Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 10, Issue 9

NFV Evolution: Defining the Missing Link

By Jesse Cryderman

Virtualization—replacing single instance, purpose-built hardware systems with distributed software solutions that can run on commercial off-the-shelf (COTS) servers—has impacted nearly every element of the IT landscape. It began with basic storage and backup services, then moved to software, then computing power, and then complete platforms and infrastructure. In telecom, even operational support systems (OSS) and business support systems (BSS) can be deployed in the cloud, offering unprecedented scalability and agility.

At the dawn of telecommunications, an operator seated at a switchboard was responsible for manually connecting signals from one circuit to another. These physical operations were replaced by mechanical switches and routers that evolved over time to handle thousands of very high bandwidth signals simultaneously, at extremely high speeds. This is the state of the network today, and it's about to change.

With the advent of software defined networking (SDN) and its sibling, network functions virtualization (NFV), the fabric of the network itself is being virtualized. This development represents a monumental change for communications service providers (CSPs). To date, they have invested heavily in the network equipment, human resources, and support contracts that keep their networks ticking; now the limitations of the status quo are hindering their evolution.

Driven by a desire for accelerated service velocity and reduced network operational expense (OPEX), global CSPs are actively pursuing NFV and SDN strategies. Virtualizing network functions with NFV represents a paradigm shift; like any paradigm shift, it offers immense advantages over legacy networking, but not without challenges.

Network functions go virtual

The European Telecommunications Standards Institute (ETSI) created the NFV industry specification workgroup and has taken the helm in defining a framework for NFV. By virtualizing functions that once required physical hardware and manual programming configuration, extreme efficiency increases and cost reductions can be realized. Using commoditized computer hardware, not specialized, vendor-controlled equipment, network functions such as firewalls, DPI appliances, tunneling gateways, and more can be programmed automatically and instantiated in numerous locations. A telecom server could host a router one day and a session border controller the next, depending on demand, latency, and other network conditions. This would require new equipment, a truck roll, and a network engineer in the past. Figure 1 above illustrates the NFV network architecture compared to legacy architecture.

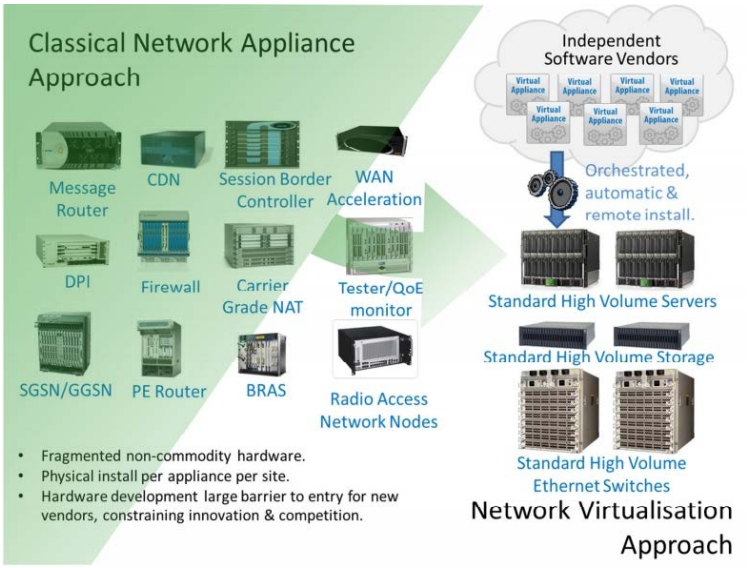


Figure 1 - Network Virtualization Approach *Source: ETSI, 2012*

The advantages outlined by ETSI are significant, compelling, and lead to the reasons why CSPs, themselves, are driving the technology faster than vendors (a unique situation in telecom). These advantages include:

- Reduced operator CAPEX and OPEX through reduced equipment costs and reduced power consumption
- Reduced time-to-market to deploy new network services
- Improved return on investment from new services
- Greater flexibility to scale up, scale down or evolve services
- Openness to the virtual appliance market and pure software entrants
- Opportunities to trial and deploy new innovative services at lower risk

Of these benefits, accelerating new service delivery is top of mind as the primary driver among network operators. The pressure placed on CSPs from over the top (OTT) providers like Google Voice, Skype, and WhatsApp are substantial. Never in the history of telecom have the business' core services been so threatened. CSPs simply can't afford to wait 12 months, a typical development cycle today, to release competing offerings.

