OPEN NETWORKING FOUNDATION

OpenFlow-enabled SDN and Network Functions Virtualization

ONF Solution Brief
February 17, 2014

Table of Contents

2 Executive Summary
3 SDN Overview
4 Introduction to NFV
5 NFV Network Challenges
6 NFV/SDN Example Use Cases
8 NFV Networking Requirements
9 OpenFlow-enabled SDN: A Flexible NFV Networking Solution
11 Summary and Conclusions
11 Contributors
12 References

Executive Summary

Network Functions Virtualization (NFV) offers the potential for both enhancing service delivery and reducing overall costs. By enabling NFV with OpenFlow-enabled Software-Defined Networking (SDN), network operators can realize even greater benefits from this promising new use of cloud technology.

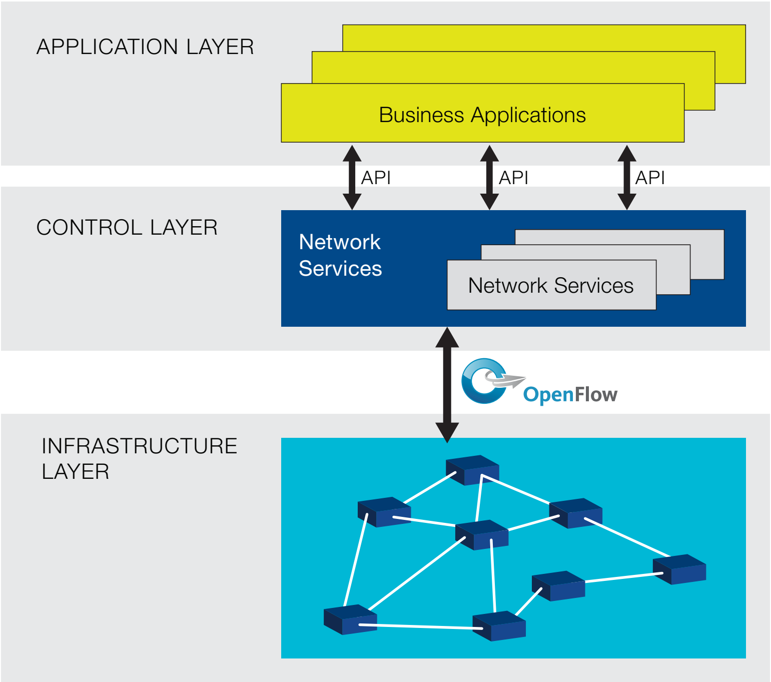
OpenFlow-based SDN can accelerate NFV deployment by offering a scalable, elastic, and on-demand architecture well suited to the dynamic NFV communications requirements for both virtual and physical networking infrastructures.

This solution brief showcases how operators can combine NFV and SDN to achieve the common goals of both technologies. It discusses the new IP connectivity challenges imposed by NFV, and presents use cases that exemplifies how OpenFlow-enabled SDN can meet the need for automated, open, and programmable network connectivity to support NFV.

SDN Overview

Software Defined Networking is a new architecture that has been designed to enable more agile and cost-effective networks. The Open Networking Foundation (ONF) is taking the lead in SDN standardization, and has defined an SDN architecture model as depicted in Figure 1.

FIGURE 1
ONF/SDN architecture



The ONF/SDN architecture consists of three distinct layers that are accessible through open APIs:

- **The Application Layer** consists of the end-user business applications that consume the SDN communications services. The boundary between the Application Layer and the Control Layer is traversed by the northbound API.
- **The Control Layer** provides the logically centralized control functionality that supervises the network forwarding behavior through an open interface.
- **The Infrastructure Layer** consists of the network elements (NE) and devices that provide packet switching and forwarding.

According to this model, an SDN architecture is characterized by three key attributes:

- **Logically centralized intelligence.** In the ONF SDN architecture, network control is distributed from forwarding using a standardized southbound interface: OpenFlow. By centralizing network intelligence, decision-making is facilitated based on a global (or domain) view of the network, as opposed to today's networks, which are built on an autonomous system view where nodes are unaware of the overall state of the network.

