What will it take to become NFV-ready?

The communications industry is undergoing an unprecedented level of change. These changes have a profound impact on the operational aspects of virtual networks to the extent that existing processes and operational support systems (OSS) must adapt and evolve in order to become NFV-ready, writes Justin Paul

Four key challenges must be overcome to successfully operationalise an NFV-ready network: hybrid networks, real-time operations, service agility and a multi-vendor environment. Having delivered a number of advanced proofs of concepts with some of our Tier 1 customers, Amdocs has learned a lot about how to surmount these challenges and realize the benefits of NFV.

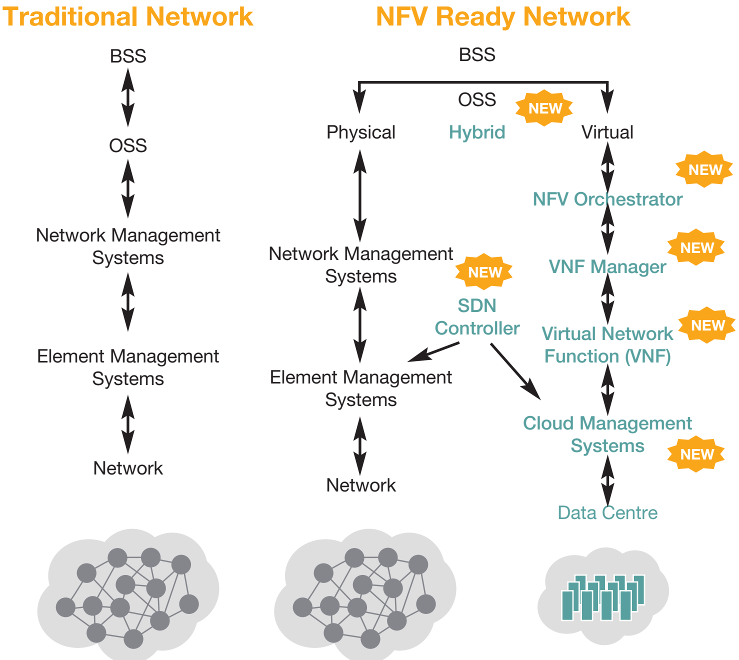


Figure 1: What's new for the NFV-ready network

IN ASSOCIATION WITH AMDOCS

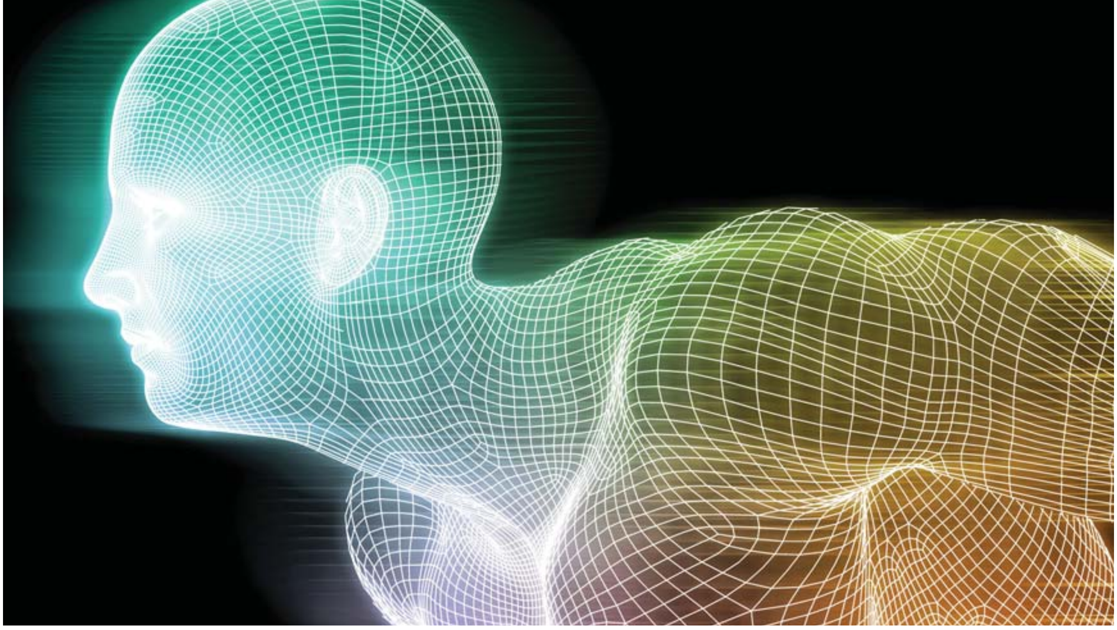
The hybrid reality

According to Heavy Reading's NFV operator survey, published in September 2015, levels of NFV readiness are high, with 29% of communications service provider (CSP) respondents already deploying the first wave of virtual network functions (VNFs) in cloud infrastructure.