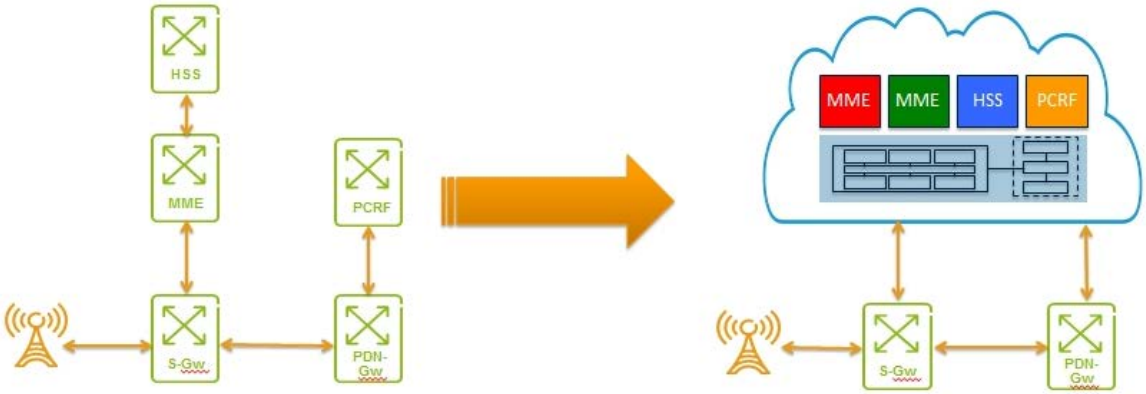


Figure 2 - Virtualizing Mobile Managment Entities (MMEs)
Source: Tail-f Systems

An Infonetics Research survey in July, 2013, found that operators are in select domains, but eager to move faster. "For the most part, carriers are starting small with their SDN and NFV deployments, focusing on only parts of their network, what we call 'contained domains,' to ensure they can get the technology to work as intended," wrote Michael Howard, co-founder and principal analyst for carrier networks at Infonetics Research.

He added, "But momentum for more widespread use of SDN and NFV is strong, as evidenced by the vast majority of operators participating in our study who plan to deploy the technologies in key parts of their networks, from the core to aggregation to customer access. Even so, we believe it'll be many years before we see bigger parts or a whole network controlled by SDNs."

NFV in the Evolved Packet Core (EPC)

The benefits of NFV as it applies to mobile packet core networks will most likely be realized in the control plane, especially within EPC deployments. Components such as Mobile Management Entity (MME), Policy and Charging Rules Function (PCRF) and Home Subscriber Server (HSS) rely more on compute resources than packet processing resources. This allows a natural progression to virtualized instances of these functions using NFV.

Typically, MME's are deployed in a clustered and load-balanced configuration to handle call setups, handovers, and radio updates. Traditional MME's are based on large, expensive, and usually custom hardware. Deploying MME's require extensive planning and engineering. As you can see in figure 2 below, with a fully virtualized MME, a mobile operator leveraging NFV can dynamically deploy virtualized MME's during times when loads are high and can decommission MME instances when loads are low. The same concepts can be applied to PCRF and HSS solutions.

NFV Challenges

While ETSI's framework offers a nice overview of NFV, there are many pieces left out of the equation, as well as challenges related to upending the status quo. To leverage the potential benefits, there are a number of technical deficits which need to be addressed. A white paper published in October, 2012, by a group of 13 global services providers outlined the following challenges:

- Virtualized network appliances must be portable between different hardware vendors, and with different hypervisors.
- Virtualized network elements must coexist with legacy hardware while enabling an efficient migration path to fully virtualized network platforms.
- Network Functions Virtualization will only scale if all of the functions can be automated.
- Network operators need to be able to mix and match hardware from different vendors, hypervisors from different vendors and virtual appliances from different vendors without incurring significant integration costs and avoiding lock-in.

Operators must be able to manage and orchestrate many virtual network appliances while ensuring security from attack and misconfiguration.

As you can see, although ETSI has defined a framework for NFV, there are numerous elements and challenges that arise in real-world implementation that are beyond the scope of ETSI's architecture. These challenges are particularly painful in multi-vendor environments, such as mobile networks, and the reason the technology is not coming online as fast as operators demand.

In the ETSI architecture, the interface between element management systems (EMSs) and virtualized network functions (VNFs) is classified as out of scope by ETSI, with the expectation that NFV vendors will supply this interface. ETSI's framework does not address the management and orchestration of the actual VNFs being deployed on that infrastructure (beyond starting and stopping VNFs). The various VNFs are controlled by closed and static vendor-specific EMSs that do not support automation. The following problems arise:

1. EMS sprawl: no single console to the VNFs, learning curve for various EMS systems, no automation, OPEX/CAPEX cost of EMS
2. Amplification of existing bottlenecks: assuming closed EMS systems in place, manual work and OSS integration efforts will increase since the requirements for dynamic services are increasing with NFV.
3. Orchestration sprawl (on the north side): automation requirements ripples to the orchestrator on the top which will be a very complex integration task.

Ultimately this short-circuits the promises of NFV. Instead of increased agility, faster time to market, reduced complexity, and cost reduction, service providers are bogged down by more complexity and costly, time-consuming data transformation projects—headaches they know all too well. The fundamental problem, which at least 13 service providers recognized in 2012, is that for NFV to truly deliver, orchestration of all functions must be automated and, in current implementations, this is not the case.

What is required is a network service orchestration system providing a service-oriented northbound API based on data models and transactions. This removes the need for EMSs and it provides automated real-time service provisioning.

