We are entering a new era of broadband. Competitive, customer and regulatory pressures are forcing operators to significantly boost ultra-broadband availability. As a result, networks and network operations are becoming more complex. To meet the imperatives of bandwidth and coverage, operators are deploying multiple access technologies, which increases network and operational complexity. Virtualization is key to managing this and renewing an operator’s agility and ability to scale. However, the adoption of SDN/NFV requires a fundamental shift in access network management systems. NMS must be cloud-based and open to simplify network management and increase service agility.
Contents

Introduction 3
Classic NMS and its role 3
The limitations of classic NMS 3
The NMS revisited 4
A new dawn with SDN/NFV 4
Easy to integrate 5
Open ecosystem 5
The role of NETCONF/YANG 6
Conclusion 6
Acronyms 7
Introduction
In the era of Intelligent Access, service providers are starting to deploy SDN/NFV in order to manage complexity, reduce costs, and unlock new opportunities within their networks. In doing so, there is an increasing realization that a fundamental change is needed in the network management system (NMS) layer. Traditional NMS strengths such as intuitive visualization, network-wide reconciliation, consistent controls and network health won’t go away, of course. But to keep pace with the network elements, that face shifting responsibilities and capabilities with SDN/NFV, access network management needs to evolve beyond its traditional role.

Classic NMS and its role
In this paper, a NMS managing a non-SDN/NFV network is referred to as a classic NMS. Traditional network elements are self-contained nodes with all the critical management plane functions embedded. The primary management interfaces (CLI, TL1, SNMP) offered by most network elements are either completely proprietary or have significant proprietary extensions to a standardized data model. For OSS/IT integrators, the classic NMS takes care of vendor-specific data model differences and provides abstracted interfaces that the OSS can integrate with, even in a multivendor environment. Additionally, a classic NMS provides simple but elegant man-machine interfaces (GUI/CLI) with which operators can explore and manage configuration, fault and performance data. Expert network operators can use a classic NMS as a powerful tool for configuring network elements and troubleshooting issues at the device level. Classic NMS systems have not stopped evolving and continue to provide value within the FCAPS (Fault, Configuration, Accounting, Performance, Security) silos.

The limitations of classic NMS
However, while a classic NMS has open NBI (northbound interfaces), there is limited standardization across vendors. Each vendor has a different NBI with different syntax and semantics delivered over many different protocols (SOAP, CORBA, FTP, CLI, etc.), and operators can’t directly interrogate or manipulate data. This closed environment has resulted in operators having to perform custom integrations and build multiple vendor-specific management silos.

Over the lifespan of each product, vendors’ release cycles deliver new features and the equipment and NMS go through a number of upgrades. Consequently, testing and validation is required for every new update, which equals additional effort for every vendor, solution and release. This vertically integrated architecture is difficult to maintain and forms a significant bottleneck for the introduction of new services. This challenge is not just limited to multivendor environments; regardless of the vendor landscape, it also affects service provisioning across different network domains or technologies.

The high integration effort and slow innovation cycles are possibly the reasons why classic NMS has become notorious with service provider Chief Information Officers. While the classic NMS is a powerful tool for advanced operators, the specialist knowledge and vendor-specific variations can form a significant challenge for others. As a consequence, it does not encourage a rich ecosystem of tools or ease-of-use for humans or even machines.
The NMS revisited

The next generation of network management systems for the Intelligent Access era needs to be built around a new set of principles. The NMS must support SDN and NFV architectures, be easy to integrate, and fit within an open ecosystem.

A new dawn with SDN/NFV

The NMS takes on new roles for a multi-domain SDN architecture (as shown in Figure 1). The new capabilities and responsibilities that an NMS should acquire are clarified by both SDN and NFV evolutions and explain why purpose-built products are needed to match the multi-layer roles.

As depicted in Figure 1, each network segment or technical domain is managed by a domain-specific controller, now called the domain controller. The architecture is no longer vertically segregated but governed by a hierarchy of horizontal abstraction layers. Each domain controller exposes an abstracted service model northbound. Based on the individual domain controller’s NBIs, a cross-domain (LAN/WAN) service orchestrator can program the end-to-end network. In this view, NMS takes on the role of a domain controller in the multi-domain SDN architecture, providing the integration points for cross-domain service chaining and the home for policy-based management and analytics-driven applications.

Figure 1: The NMS is dead, long live the domain controller

In its new role, the NMS decouples the OSS from underlying implementations, and also programs and automates the underlying network and its virtual network functions (VNF). Apart from the functionality provided by classic NMS, the new architecture must also deal with functionality that was traditionally embedded in-the-box. Most management functions embedded in network elements today can be
virtualized and run as a VNF in the cloud in line with the ETSI-NFV reference architecture. The virtualization of management functions takes the load off network elements, allowing them to transcend CPU/RAM node limitations, elastically scale in the data center and deliver an always on-line experience. Carrier-grade network functions, built and optimized for the cloud, deliver service agility, performance and scale. However, it should be noted that the fixed access domain has a large installed base of non-virtualized network elements; the NMS has to make sure it provides unified management of both traditional and SDN/NFV network functions, for network operators and for OSS integrators. This hybrid network management is made possible by building the right levels of abstraction for the underlying SNMP/MIB network.