- **Programmability.** SDN networks are inherently controlled by software functionality, which may be provided by vendors or the network operators themselves. Such programmability enables network configuration to be automated, influenced by rapid adoption of the cloud. By providing open APIs for applications to interact with the network, SDN networks can achieve unprecedented innovation and differentiation.
- **Abstraction.** In an SDN network, the business applications that consume SDN services are abstracted from the underlying network technologies. Network devices are also abstracted from the SDN Control Layer to ensure portability and future-proofing of investments in network services, the network software resident in the Control Layer.

Introduction to NFV

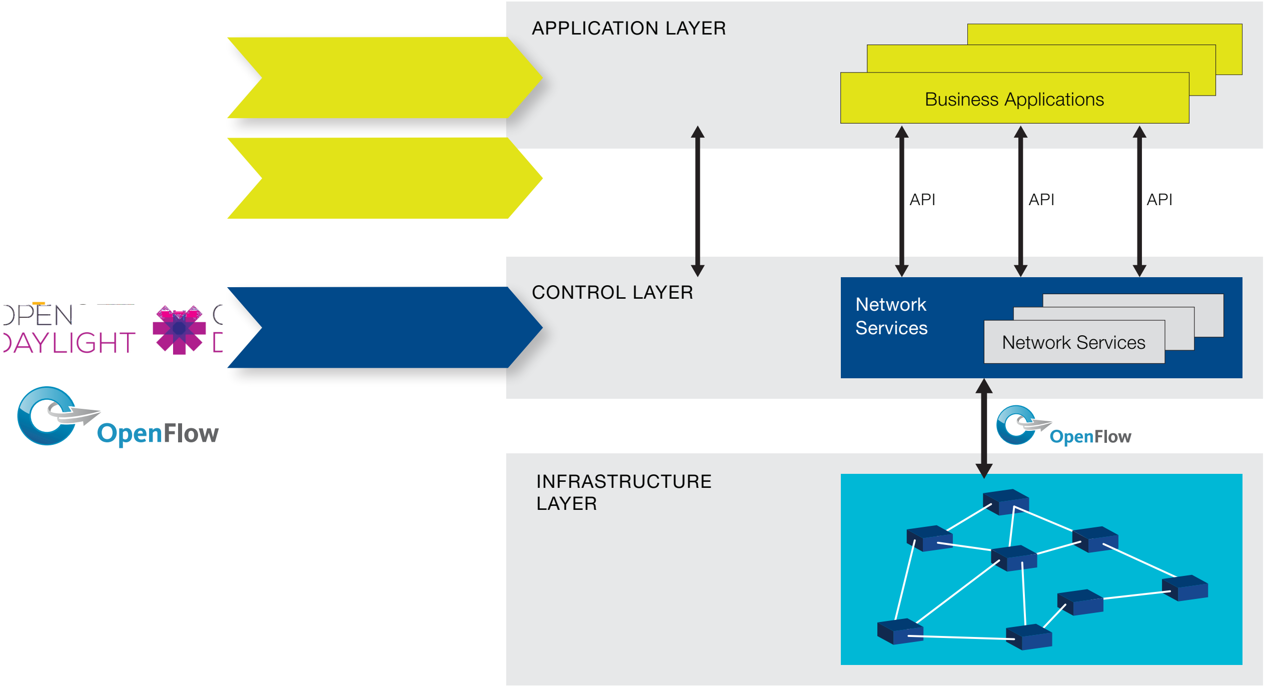
In late 2012, over twenty of the world's largest telecommunications service providers formed an Industry Specification Group (ISG) within the European Telecommunications Standards Institute (ETSI) to define Network Functions Virtualization (NFV)[1]. Since then, the NFV initiative has generated a great deal of interest, involving more than 28 network operators and over 150 technology providers from across the telecommunications industry.[2]

The NFV initiative is intended to address the operational challenges and high costs of managing the closed and proprietary appliances presently deployed throughout telecom networks. By virtualizing and consolidating network functions traditionally implemented in dedicated hardware, using cloud technologies, network operators expect to achieve greater agility and accelerate new service deployments while driving down both operational (OpEx) and capital costs (CapEx).

NFV AND SDN

NFV aims to reduce equipment costs and decrease time to market while attaining scalability, elasticity, and a strong ecosystem. The Open Networking Foundation is pursuing similar goals through OpenFlow-enabled SDN. Much like NFV, SDN accelerates innovation by breaking the bond between proprietary hardware and control/application software. Both architectures are optimized for the dynamic cloud environment at carrier scale.

