has considered useful to provide the Carrier industry with a deliverable addressing the basic issues related to the operations of virtualize network platforms focusing on:

a) General areas of impact

b) Highlight the areas that need to be further analyzed

In the following section we used as a guideline a clear distinction among the operational impacts related to:

- Processes
- Technical
- Organizational

5. Process Impacts

The following teams and processes are being impacted specifically by any NFV component identified are:

Team/Process	Impact
Engineering	Understand vendor evaluation criteria, and architect the overall solution
QA	Create and perform PoC testing in the QA Lab
Commercial/Purchase/ Vendor Management	Change Commercial Agreement for NFV specific terms
Site Technician	Site Survey (Power, Space, IPs) required by NFV
Program Manager	To oversee the entire project
IP	Network connection and IP assignments for NFV deployments
Security	Create assessment for security vulnerabilities for the specific NFV function
Mediation	Ensure the CDRs are in correct format and system has the ability to retrieve CDR
Alarm	Integrate the new device SNMP traps in alarming system or use new technology (see technical impact)
Provisioning	Training to add new customer
Automation	Automation of the provisioning Process
Support	Training to support and troubleshoot customer issues

Systems

- Backend database – Has to support new device data
- Inventory System – Has to add the new device into the inventory system

All of the processes will be impacted by any new addition (not related to NFV), however the processes that are mostly impacted by NFV are the one that are bold in the tale above.

6. Technical Impacts

According to the several research papers (Deloitte, ATIS, ONF), the following technical impacts need to be taken in consideration:

- Activation and Provisioning
- Change management
- Inventory management
- Performance management
- Fault Management
- SLA management
- OSS/BSS
  - Interfacing and interworking with existing network
  - NVF Manager
  - Orchestration
- Other (e.g., dimensioning, security)

While some of the above aspects will be touched upon, the most important technical aspects come from integration with existing OSS/BSS systems, and the ability to perform in a hybrid physical/virtual environment.

6.1. Activation and provisioning

- Portal for workflows
- Templates
- Provisioning interfaces such as YANG, NETCONF, and TOSCA

6.2. Change management

- A software-based workflow should be implemented to acquire approvals for changes, and automatically effect approved changes via the centralized orchestrator

6.3. Inventory management

- Physical inventory data needs to be enhanced to include VNF and virtual network details in order to build an integrated view of utilization of logical and virtual resources across the infrastructure
- A software repository will be needed to maintain details such as package versions and license usage
- Auto discovery algorithms and version controlled archival systems need to be implemented which can help establish a real-time topology view and inventory reporting system. This reduces troubleshooting issues by providing the ability to identify the exact topology at the time of an event

6.4. Performance management

- New or revised KPIs/KQIs e.g., Infrastructure Response Time, VNF Contention Analysis, and sophisticated algorithms need to be defined that can correlate inputs at

all levels and provide insightful performance views across VNFs and virtual infrastructure

- Predictive analytics needs to be leveraged to proactively manage resources based on predicted faults, dynamically update policies and rules based on real-time traffic characteristics. This can help minimize the occurrence of issues across the virtualized infrastructure
- Self-optimization capabilities need to be introduced in performance management modules which can optimize configuration based on current network performance, e.g., scale up VMs, add new VNF instances for load balancing, configure new routes between VMs, etc

6.5. Fault Management

- The service model should be leveraged to identify all components and links impacted by a particular fault. This can be done by using the YANG model to identify which components of a service are impacted, trigger policy-based alarms, and suppress duplicate alarms
- Policy driven self-healing strategies need to be implemented to route around faults identified via monitoring of various instances of a VNF across VMs and performing distributed failure checks

6.6. SLAs

- Carrier-grade SLA/OLAs need to be enforced on Commercial off the Shelf (COTS) hardware and software components to ensure that off-the-shelf solutions can support carrier-grade network requirements. These SLAs and OLAs also need to be enforced across organizations supporting the underlying platform on which network services are provided
- A common SLA/OLA framework needs to be established with all vendors providing software-based VNFs or controllers. While the framework can be used to establish implementation guidelines, it must be flexible enough to support different requirements based on VNF type
- SLAs and OLAs need to include key operational parameters such as service response time and scalability, packets lost, etc. and not be limited to the time in which an assigned ticket is acknowledged

6.7. OSS/BSS

Carrier OSS/BSS environment provides essential business functions and applications such as billing, and operational support.

With the NFV, some of the functions that were statically determined become automated, creating the benefits that are expected to come with NFV:

- Agility

- Openness
- Speed
- Automation

By design, NFV infrastructure dynamically reallocates its resources between different virtual network functions to meet variations in traffic composition. Current OSS systems cannot support this level of real-time dynamics and policy driven real-time service variation.

