White Paper

Practical Implementation of SDN & NFV in the WAN

Prepared by

Sterling Perrin, Senior Analyst, *Heavy Reading*; and
Stan Hubbard, Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

www.hp.com

www.intel.com

WIND RIVER

www.windriver.com

October 2013

Introduction

Software-defined networking (SDN) and network functions virtualization (NFV) have exploded over the technology horizon in the past 18 months, surprising many with the speed at which interest has evolved and spread.

SDN, initially centered on the OpenFlow protocol, emerged first in the campus and data center, but has since migrated rapidly into the WAN. More recently, network operators have rallied around bringing IT concepts of virtualization and commoditized hardware into the WAN, in the form of network virtualization.

This white paper explores SDN and NFV with an emphasis on the benefits, use cases and challenges that must be overcome to move forward. We conclude with a proof point, describing how Intel, Wind River and HP have partnered to address several of the challenges posed by SDN/NFV and using open standards and low-cost commercial off-the-shelf (COTS) hardware.

SDN & NFV Benefits for the WAN

SDN and NFV, both separately and together, hold tremendous promise to address service provider and enterprise network challenges caused by increasing traffic volumes, stagnant revenues, requirements to break away from proprietary lock-in and the new elastic/flexible network demands of the cloud.

In early 2013, *Heavy Reading* conducted a series of in-depth interviews with 27 senior executives and strategists working at 18 network operators to gauge opinions and plans for SDN and NFV. The interviews were mainly with large Tier 1 operators, but also included some smaller operators, especially in the enterprise/ wholesale sector.

Based on these interviews, the key drivers for deploying NFV and SDN, in rough order of importance, were:

- **Lower-cost hardware** – big savings are expected here
- **Much faster upgrade cycles** for both hardware and software components
- **Lower opex**, especially in maintaining distributed equipment
- **New products and features** that are only feasible in an SDN environment
- **Revamp OSS** using SDN
- **Lower energy costs** – particularly important for some
- **Reach new customers** via the virtualized service environment

The expectations for cost reduction are often radical; incremental improvement is not the objective. For example, one operator interviewee said that the underlying hardware should fall to only 10 percent of its current cost. Another estimated that the cost of deploying peripheral network functions that were used by only a portion of customers would fall by more than 95 percent.

Service providers have equally high expectations regarding upgrade cycles for network software, anticipating that this can be achieved in days, rather than weeks or months. A common refrain among the network executives we've interviewed is that, if the IT services can be provided in seconds with cloud computing technologies, it should not take days or weeks to deliver the network services that support them.

New revenue-generating services and reaching new customers are particularly important drivers/benefits for those on the "product" side of the organization, such as those involved in cloud, Ethernet and VPN services offered to enterprises.

For some, SDN was also an enabler for a better and more reliable set of cloud services. As one put it: "SDN abstraction delivers more scale and predictability and a faster turnaround for customers. Making control of cloud/network infrastructure transparent (i.e., through self-service) removes [the] hurdle to cloud adoption."

SDN & NFV Use Cases for the WAN

As service providers and enterprises now understand the potential benefits of SDN and NFV in general terms, there is strong momentum on both technologies in defining specifics. In the past six months, we have seen strong interest in identifying and defining practical use cases.

Figure 1 encapsulates a range of SDN potential use cases that *Heavy Reading* has observed in recent months.

Figure1: SDN Potential Use Cases

USE CASE	ROLE OF SDN
Bandwidth on demand	Enable programmatic controls on carrier links to request extra bandwidth when needed.
Performance on demand	API-driven service in which the network dynamically ensures not only that the appropriate capacity is available for a given application, but also that a guaranteed level of performance is delivered.
Dynamic WAN interconnects	Create dynamic interconnects at interchanges between enterprise links or between service providers using high-performance switches.
Dynamic WAN reroute – move large amounts of trusted data bypassing expensive inspection devices	Provide dynamic, yet authenticated, programmable access to flow-level bypass using APIs to network switches and routers.
Virtual edge / CPE	In combination with NFV, replace existing customer premises equipment (CPE) at residences and businesses with light-weight versions, moving common functions and complex traffic handling to the service provider edge or data center.
Virtual private cloud	Operator offers a virtual cloud service within its network that provides enterprise-grade security, performance and control attributes associated with a private cloud.
Service chaining / traffic steering with SDN	In SDN networks, the ability to associate the right traffic to the right appliance, thus making use of the appliance only when needed. (Can be used in conjunction with NFV.)
Network virtualization – multi-tenant networks	To dynamically create segregated topologically-equivalent networks across a data center, scaling beyond typical limits of VLANs today at 4K.
Network virtualization – stretched networks	To create location-agnostic networks, across racks or across data centers, with VM mobility and dynamic reallocation of resources.
Network slicing	Having several customers each running different types of protocols over different virtual topologies based on a single physical network.

Figure 2 is drawn directly from early European Telecommunications Standards Institute (ETSI) work in defining use cases for NFV.

Figure 2: NFV Potential Use Cases

USE CASE	DESCRIPTION
Virtualization of mobile core network nodes	Virtualization of core network nodes, including IMS. Affected functions could include packet data network gateways, serving gateways, mobility management entities and mobile home subscriber servers.
Virtualization of mobile base stations	Aims at realizing the base station function (at least specific functional block) with software based on standard IT platform. Mainly focused on LTE LTE-A, but similar concept can be applied to 2G, 3G and WiMax.
Virtualized home environment	Aims to shift functionality away from the home to a network-located environment as a way to solve many installation and lifecycle upgrade problems, consolidating the corresponding workloads into equipment installed in the network operator premises. Virtualization targets include: residential gateway; set-top box; Wi-Fi access points; home eNodeB.
Virtualized network function as a service	Possible virtualization targets: enterprise access router/enterprise CPE, provider edge router, enterprise firewall, enterprise NG-FW, enterprise WAN optimization, deep packet inspection (appliance or a function), IPS – and other security appliances, network performance monitoring.
Service chains with NFV	Virtualizing the appliance functions and putting them into applications on a server in a single location or area – making service analysis more efficient and streamlining the flow of traffic in the network.
Virtualization of CDNs	Virtualization of content delivery networks (CDNs) potentially covers all components of the CDN, though the initial impact would probably be on cache nodes for achieving acceptable performance (e.g., throughput, latency).
Fixed access network functions virtualization	Target network functions for virtualization in fixed access networks may include Layer 2 control functions from: OLTs, DSLAMs, ONU/ONTs and MDUs. Virtualization also supports multiple tenancy, whereby more than one organizational entity can either be allocated, or given direct control of, a dedicated partition of a virtual access node.

Source: ETSI, 2013

We make two points regarding the use cases described above:

- We have written up SDN and NFV use cases separately, but there is clear overlap between the two technologies: NFV plays a role in certain SDN cases, and *vice versa*. Where the interaction is obvious, we made note within the descriptions.
- It is early days for both SDN and NFV, and use cases will evolve over time. New use cases will be added, while some early cases will prove impractical and be dropped. In focusing on the practical, service providers and enterprises also need to understand the challenges associated with use cases and applications. These are detailed further in the next section.

SDN/NFV Challenges to Overcome

SDN and NFV are passing the "euphoria" phase of their evolution and moving into a new phase in which barriers and challenges are starting to arise. It is a natural evolution of new technology that flows from the fact that users are moving past the basic questions of understanding the potential benefits of SDN/NFV and toward deeper questions of how these new technologies can realistically be implemented in their own networks.

Just as the potential benefits of SDN and NFV vary from organization to organization – and even from department to department – so do the challenges. In our interviews with service providers, *Heavy Reading* identified different sets of challenges for the network side of the organization and from the cloud/IT side.

Figure 3 shows the key barriers to SDN/NFV adoption cited by service provider executives and separated by their department within the organization (network-side or cloud/IT).

Figure 3: Key Barriers to SDN/NFV Adoption by Organization Department

NETWORK	CLOUD/IT
Lack of clarity on who key suppliers or ecosystem builders would be	Applications are not designed to run in the cloud and will be costly to re-engineer
Issues around legacy OSS	Need to manage and orchestrate "bare metal" IT systems in parallel with cloud for workloads that can't be migrated
Changing the corporate culture (operations, product development)	Insufficient information about the performance requirements of virtualized apps/functions
Lack of standards in some areas	Uncertainty about the impact of allowing customer self-provisioning of the network
Lack of orchestration layer	Difficulty keeping up with the speed of market development
Throughput issues at high end	Financial reporting rules are currently based on physical hardware allocations
Lack of clarity on "hybrid" approaches	Need for interoperability with existing infrastructure/OSS
Latency and other net/app-specific issues	

The threat to incumbent network equipment providers looms large among service provider and enterprise concerns regarding both SDN and NFV. There is widespread concern that existing switching and router suppliers would be reluctant to provide what is being asked for. For example, as we noted earlier in this paper, some service providers are expecting hardware costs to fall by as much as 95 percent. Such expectations do not bode well for today's suppliers. The ultimate role of incumbent network equipment suppliers in the SDN/NFV future remains an open question.

Key Standards Activities & Timelines

Open standards will be instrumental to the success of SDN and NFV. The value propositions for both SDN and NFV derive heavily from breaking away from the proprietary network equipment architectures of the past. Thus, openness is a requirement, and standardization yields openness. While suppliers can address a portion of SDN benefits with proprietary technology, it is not what the industry wants. Here we describe four relevant major standards activities.

OpenFlow

Founded in March 2011, the Open Networking Foundation (ONF) is focused on fostering a healthy market for SDN products and services. The organization has taken responsibility for defining the OpenFlow standard, promoting OpenFlow interoperability testing and helping to ensure that OpenFlow can be smoothly integrated into existing network environments. More than 90 service providers, equipment providers, testing providers and other organizations have joined the ONF. The organization's board is composed of the co-founders of Nicira and experts from major companies that use communications networking equipment – including Deutsche Telekom, Facebook, Google, Microsoft, NTT and Verizon.

ETSI NFV

NFV work is driven by ETSI, which formed an Industry Specification Group (ISG) in 2012 to accelerate progress in network virtualization. While ETSI is a standards body, the output of the NFV ISG will not be a standard itself. Rather, the goal of the ISG is to use existing standards – from the ONF, the IETF, and others – in a common (or standardized) way, in order to speed adoption. The NFV work is driven by large Tier 1 network operators globally, including AT&T, BT, China Mobile, Verizon, NTT and Telstra, among others.

OpenDaylight

Launched in April 2013, OpenDaylight is the newest of the SDN-related initiatives discussed in this paper. OpenDaylight is a collaborative open-source project managed by the Linux Foundation that aims to further adoption and innovation in SDN "through the creation of a common industry-supported framework." Founding members include Arista Networks, Brocade, Cisco, Citrix, Dell, Ericsson, Fujitsu, HP, IBM, Intel, Juniper, Microsoft, NEC, Nuage Networks, PLUMgrid, Red Hat and VMware. (Big Switch was also a founding member but has since left.) As of the end of July, there were 27 member companies. The initial goal of OpenDaylight is an open-source SDN controller, based on the OpenFlow protocol along with other popular networking protocols, including Open vSwitch and BGP.

OpenStack

Founded by Rackspace Hosting and NASA, OpenStack is a global collaborative project aimed at building free, open-source cloud computing software for public and private clouds. The OpenStack Foundation, established in September 2012, manages OpenStack. All of the code for OpenStack is freely available under the Apache 2.0 license, and anyone can run it, build on it or submit changes. Platinum members are AT&T, HP, IBM, Nebula, Rackspace, Red Hat, Suse and Ubuntu. The total membership exceeds 150, including Yahoo! Cisco, Intel, NEC, Dell.

Intel/HP/Wind River Reference Design Demo

Intel has partnered with HP and Wind River to demonstrate that the performance of a standard open-source Open vSwitch can be improved upon by an order of magnitude by fusing Intel's Data Plane Development Kit (DPDK) with Wind River's Open Virtualization Profile (OVP) and running the software on industry-standard hardware (as supplied by HP in this demo). The reported tenfold performance gain in packet switching throughput promises to enable service providers to support more virtual machines (VMs) in a virtual appliance model than previously anticipated with a standard approach to virtual switching.

The Intel/HP/Wind River solution represents an important step toward realizing the benefits of NFV by eliminating performance bottlenecks and enabling numerous applications that run on dedicated operating systems and hardware to be consolidated onto a single, more scalable, intelligent and efficient networking platform. Significantly, the Intel/HP/Wind River combination is built to be used "horizontally" across a number of the use cases described in this paper.

Below, we offer a brief overview of the standard Open vSwitch and discuss how the DPDK/OVP virtual switching solution overcomes limitations with this approach.

Standard Open vSwitch – Purpose & Current Limitation

Open vSwitch is a production-quality open-source software switch designed to run on industry-standard hardware, such as the HP ProLiant DL380, in a virtualized server environment. Support for Open vSwitch was integrated into release 3.3 of the Linux kernel in March 2012, thus enabling the vSwitch to operate on modern Linux-based virtualization platforms.

Open vSwitch forwards traffic between different VMs on the same physical host and between VMs and a physical network. Like a physical switch, Open vSwitch operates at Layer 2, but it can also operate at Layer 3. Packets can be directed based on both the MAC address and the IP address. Open vSwitch supports standard management interfaces and is open to programmatic extension using OpenFlow and the Open vSwitch Database (OVSDB) management protocol.

Open vSwitch developers originally envisioned the Linux kernel module providing the highest data path performance possible, but they also designed the vSwitch to be able to operate in user space without assistance from a kernel module. While this user space was originally regarded as experimental territory, it is now being utilized by Intel and Wind River, as explained below.

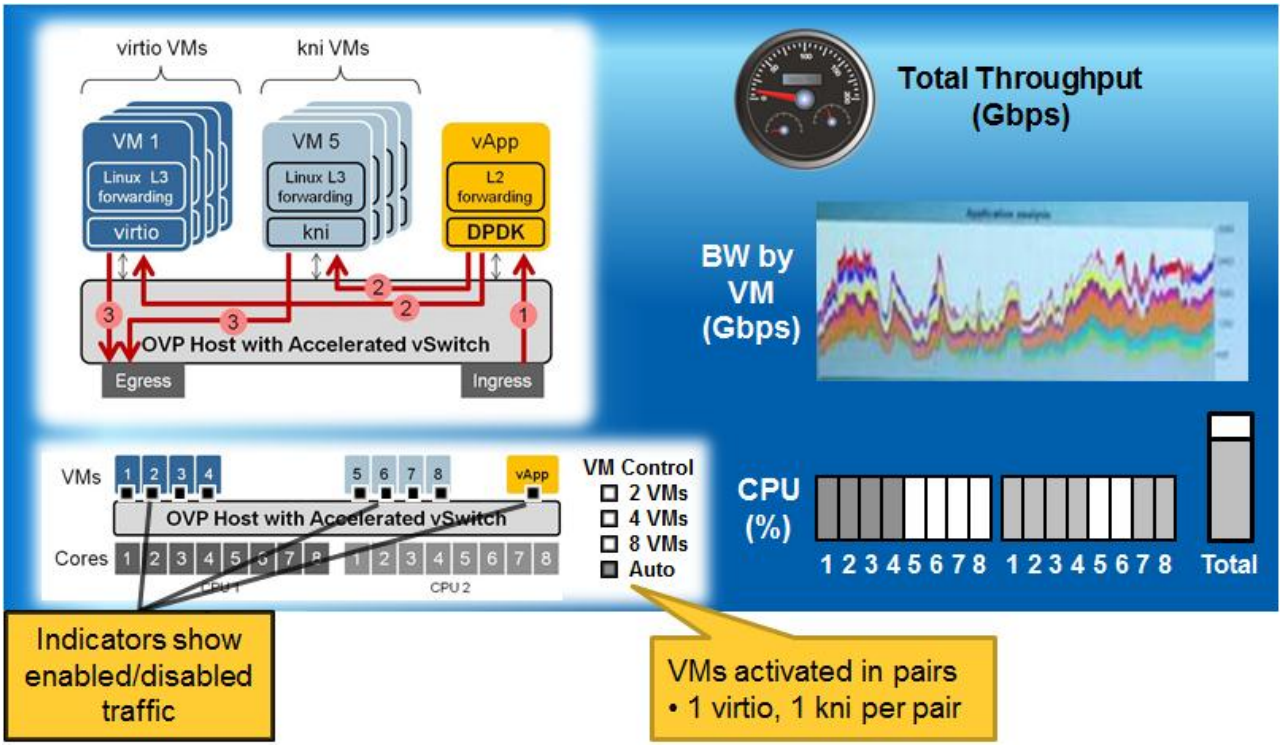
Unfortunately, experience with the standard Open vSwitch thus far has reportedly revealed that use of the data plane within the Linux kernel has not provided the high performance necessary to deliver sustained, aggregated network traffic to virtual network functions as appliance demands scale. The standard vSwitch can quickly become overloaded when the number of supported virtual appliances (vApps) increases. When the vApp becomes a bottleneck, vSwitch VMs will suffer from lower utilization.