**Easy to integrate**

The virtualized management functions fit in a modular software architecture with stateless and state-efficient designs, for both centralized and distributed deployments. Management functions are no longer monolithic blocks but consist of modular, sharable, independently installable and scalable microservices. Web scale technologies like Ansible and Docker Compose are used to tie these independent microservices together. In line with Figure 1, an SDN orchestrator manages the lifecycle and VNF managers can scale-in/scale-out these services.

In a 2016 survey by IHS Markit, agility of service development and deployment was rated as one of the top reasons service providers will adopt SDN/NFV in their networks. DevOps tools are used to automate the steps from programming to testing to delivery; these must be extended into the service provider space to automate acceptance testing and field deployment. The sandboxes, which are the self-contained infrastructure elements configured to recreate a real deployment environment, are used in conjunction with DevOps tools. In this way, the time to develop and deploy services is reduced from several months to just a few days.

Continuous integration and delivery practices support agile transformation. Some service providers, as part of their SDN migration plan, need their classic NMS to manage the SDN/NFV network. This is made possible by slicing a piece of the SDN/NFV network manager and integrating it under the classic NMS. The modularity of the SDN/NFV network management is very useful in such a deployment.

**Open ecosystem**

The new architecture consists of a purpose-built software suite leveraging open-source, supporting a large array of platforms and protocols that allow easy integration with 3rd party systems, networks and partners. As today’s proprietary data models largely contribute to a level of OEM stickiness, next-generation networks need to be based on industry standardized data models as defined by the BBF. Their adoption will enable multivendor support in the management functions and support the development of network extensions while avoiding vendor lock-in.

The concept of programmable networks is realized through centralized data lakes with powerful northbound interfaces for data manipulation and southbound interface to keep the data in sync with the underlying network. Data lakes have different databases for configuration, fault and performance data.

---

1 Carrier SDN Strategies Service Provider Survey, IHS Markit, 2016
because there are fundamental differences in the operations performed on the data, the periodicity of synchronization, the granularity, and the historical duration/size of data being stored. For example, configuration is managed through NETCONF/YANG where the underlying data is stored in a SQL database, while the performance data is stored in a time-series database and has model-driven interfaces for defining the data to be collected, derived metrics to be calculated, and the threshold crossing alarms (TCA) to be raised. The open ecosystem with data and config in the cloud opens up opportunities for automation to focus on customer operations cutting across FCAPS silos.

The role of NETCONF/YANG

The telecommunications industry is adopting open interfaces and open models such as the NETCONF protocol and YANG modeling language. The industry-wide adoption and standardization of NETCONF/YANG will enable easy integration with existing and new architectures. This is important when applying SDN to the access network to make it more flexible and programmable. NETCONF/YANG provides several benefits which cannot be natively delivered in traditional SNMP networks:

- NETCONF/YANG is cloud-friendly. Devices connect to their manager with call home and strong security models for authentication, integrity, and confidentiality are supported by design.
- NETCONF/YANG is easy to program and automate. No micro operations nor hand-coded rollback are needed as ACID (Atomicity-Consistency-Isolation-Durability) properties for the transactions are guaranteed. Interactions with the network are enhanced with databases that can be easily manipulated by humans and machines. The full transparency - nothing under the hood - allows easy integration with other components.
- NETCONF/YANG fits the IT environment. A rich ecosystem of IT tools becomes accessible for interacting with the network. The network is no longer the exclusive realm of experts.

Conclusion

In Intelligent Access, the management of the SDN/NFV network virtualizes management functions that were embedded in network elements. This offers multivendor and cross-domain service management capabilities that can be deployed in the cloud in a highly scalable way. Networks become programable by creating data lakes that offer powerful northbound interfaces to manipulate data and southbound interfaces that keep the data lakes and network element data in sync. A new breed of applications is building policy-based management and analytics-driven use cases, leveraging a rich ecosystem of workflows and tools to visualize, automate, optimize and enhance the network.

Different stakeholders from IT, planning, installation and troubleshooting teams will benefit from this evolution. A good example of policy-based management is TWDM on-the-fly wavelength mobility for equipment protection, bandwidth rebalancing and power management. Other examples include automation of troubleshooting workflows, simplification of field deployments and turn-up of G.fast nodes, mass software upgrades, and campaign managers which can help service providers move a sub-set of subscribers to a trial service plan as part of a marketing campaign.

New IT and web scale tools are being leveraged to build management systems for SDN/NFV networks which increase the modularity of the software and increase operators’ service agility. They also offer unified management for legacy networks alongside SDN/NFV networks.
Acronyms

ACID  Atomicity-Consistency-Isolation-Durability
BBF  Broadband Forum
CLI  Command line interface
CORBA  Common object request broker architecture
ETSI  European Telecommunications Standards Institute
FCAPS  Fault, Configuration, Accounting, Performance, Security
FTP  File transfer protocol
GUI  Graphical user interface
IT  Information technology
LAN  Local area network
MIB  Management information base
NBI  Northbound interface
NFV  Network function virtualization
NMS  Network management system
OEM  Original equipment manufacturer
OSS  Operations support system
SDN  Software-defined networking
SNMP  Simple network management protocol
SOAP  Simple object access protocol
SQL  Structured Query Language
TCA  Threshold crossing alarms
TL1  Transaction language 1
TWDM  Time wavelength division multiplexing
VNF  Virtual network functions
WAN  Wide area network

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1709015667EN (October)