NFV and its Implications on Network Fault Management

Abhinav Anand
# Table of Contents

Introduction ...................................................................................................................................................................................... 03
Network Fault Management operations today ........................................................................................................................................ 03
NFV and Network Fault Management ........................................................................................................................................... 04
Fault Management of NFV ............................................................................................................................................................. 04
Alarm Mediation for NFV monitoring ........................................................................................................................................... 05
Fault Correlation in the OSS tools ....................................................................................................................................................... 05
Future Directions ............................................................................................................................................................................. 05
Conclusion ......................................................................................................................................................................................... 06
Introduction

Network Function Virtualization (NFV) has brought the capability of the Telcos networks on commodity hardware and software. Never before was the pace of change so fast and so disruptive. The question being asked today is whether the disruptions brought on by these technologies will create a paradigm shift in the way networks are being operated today. Another question is how NFV will actually result in significant savings for service providers on Capex and Opex front. This paper focuses on the network fault management area and how it is impacted for providing assurance for virtualized and hybrid networks.

Let us take the instance of network assurance operations and see how it will evolve over time.

Network Fault Management Operations Today

Networks are operated and managed by network operations team, which are typically organized as Level 1-1.5 – or the Network Operation Center (NOC) team where field engineers and Level 2-Level 3 teams are the subject matter experts. Network and IT operations are handled in silos, with duplicate set-ups and teams created for managing the same. We shall see that NFV has both qualitative and quantitative impact on these teams. We will see, on the one hand, some sort of convergence where people in these teams would have to get familiar with both IT and Network operations. On the other hand, their numbers will come down as more automation will kick-in, which NFV technology will inherently provide and support.
Impact on Systems

Service providers currently assure their network by using the point solutions such as fault management (or network surveillance), performance management for capacity management and detecting soft failures in the network, service management by focusing on both SLA management and service quality management. In case of wireless networks, customer experience management has also gained a lot of focus and traction in the recent years.

With NFV, the physical network will start getting augmented with virtual networks. There will be co-existence of these hybrid networks for some time with new virtual networks before the physical networks are completely replaced by the latter. In the context of assurance, one would require additional instrumentation for visibility on the whole new virtual set-up that gets created for delivering the Virtual Network Functions (VNFs).

NFV and Network Fault Management

ETSI ISG has defined a Management and Operations framework called NFV-MANO for management of end-to-end network services deployed over the virtualized Network. This network service (NS) will typically consist of Virtual Network Functions (VNFs), Virtual Machines (VMs), NFV Infrastructure (NFVI), virtual links, legacy devices or PNFs and VNF forwarding graphs. This framework consists of the following functional blocks:

» Virtual Infrastructure Manager (VIM): Performs the orchestration and management function of NFVI resources within a domain. There could be multiple VIMs in the set-up based on Hypervisor technologies used.

» NFV Orchestrator (NFVO): Performs orchestration and management of NFVI resources across multiple VIMs and lifecycle of various network services. The NFVO interacts with OSS/BSS for provisioning, configuration, capacity management etc.

» VNF Manager (VFM): Performs orchestration and management function of various VNFs.

Each of the VIM and VNF Manager supports complete FCAPS (Fault, Configuration, Accounting, Performance and Security) capability as per MANO framework.

Fault Management of NFV

In the initial phases, the strategy or toolsets for monitoring of NFV will not be significantly different from what is currently available for the physical networks. Looking at the ETSI NFV-MANO framework, typically the fault collection or mediation of alarms will happen at the VIM and VNFM from where it will be forwarded to OSS. The faults are related with:

» NFV Infrastructure (Compute, Storage and Network)

» VM related faults

» VNF related faults

The further processing for monitoring, fault correlation and root cause analysis is currently designed to happen at the OSS (on Network assurance) tools. The architecture of assurance will typically look as shown in the following diagram:

In the current scenario, the assurance OSS used by network operations team consists of an umbrella fault management solution or respective element managers to monitor their Transmission, Switching or IP

Figure 1: Architecture for NFV Assurance
Transport networks. However, for monitoring IT infrastructure including applications, servers and data-centers, there is a separate set of enterprise management tools, which had been traditionally used by IT operations team. With NFV, the boundaries between the two will start getting further blurred - a movement that started with the advent of Value-Added Services (VAS), Intelligent Networks (IN) and Service Delivery Platforms (SDP). This would mean enhancement of IT assets monitoring capabilities in the existing network fault management tools or a separate domain manager for IT domain.

**Alarm Mediation for NFV Monitoring**

The key for alarm monitoring is to gather the alarms from various sources in the NFV environment in a 'single pane of glass'. A few illustrations are given below for showing how it can be done in a typical NFV environment:

- Direct SNMP based monitoring of the underlying physical infrastructure (e.g. Esxi hosts) however, this may not be required if VIMs are able to forward the respective fault and performance alarms to OSS systems.