It's clear that, with the exception of greenfield service providers, all CSPs introducing NFV will need to support existing networks alongside virtual networks for the foreseeable future. CSPs are still investing billions of dollars in technologies such as LTE, LTE-Advanced, FTTx, Carrier Ethernet, and even 5G; these next generation technologies will not disappear overnight. The challenge of combining physical network functions (PNFs) and virtual network functions (VNFs) will be with us for the next decade at least. And the challenge of hybrid goes beyond the new complex requirement of the VNFs and NFV orchestration (NFVO) to a requirement to orchestrate services that are provisioned across both virtual and physical domains. One scenario at the top of many service providers' agendas is the complex orchestration of an enterprise Virtual Private Network (VPN) across different enterprise sites with both physical and virtual customer premises equipment (vCPE).

Evolving to real-time operations

Virtualised networks are highly dynamic and require accurate real-time visibility of network status for efficient operations, something that existing resource management – inventory – systems do not provide. Operating an NFV-ready network requires a near



real-time and consolidated view of capacity, serviceability and feasibility, as well as just-in-time resource allocation of all network resources, physical and virtual. Inventory capability must evolve from an offline repository of relatively static resources and capacity to include a near real-time active inventory that constantly interacts with the network. This real-time awareness of the exact status of network resources will enable service providers to achieve the elasticity and scalability that NFV promises – moving from static, over-provisioned, pre-allocation of network resources to dynamic resources utilisation according to usage.

Service agility becomes a reality

There are two key aspects to service agility. The first is the question of time to market. Existing slow, cumbersome and resource-intensive manual processes must be transformed into a highly automated service development lifecycle in order to accelerate the time to onboard VNFs and to design, test and launch new NFV-based and hybrid services. Cutting the time and cost to innovate and to adapt existing services from a typical nine months or more to just weeks breaks these time and cost barriers, and empowers service providers to emulate OTT-like levels of innovation.

The second is the question of time to revenue. In place of cascaded fulfilment and assurance processes, CSPs investing in NFV and SDN need an automated, end-to-end NFV orchestration solution that delivers continuous, zero-touch and closed-loop fulfilment in seconds or minutes instead of days or weeks.

Having completed a number of advanced proofs of concepts with Tier 1 customers, Amdocs has demonstrated the potential to develop, test and launch a multi-vendor service in weeks with service development lifecycle automation and to fulfil an order in minutes or even seconds through automated end-to-end NFV orchestration.

The need for a multi-vendor approach

Amdocs is seeing an increasing interest in end-to-end NFV services based on diverse VNFs. It is widely recognised that enterprise services are likely to be the first commercial NFV services launched, yet the network equipment providers (NEPs), who have dominated the earliest proofs of concept trials (PoCs) which looked at virtualising standard physical network functions, often lack the specific VNFs required to launch enterprise services. Looking in more detail at enterprise security services, we see that there are a number of virtual firewall (vFW) providers, and that each vFW has specific capabilities and parameters that make it ideal for a specific market or segment. The firewall requirements for a major financial institution, for example, are very particular. The beauty of NFV is that it allows best-in-breed services to be developed that match the reliability, scalability, resilience and price requirements of diverse customers. This means that the virtual networks of the future must support multi-vendor VNFs, and that there will be a focus on the ability to design, test and pre-integrate end-to-end services from multiple vendors.

In Amdocs' recent PoCs, we have integrated with firewalls from Juniper, Fortinet, and Checkpoint, and the Amdocs Network Cloud Ecosystem, our NFV partner program, contains at least five different vFW vendors. Tied into the multi-vendor requirement is the need to recognise that there are many proposed approaches to defining VNFs including TOSCA and Yang. These standards are still evolving so it is important to take a flexible approach – openness is key to NFV success.

What's on the horizon for virtualisation?

The large number of NFV PoCs undertaken by Amdocs in 2015 has contributed significantly to our understanding of the NFV domain, and how to help our customers implement and monetise NFV.

Virtualisation can deliver significant business benefits in terms of profitability and flexibility, confirming service agility as the primary driver for NFV. The PoCs have also served to highlight some of the challenges faced by CSPs in operationalising and monetising NFV as well confirming the value of Amdocs' solutions to these challenges. Implementing NFV is transformational, but an evolutionary approach to operational processes and systems will help CSPs to access the benefits of this technology. In 2016, Amdocs expects to see a number of our PoC customers accelerate their adoption of NFV with more, and increasingly complex, commercial services. Amdocs will be with them for the journey.

The author, **Justin Paul,** is the head of OSS marketing at Amdocs

www.amdocs.com