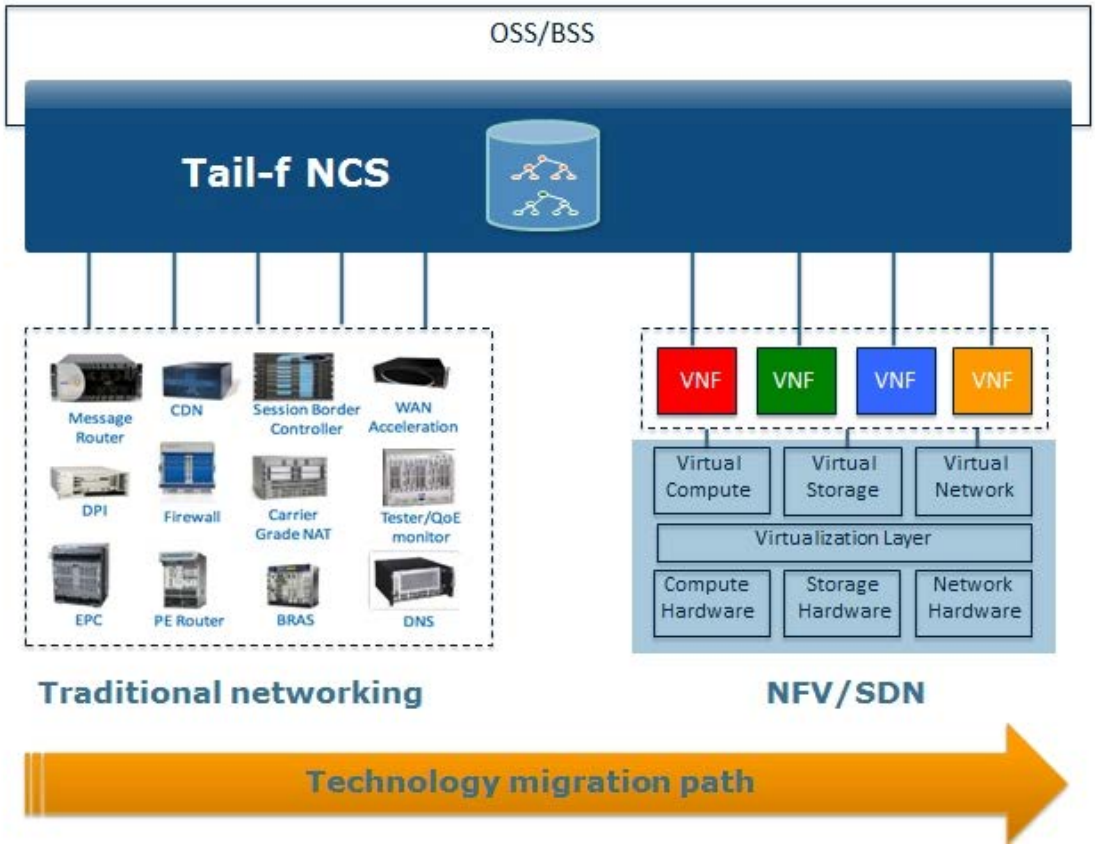
Service orchestration

Network Control System (NCS) from Tail-f Systems is one of the products available today that addresses these issues. NCS is a software solution for provisioning multi-vendor services and configuring network devices in a virtualized network environment. As you can see in figure 3 on the following page, NCS functions as a service orchestration system between network functions and the BSS.

Currently, vendors take different approaches to service orchestration. Single-vendor solutions typically focus on making their existing physical solutions work with NFV. NCS accommodates multi-vendor service provisioning and offers a clear path from existing networks. This is the key to accelerating new service delivery, as it accommodates the way networks and service provider organizations exist today, in addition to what they may look like in the future.

Deutsche Telekom, an NFV pioneer, has successfully implemented NCS in its TeraStream project. "We believe carriers can no longer afford to hard-code services into the OSS if they want to get to market quickly with new services," said Axel Clauberg, Vice President, Aggregation, Transport, IP and Fixed Access, Deutsche Telekom AG. "The Tail-f NCS solution, with both services and the network modeled in a

Figure 3 Source: Tail-f Systems



standardized high-level language, shortens time to market, increases vendor independence and dramatically improves the cost structure. This SDN solution is a key component in TeraStream's real-time OSS," he adds.

(*Pipeline* hosted a webinar with Deutsche Telekom and Tail-f in 2013. which is available on demand.)

Hakan Millroth, CTO of Tail-f Systems, sees the TeraStream use case as fundamental to the adoption of NFV. "Tail-f has been driving standardization of network service programmability for a long time to reduce key pain points such as vendor dependence, lack of service innovation and high operating costs. The adoption of these standards by TeraStream and its network equipment providers will fundamentally change the networking industry."

Delivering on the promise of NFV

ETSI specifications do not outline the need for a single orchestration layer. In order to rapidly deliver new services in a virtual network environment and deliver on the promises of NFV, a network service orchestration layer is needed that enables services to be programmed and automatically translated into configuration changes on network devices in a way that supports the rapidly emerging, software-centric processes. This layer must accommodate multiple vendors as well as legacy hardware, while providing a migration path to total SDN/NFV deployment. One of the solutions available to CSPs, Tail-f's NCS, solves both the technical and business challenges service providers face as they seek to swiftly launch new services in their constantly evolving, multi-vendor network environments.