- The element managers deployed for doing FCAPS of the respective VNFs will be a source of alarm for the OSS. These element managers today come with various flavors of north-bound interfaces, which are used for integration with service providers’ existing umbrella fault management systems.

- VNF Managers also have the capability to collect and forward alarms to OSS solutions.

- Both element managers and VNF managers have overlapping capabilities today. However, one significant difference between the two is that while element managers implement proprietary interfaces for managing their respective VNFs, VNF Managers will do the same with industry standard interfaces. Most likely, the network equipment vendors will enhance their respective element managers to play the role of VNF Managers. In either scenario where both EMS and VNF Managers are co-existing or one gets replaced by the other, both or one type will become a source of alarms for OSS umbrella fault management system.

- Apart from the above, syslog based monitoring can be implemented to monitor the VNFs directly by the OSS tools.

- Process and services monitoring is also implemented along with URL and port monitoring in certain cases to get a good visibility of the environment.

- Agents doing Synthetic transactions can also be deployed to monitor customer experience.

**Fault Correlation in the OSS Tools**

A single fault in the network may trigger multiple alarms at the resources and services layer. The number of these alarms may cause ‘noise’ that may overwhelm the monitoring team. Therefore, it is important to correlate these alarms coming from different sources to identify the root cause and cutting down the ‘noise’ for improving operational efficiency. The fault correlation also helps understand how resource failures at NFVI impact network services and customers so that limited operations resources can be aligned and prioritized accordingly.

However, it is important to note that doing fault correlation in a virtual environment will be a complex task as there is a many-to-many relationship between VNFs, VMs and underlying physical resources. Secondly, network Services will be orchestrated through complex service function chaining or VNF forwarding graphs across both VNFs/PNFs. In case network service is provided through multiple service providers deployed in multiple data-centers, the complexity for correlation of the alarms will get further compounded.

**Future Directions**

**Fault Management Evolution and Implications for Network Availability**

The faults that emanate in the Physical world typically require a lot of manual interventions. The capacity issue or hardware related faults in the physical environment are the ones that require manual trouble-shooting, i.e., visit by field engineers etc.

However, in the virtual environment due to in-built resiliency in the environment, these manual activities can be completely done away with. Further, VIMs and VNF Managers are designed to have comprehensive configuration management capabilities of their respective domain, which can be leveraged to fix the Infrastructure issues dynamically in real-time, remotely and even without manual intervention.

One can foresee that each of these VIMs and VNF Managers will be enhanced to have a separate in-built resolution modules that would trigger a corrective action based on alarms generated at the NFVI layer and VM/ VNF layer. Over a period of time with advanced analytic capabilities further augmented in these systems, they will be able to identify not only the issues proactively but also will be able to trigger a series of actions to avoid a larger system impact. This would facilitate a movement which is called “self-healing” networks.

The umbrella fault management system (OSS) will get the notifications of the issues, the automated corrective actions, the resolution status or the events (issues) that could not be resolved even after the launch of corrective actions. This system will also get enhanced with an auto-healing engine that would trigger certain corrective actions through the NFV Orchestrator.
Conclusion

It is a matter of time when inherent resilience of virtual environment, automated workflows and corrective actions within the VIMs or VNF Managers or OSS assurance systems as described above will be able to solve significant number of the problems dynamically and this would result in major effort reduction in the network assurance operations.

Therefore, NFV as a technology is not only going to impact the Capex for acquisition of new networks and services but is also going to have a far reaching implication of reducing Opex for the network organizations.

The industry collaboration is bringing these changes at a breakneck speed. Hence, it is important for operators and their service providers to align their focus for achieving the benefits of this technology.
About the Author

Abhinav Anand is a Consulting Partner in the OSS-BSS practice team of Global Media & Telecom vertical at Wipro. He has played various roles like Head-OSS Design and Solution Architect in various customer delivery engagements. He has around 19 years of experience, 15 of which have been in the network and OSS-BSS space for telecom customers.

He has played program leadership and practice leadership roles providing delivery support, building domain expertise and leading solutions for automation of customer business processes. He is certified on TOGAF Foundation and has detailed knowledge and experience of industry/telecom standard processes and frameworks like eTOM, ITIL. He holds engineering and management degrees from premier institutes and his point of view article on customer/service experience has been published in Vanilla Plus, a leading telecom magazine.

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading information technology, consulting and business process services company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of “Business through Technology.” By combining digital strategy, customer centric design, advanced analytics and product engineering approach, Wipro helps its clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, Wipro has a dedicated workforce of over 160,000, serving clients in 175+ cities across 6 continents.

For more information, please visit www.wipro.com