Both NFV and SDN seek to leverage automation and virtualization to achieve greater agility while reducing both OpEx and CapEx. Whereas NFV is intended to optimize


APPLICATION LAYER
Business Applications
API
API
API
CONTROL LAYER
Network
Services
Network Services
OpenFlow
OpenFlow
INFRASTRUCTURE
LAYER

- **Manually intensive management.** Provisioning and configuration for network appliances are complex, manually intensive, and time-consuming tasks. Provisioning for virtual appliances (referred to in the NFV environment as virtualized network functions [VNFs]) must be automated to address the dynamic NFV environment. Such automation will reduce provisioning and configuration times along with manually induced configuration errors.
- **Rapid growth of IP end points.** Because of the virtualization of network appliances, the number of network endpoints in the NFV environment will increase far faster than for existing networks, potentially resulting in millions of endpoints for residential and mobile applications. This will increase the stress on existing network mechanisms such as Layer 2 VLANs, or necessitate additional complexity for bi-sectional bandwidth scaling such as SPB and TRILL.
- **Network endpoint mobility.** Physical appliances are typically provisioned once in their lifetime and stay fixed in the same network location. VNFs can be migrated readily to disparate physical servers, which may appear in different sub-networks or even physical locations, use different tunneling addresses, or even have different protocols that dictate how they will be reached. NFV breaks the traditional linkage between IP location and identity.
- **Elasticity.** In the NFV environment, VNFs are created, adjusted, and destroyed in real time on demand. Networks must be capable of being reconfigured rapidly to achieve the elasticity needed to optimize the pooled resources in the dynamic NFV environment.
- **Multi-tenancy.** Many of the NFV use cases are based on cloud-like “as a service” offerings whose viability hinges upon efficient multi-tenancy. Granular policy management is required that can be assigned to services and flow, but decoupled from the physical infrastructure.

NFV/SDN Example Use Cases

To illustrate the challenges that operators face in migrating to NFV over today’s static inflexible network architectures, we present a pair of use cases that are defined in the ETSI NFV ISG Use Cases document:[3]

- Virtual network function forwarding graph (VNF-FG) to enable service chaining
- NFV infrastructure as a service (NFVIaaS) to virtualize the global network

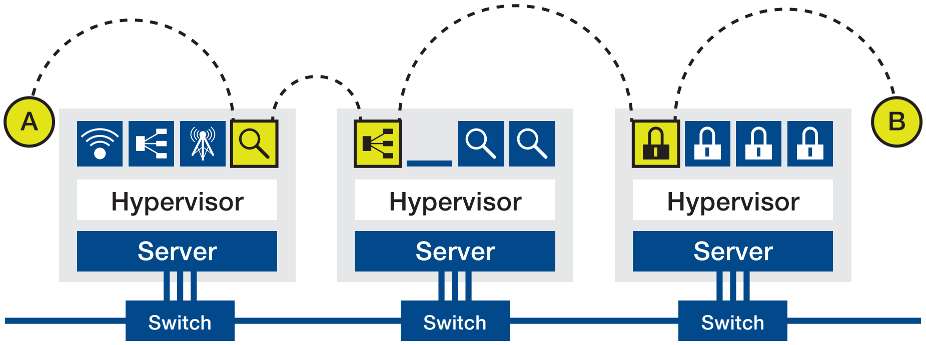
Both of these use cases will benefit from the highly flexible and dynamic behavior of an OpenFlow-based SDN network, especially at scale.

VIRTUAL NETWORK FUNCTION FORWARDING GRAPH

The ETSI NFV ISG published a document that provides a representative set of NFV use cases that drive the NFV architecture and requirements. One NFV use case describes the virtual network function forwarding graph, which allows virtual appliances to be chained together in a flexible manner.

In this use case, a user, an application, or content flow must pass through several virtual appliances before being delivered. This is commonly referred to as Service Chaining. Figure 3 illustrates the concept where a flow originating from endpoint A passes through a network monitoring VNF, a load balancing VNF, and eventually a firewall VNF before arriving at destination point B.