Two main requirements are being imposed on the OSS to support NFV:

- Service modeling to automate mapping to devices, vs. static adapters or rigidly specified service parameters
- Interworking with network orchestration platform: The OSS will configure the NFVI, but the NFV orchestrator will configure the actual virtual network functions (VNFs) running on this infrastructure and the allocation of resources to VNFs. The OSS and NFV orchestrator must be able to interwork and refer to a common policy platform and management information mode

There will be a sharing of responsibility between the traditional OSS and the newly deployed NFV orchestration. The OSS will manage the relatively static configuration parameters and limit overall resources assigned to sub-networks or services. The NFV orchestration platforms will then dynamically manage these network resources to apply policy-based services in real-time to individual traffic flows.

OSS systems, consistent with the ETSI NFV architectural framework, must support the Os-Ma interface between the traditional OSS/BSS and the NFV Management and Orchestration (MANO) framework as shown in figure below. OSS/BSS systems delegate fine-grained management of the NFV Infrastructure and the specific VNFs to the VIM and the VNF Manager, which in turn are orchestrated by the NFV Orchestrator (NFVO). Thus, the OSS/BSS will be responsible for the high level configuration of the infrastructure and network functions, but the NFV MANO framework will manage the dynamic aspects of infrastructure and services.

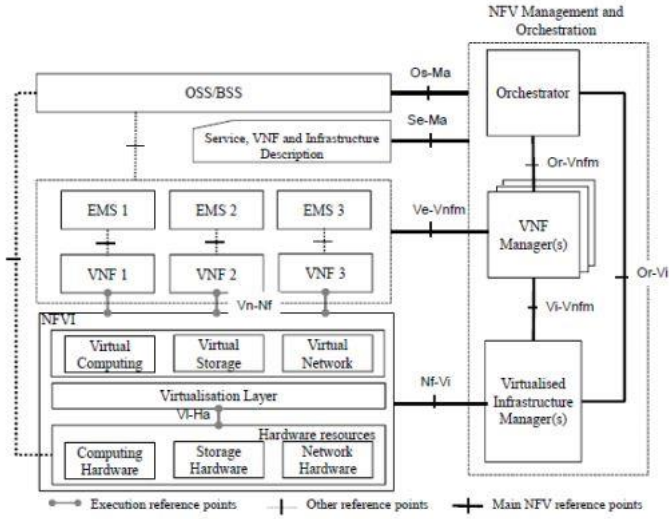

Figure 1: ETSI NFV Reference Architecture

OSS/BSS Evolution

Carriers moving to deploy virtualized network architectures based on NFV, are likely to evolve the OSS/BSS systems in stages. Existing operator networks have a significant installed base and it is unrealistic to replace all existing infrastructure.

According to the Open Network Foundation, the following figures depict typical network of today, where the network functions are based on physical hardware (PNF) and are controlled by their individual EMS through the OSS/BSS layers, and network connectivity is provided by a static EMS provisioned WAN network, transitional stage and the longer term vision where the network functions are all virtualized and orchestrated by an NFV Orchestration platform:

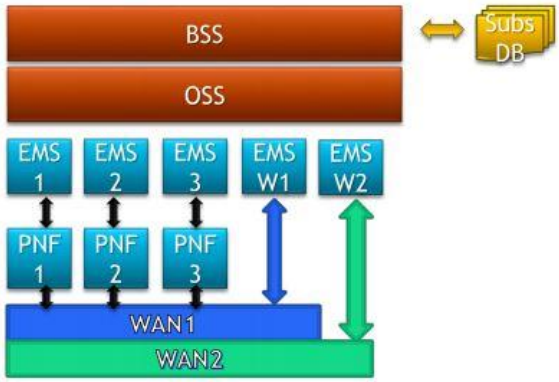

Figure 2: Existing OSS/BSS

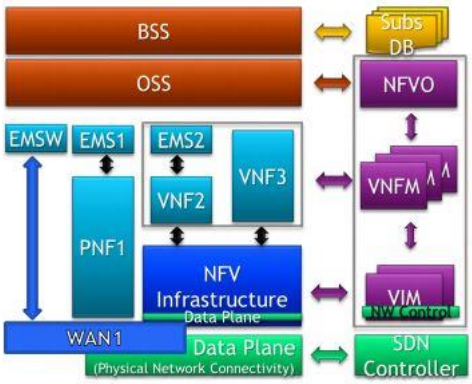

Figure 3: Transitional Stage

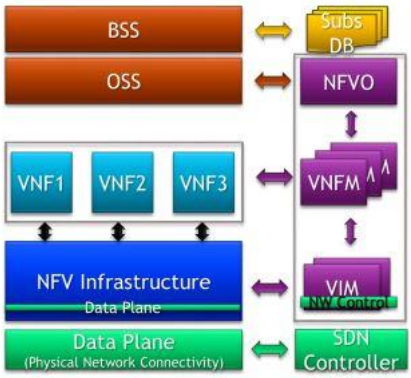

Figure 4: Long Term Vision

The ETSI NFV ISG anticipates that, in the long term, the VNF will be fully managed by the corresponding VNF managers, but, in the interim, there will still be a (possibly reduced) EMS manager attached to each VNF that will assist the VNFM in the management of the VNF.