Intel & Wind River Accelerated vSwitch Solution

Intel and Wind River designed a virtualization solution that entirely bypasses the vSwitch in the Linux kernel in order to boost packet switching throughput. While the

companies kept the control path the same, they took the vSwitch data path out of the Linux kernel and recreated the data plane in Linux user space by building switching logic on top of the Intel DPDK library. The diagram below illustrates how customers can take a vApp (i.e., load balancer, firewall, etc.) and serve all the VMs on the platform.

Figure 4: Intel & Wind River Accelerated Open vSwitch



Source: Intel and Wind River

Intel and Wind River use a shared memory model, so that when packets come in the vSwitch analyzes the header and does not have to copy the packet. The vSwitch passes a pointer to get better overall performance.

This reference design is based on the HP DL380p Gen8 ProLiant server. The HP server configuration used in the reference design is fully NEBS certified and can be ordered in either AC or -48V DC for telecom central office installations. HP servers support Intel's Open Networking Platform reference designs, and with Intel's latest processor refresh they are faster, smarter and more efficient, so that businesses can adopt this new style of IT for their network applications.

Benefits of Accelerated vSwitch & Conclusions

SDN and NFV are passing the euphoria phase of their evolution and moving into a new phase focused on building practical use cases and overcoming the barriers and challenges posed by real-world implementation. Significantly, the Intel/HP/ Wind River partnership described in this paper addresses several of the major challenges posed by SDN and NFV, including:

- Service providers seek clarity on key suppliers and ecosystem builders for SDN and NFV. The Intel/HP/Wind River partnership, as exemplified in the Accelerated vSwitch demonstration, is a real example of a supplier ecosystem built specifically around SDN and NFV and based on open standards and low-cost COTS hardware.
- The Accelerated Open vSwitch is a "horizontal" platform that can be used across multiple use cases emerging for both SDN and NFV.
- The accelerated vSwitch solution can remove the vApp as a bottleneck and thereby enable higher VM utilization and up to a tenfold improvement in throughput compared to the standard Open vSwitch. The solution also addresses latency in a virtual environment, which is a requirement in certain applications.

Moving forward, the networking industry needs more refinement of the use cases identified for NFV and SDN, as well as more proof points identifying practical implementations of SDN and NFV standards and technologies. For their part, Intel, HP and Wind River are engaging with customers to discuss a wide range of applications that could benefit from their virtualization solution, including everything from network appliances in the data center to radio access network applications and Evolved Packet Core applications. They are also accepting proposals from service providers to create proofs of concept surrounding these use cases.

Appendix: SDN & NFV Definitions

There are many definitions of SDN, which has caused tremendous confusion over the past two years. The definition cited below comes from the ONF, which is the steward of the OpenFlow protocol and its development:

> Software Defined Networking (SDN) is an emerging network architecture where network control is decoupled from forwarding and is directly programmable. This migration of control, formerly tightly bound in individual network devices, into accessible computing devices enables the underlying infrastructure to be abstracted for applications and network services, which can treat the network as a logical or virtual entity… Network intelligence is (logically) centralized in software-based SDN controllers, which maintain a global view of the network.

Key themes of the ONF definition are:

- Decoupling the control from the forwarding plane
- Software programmability of network elements
- Centralized network control

Decoupling the forwarding/data plane from the control plane and software programmability are universally common among the various definitions we've seen. Centralized network control is more controversial: Centralization may work well in certain applications but may be inefficient in others, according to some SDN proponents.

Network virtualization has emerged as another trend with strong potential to transform the WAN. Network virtualization, like SDN, takes concepts and technologies that have succeeded in IT and adapts them to the WAN. Many major telecom network operators have rallied around network virtualization and have formed an NFV Industry Specification Group (ISG) within the ETSI standards body to accelerate industry progress. Network operators driving the new ISG include AT&T, BT, China Mobile, NTT, Telstra and Verizon, among others.

ETSI describes NFV as follows:

> Network Functions Virtualisation aims to transform the way that network operators architect networks by evolving standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises… It involves the implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment.

Heavy Reading uses the term "NFV" to describe the ETSI work specifically. We use the term "network virtualization" to address the trend more broadly, as some suppliers may virtualize functions but in ways that are ahead of, or different from, the ETSI NFV roadmap.