FIGURE 3
Virtual network function forwarding graph (VNF FG)



Today's hardware-based approach makes it extremely complex and time-consuming to implement service chaining, and expensive to scale and manage. Appliances must be physically installed and cabled, then assigned to physical domain qualifiers such as VLANs, sub-networks, etc., which typically limit their connectivity. Configuration must be manual and meticulous to implement the service chain.

In an NFV environment, a VNF FG can be created, updated, scaled, and removed much more quickly and efficiently. For instance, to add a new VNF to one or more service chains, a virtual machine can be instantiated and the forwarding graph updated. Scalability can be achieved similarly.

Among the challenges to effectively implement and deploy a VNF FG is ensuring that sufficient performance, capacity, and resiliency are achieved in an open, multi-vendor environment. Also, provisioning and forwarding plane programmability must be automated across both virtual and physical boundaries.

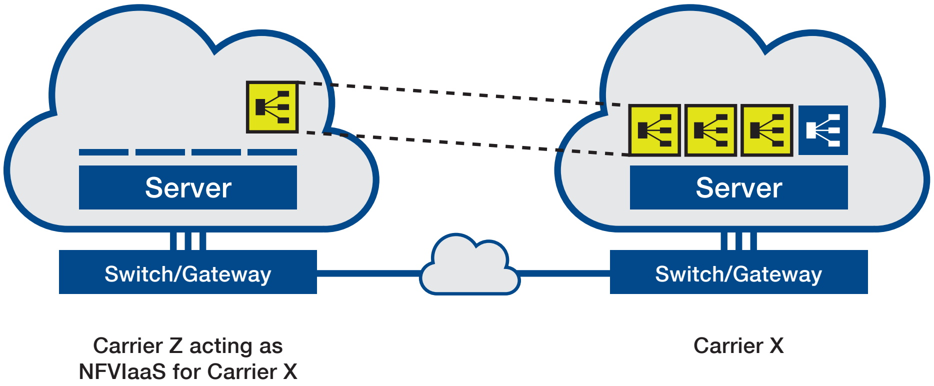
NFV INFRASTRUCTURE AS A SERVICE (NFVIAAS)

Another NFV use case promoted by ETSI is NFVIaaS, which is required for the delivery of cloud services. In this use case, one service provider can offer services using the

NFV infrastructure (NFVI) of another service provider. This approach can greatly expand a carrier's reach in locations where it maintains no physical network assets.

Figure 4 illustrates the concept of NFVIaaS. In this example, service provider X offers a virtualized load balancing service. Some of carrier X's customers need load balancing services at locations where that company doesn't maintain NFVI, but where service provider Z does.

FIGURE 4
NFV infrastructure as a service (NFVIaaS) (Example)



NFVIaaS offers a means for carrier Z to lease NFV infrastructure (compute, network, hypervisors, etc.) to service provider X, which gives the latter access to infrastructure that would otherwise be prohibitively expensive to obtain. Through leasing, such capacity is available on demand, and can be scaled as needed.

The value proposition for this NFV use case is significant. By eliminating the cost and complexity of deploying new hardware or leasing fixed services, Carrier X can deploy and scale virtualized services rapidly, and extend the reach across other service providers as well. Carrier Z benefits by monetizing excess capacity and leveraging its investments in NFV and SDN infrastructure.

NFVIaaS also simplifies deployment by abstracting differences among diverse carriers in tunneling, addressing, QoS, policy enforcement, security, and operational procedures. Other key requirements include multi-tenancy to ensure sufficient traffic isolation, and tenant-specific policy enforcement and elasticity to reduce the cost and complexity of scaling in a dynamic cloud-services environment.

Like SDN, NFV is predicated upon an open and multi-vendor environment to maximize choice and reduce CapEx costs. A common automation framework capable of provisioning both physical and virtual infrastructures is required, along with a common deployment model that spans service provider and geographical boundaries.

NFV Networking Requirements

There are a number of challenges to support NFV using today's static, expensive-to-manage networks, as illustrated by the use case examples cited above.

