

Three Key Issues with Integrating SDN/NFV and How Service Providers Can Solve Them

By: Dinesh Dhanasekharan

2017 is becoming the year of software-defined networking (SDN) and network function virtualization (NFV). Boosted by early adoption from carriers such as AT&T, communications service providers (CSPs) are beginning to ramp investments in the NFV and SDN ecosystems to the tune of [\\$158 billion by 2021](#), according to research firm Technology Business Research. The move to a more virtualized, cloud-based network architecture is seen by some as the first layer of the Digital Transformation, where a more open, flexible architecture includes tools such as data analytics and automation.



The market has seen a series of ups and downs—no surprise given the expansive work at hand to virtualize networks built up over the course of a century—but now it seems to be moving more consistently. AT&T threw down the gauntlet to the rest of the industry with its announcement in February that it plans to virtualize 55 percent of its network to software by the end of 2017. The service provider noted at the time that it had beaten its internal goal for 2016, converting 34 percent of its network to SDN. The company's 2020 goal of 75 percent suddenly seems achievable. AT&T also revealed its plans to allocate a significant portion of its capex budget to invest in integrated wireless and wireline solutions for its business customers, enhancing the reach of its software-driven solutions like SD-WAN.

AT&T is not the only provider making progress on virtualizing their networks. Internationally, Telefónica and China Mobile have also made significant progress on their SDN/NFV initiatives, taking different courses while being driven by the same need to drive down costs and increase efficiencies. And according to a December 2016 virtualization index from research firm Heavy Reading, which “provides all CSPs with a compelling reality check for measuring their own progress in three critical areas: planning, deployment and spending,” 45 percent of providers surveyed plan to have at least 20 percent of their network virtualization efforts in live production by the end of 2017, and another 27 percent plan to have 50 percent or more in live production by year's end.

The benefits of moving to a virtualized network infrastructure that providers like AT&T are finding so appealing are well documented, but worth repeating. The three main motivators include:

Reducing expenditures:

- CAPEX savings through commodity network infrastructure
- OPEX savings due to increased automation

Improving operational efficiency and performance:

- Centralized control improves traffic management and enables rapid failover in managing failures
- Centralized traffic engineering provides a global view of the supply and demand of network resources
- Implementation elasticity allows dynamic scaling of network and services

Accelerating time-to-market for new services

- Features and capabilities can be added through software
- Additional capacity can be added through configuration

Yet despite the early advances we've seen from service providers around the world, based on the timelines and projections above, providers are going to be living with hybrid networks—a combination of legacy networks and new virtualized networks—for quite some time, perhaps even decades. This brings a bevy of new challenges, especially on the OSS side of the house. The introduction of a software-based model into a predominately hardware-based network means new ways of managing those domains and the assets within them.

Just as the networks won't be turned from physical to virtual with the flick of a switch, OSS transition will also happen gradually which will, at times, be painful for providers. We've pinpointed three key areas that providers will continue to struggle with as networks become increasingly virtualized:

1) Cross-domain Orchestration. Orchestration is not new, but the new hybrid nature of today's emerging service provider networks is making it more complicated. Typically, orchestrators focus on their own contained domain—such as IP VPNs or content delivery networks (CDNs)—and that single-domain focus means they work incredibly well.

But thinking about the wealth of legacy and new service domains that providers support makes it easy to understand that orchestrating across domains is incredibly complex and, in fact, the problem has not been resolved—there is no master orchestrator of orchestrators capability built into a single piece of software with a network-wide, end-to-end view.

Given how quickly innovation is occurring, never say never, but how the industry will achieve orchestration with domains across the entire network is not yet understood. Bring in the added complexity of multi-vendor networks, each with their own orchestration systems that need to communicate with each other, and the mystery of how this will be achieved deepens.

One answer might have come from the MEF, which is developing [LSO \(Lifecycle Services Orchestration\) specifications](#) with open APIs to automate the end-to-end lifecycle for services orchestrated across multiple provider networks, as well as multiple technology domains within a provider network. According to MEF, "LSO enables service providers to transition from a silo-structured BSS/OSS approach towards flexible end-to-end orchestration within SDN/NFV networks. Standardized LSO APIs are critical for enabling agile, assured and orchestrated services over automated, virtualized, and interconnected networks worldwide."

2) Integration with B/OSS and existing infrastructure. SDN and NFV will not reach their potential value until OSS and BSS systems are aligned with the new technologies. According to a report from the Open Networking Foundation, with SDN and NFV, "a service can be turned up or torn down quickly, but until provisioning, configuration, billing and fault management are automated, dynamic, and intelligent, SDN and NFV cannot be fully leveraged."

Analyst firm Analysys Mason called for the need for an [end-to-end functional architecture](#) that pulls together NFV management and orchestration (MANO) and OSS. According to Analysys Mason, "the success of CSPs in the digital economy depends on them deploying a network architecture that can dynamically and holistically manage physical and virtual resources to support service innovation at scale." This calls for a virtual next-generation network OSS (vNGN-OSS) that has several key requirements for managing multi-vendor hybrid network environments:

- A single Service Orchestration Manager (SOM) product to support multi-domain service orchestration
- Service orchestration supports fulfillment and assurance
- Resource Order Management evolves to perform network orchestration
- Centralized policy management and enforcement
- Dynamic inventory management
 - Real-time visibility into the network and IT
 - Comprehensive model that maps customers to products, services, virtual resources (VNFs, VIMs) and physical resources (CPU, storage, network)
- Ease of configuration
 - Common set of configuration tools and IT products
 - Adoption of a Master Enterprise Catalog - B/OSS, Network, IT
- High level of automation

- Use of Big Data Analytics to:
 - Improve customer experience
 - Improve network utilization
 - Increase profitability

The industry is making progress on pulling these elements together, but it's a long evolution of processes, not a revolution.

3) Lack of mature standards. Standards, or a lack thereof, have been the downfall of many vendors and products across the history of communications networks. In the case of SDN/NFV, service providers who wanted to move full-steam ahead with their initiatives, such as AT&T and Telefónica, were forced to forge their own path, while China Mobile is relying on more of an open-source approach to deployment.

Frequently, service providers are forcing the need for standards based on their voracious appetite for the benefits SDN and NFV deployments can bring across their business: reduced costs, greater efficiency and rapid innovation. At the same time, however, there is great need to future-proof their deployment roadmaps, and only common standards that are open and interoperable can accomplish that.



Even though the industry has been talking about SDN for years, no clear standards have emerged to guide the integration process. However, the industry is moving closer, with groups like the Open Networking Foundation (ONF), ETSI, MEF, TMForum, and others each have done significant work to push standards closer to completion, which will be a very welcome sight for providers looking to advance their initiatives more efficiently.

The market is lining up to solve these issues, and different groups of players are taking on key roles:

- **Operators** are looking to coordinate between existing OSS systems and new MANO systems for the virtualized infrastructure;
- **Software vendors** are trying to position themselves as an overarching orchestration layer sitting on top of the MANO and traditional OSS;
- **Hardware vendors** are developing MANO solutions and are trying to move up the stack; and
- **Consultants** are developing BSS/OSS transformation approaches that support the incremental adoption of SDN.

NFV and SDN are being seen as the first layer as service providers undergo digital transformation, where a more open, flexible architecture includes tools and capabilities such as data analytics and automation. James Crawshaw, senior analyst at analyst firm Heavy Reading, sums up the [role of OSS in network transformation](#) quite nicely: "Widespread adoption of NFV will only happen when robust management, orchestration, and OSS architectures are defined and implemented. Operators that seek to implement NFV without preparing their OSS to support it are unlikely to be successful in capturing the new revenue-generating and cost-saving opportunities that NFV promises. OSS

should not be an afterthought; it will continue to be central to the operational efficiency and agility of the service provider.”