7. Organizational Impacts

The NFV vision of the future will only be achieved by telecom service providers that embrace NFV fully and are prepared to implement a fundamental organizational transformation to make the most of what they enable. Below is a list of potential pitfalls that could make the migration to NFV a challenging task:

1. **Culture**
   Decades of procuring and building networks in the traditional way have created a culture that may put up strong resistance to the kinds of changes that are needed. Resistance may take many forms, including:
   - Persistent disbelief that cloud-based software can ever deliver carrier-class, five-nines service availability
   - Inability to trust any vendor other than the traditional suppliers to deliver telco-grade solutions
   - Reluctance to acquire the new skills necessary to build and manage services in cloud-based software environment

2. **Headcount**
   Resistance will also arise from the simple observation that, if NFV delivers major savings in operational costs, along with more and more automation, a lot fewer heads will be involved in operations.

3. **Performance Evaluation**
   Telecom service providers must evaluate different vendors' solutions versus their existing proprietary hardware equipment. This applies in particular to transcoding evaluations, as software based transcoding still lags behind purpose-built DSPs. However, vendors are actively coming up with innovative NFV solutions for transcoding.

4. **Re-architecting NFV Solution to Fit Existing Infrastructure**
   This requires a lot of planning, from system integration to backend office modifications. The migration will likely occur in phases to be successful. For example:
   - Product introduction
   - Hybrid existence between legacy and NFV
   - Full NFV enablement

5. **Inter-departmental Commitment**
   NFV will touch many different teams within the organization. It's imperative for all departments to understand the benefits and changes that are required on their part to make NFV successful. Examples of some of the challenges include:
   - The capacity management team has to evaluate the new platform capabilities and different ways to size capacity.
   - The technical staff has to be trained on the virtual environment and new setup steps.
   - IT needs to plan for the new way of managing to, and investing in, virtualization and legacy equipment.
   - The inventory system has to be updated to reflect the virtualization setup.
   - Service Operations needs to understand out how NFV impacts the provisioning of new services.
   - IP Management needs to re-architect the new NFV schema, possibly using higher bandwidth/speed port for NFV equipment.

6. Customer Migration Plan

Customers have to be informed about the changes and the migration plan.

8. Standards

- eTOM
- ITIL
- DevOps
- TM Forum
- OPEN-Orchestrator Project
- Open Source MANO
- ETSI

9. Conclusions

Network Function Virtualization represents a step towards much increased efficiency, speed of deployment and innovation, as well as significantly decrease in operations and support.

As any new technology, the introduction phase provides carriers and vendors alike with a steep learning curve, with one of the most important aspects being the impact in the operational processes that are now in use in all carrier environment.

This paper has tried to show some of the most important impacts on processes, technology and organizational aspects.

There are several areas that have been specifically mentioned as being important and that will need further analysis:

- Security processes
- All technical impacts
- Organizational savings, which could be expanded to a more generic TOC that includes the economic benefits of NFV

10. References

1. ETSI GS NFV 001 v1.1.1 (2013 -10) Network Functions Virtualization (NFV); Use Cases
2. ETSI GS NFV 002 v1.1.1 (2013 -10) Network Functions Virtualization (NFV); Architectural Framework
3. ETSI GS NFV 003 v1.1.1 (2013 -10) Network Functions Virtualization (NFV); Terminology for Main Concepts in NFV
4. ETSI GS NFV 004 v1.1.1 (2013 -10) Network Functions Virtualization (NFV); Virtualization Requirements
5. Network Function Virtualization – Update White Paper Issues 1
6. 3GPP TS 32.502 v 11.0.0 Self-Configuration of Network Elements Integration Reference Point; Information Service
7. 3GPP TS 32.532 v11.0.0 Software Management Integration Reference Point; Information Service
8. ONF Software-Defined Networking: The New Norms for Networks ONF White Paper
9. TIP Common Model Information Agreement v 1.1
10. Impact of SDN and NFV on OSS/BSS ONF Solution Brief March 1, 2016
11. ATIS Operational Opportunities and Challenges of SDN/NFV Programmable Infrastructure
12. Operationalizing SDN and NFV Networks, May 2015 - Deloitte Consulting LLP