- **Real-time and dynamic provisioning.** VNFs, VNF FGs, etc. must be automatically deployed and managed in the NFV infrastructure.
- **Seamless control and provisioning** of physical and virtual networking infrastructures.
- **Carrier-grade scalability and robustness.**
- **Openness and interoperability.** Like SDN, NFV envision an open environment where network elements and VNFs from multiple vendors interoperate and co-exist through open interfaces (i.e., OpenFlow) and APIs.
- **NFV global reach and cross-administration.** Connectivity that spans multiple administration domains and geographies is essential.
- **Acceleration of innovation.** The unique demands of NFV potentially necessitate in a massively complex forwarding plane, blending virtual and physical appliances with extensive control and application software, some of it proprietary. SDN principles, based on OpenFlow as the cornerstone, transform the control plane to be software-centric, open, and programmable—an ideal foundation for innovation.

OpenFlow-enabled SDN: A Flexible NFV Networking Solution

Service providers deploying NFV are pursuing new business models that transform their operations to increase revenues while simultaneously lowering overall costs. OpenFlow-enabled SDN provides the flexible framework required to address the NFV networking requirements addressed above.

Figure 5 presents a network view illustrating how SDN can enable NFV. This is merely one example of how SDN can work with NFV; many others are being actively discussed.

LOWER CAPEX

OpenFlow-based SDN leverages logically centralized intelligence and network virtualization to minimize the stranded capacity and maximize network resource utilization.

A similar outcome is achieved for NFV by virtualizing storage and server resources in the NFV infrastructure (NFVI). Higher resource utilization translates into less equipment, which also simplifies the network and operations.

LOWER OPEX

Both NFV and SDN transform operations by automating current generation manually intensive network configuration, provisioning, and management. By automating the infrastructure, provisioning and configuration times improve, complexity is reduced, and manual errors are dramatically decreased.

The net result is a dramatic improvement in time to new service and agility, resulting in new and increased revenues.

SHORTER TIME TO MARKET AND LESS DEPLOYMENT RISK

Deploying a new service in a large-scale network is a long and arduous process. It also requires long cycles of validation, testing and pilots to iron out issues and glitches.

By automating the management and orchestration of the NFVI, time to market for configuration changes for new service rollout will be significantly reduced with OpenFlow-based SDN/NFV. In addition, a virtualized infrastructure for both NFV and SDN facilitates DevOps methods, where software changes can be systematically tested on the actual NFVI prior to being deployed without impacting the operational network.

OPENNESS

OpenFlow, the first SDN standard, has evolved over the past few years, with a number of deployments and products now realized. Driven by rapidly increasing adoption of cloud services, OpenFlow-based SDN is emerging as an essential data center technology, and an outstanding enabler for NFV and carrier networks.

ONF is committed to an open, robust SDN architecture, with a number of activities underway to address the specific needs for the carriers. These activities include a carrier network discussion group to address general carrier SDN issues, optical transport and mobile wireless working groups examining segment-specific extensions, and a migration working group to examine the best practices for migrating to OpenFlow-enabled SDN.

In addition, the widespread dissemination of SDN and OpenFlow knowledge, ecosystem components, open source software, education, and training will help carriers evolve their workforce as well to develop the skills to support a new software-oriented carrier network to support NFV over the long term.

Summary and Conclusions

Network Functions Virtualization offers the potential to transform carrier/network operator operations while achieving significant agility and cost reduction. SDN is emerging as the key enabler for NFV, offering the dynamic behavior, automation, and openness required for carrier networks in the future.

The unique challenges created by NFV—the need for elastic dynamic connectivity, on-demand control of physical and virtual appliances, and openness—are all synonymous goals for NFV and SDN.

As NFV leverages cloud computing and virtualization practices, forward-looking carriers will consider adopting OpenFlow-based SDN for the NFV infrastructure. The NFV use cases highlight the need for multi-supplier, dynamic, and automated control of flow forwarding across network segments—a problem well understood and solved by OpenFlow. SDN and OpenFlow are rapidly maturing and expected to emerge as an important enabler for NFV deployments.

Contributors

Michael Zimmerman, Editor
David Allan
Marc Cohn
Nabil Damouny
Christos Kolias
Jeff Maguire
Serge Manning
Dave McDysan
Evelyne Roch
Meral Shirazipour

References

1. Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action, ETSI, October 2012, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

2. Network Functions Virtualisation (NFV): Network Operator Perspectives on Industry Progress, ETSI, October 2013, http://portal.etsi.org/NFV/NFV_White_Paper2.pdf

3. GS NFV 001 Network Functions Virtualisation (NFV); Use Cases, ETSI, October, 2013, http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf