The 2015 Guide to SDN and NFV

Part 3: The SDN and NFV Ecosystem

By Dr. Jim Metzler, Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Platinum Sponsors:

Gold Sponsors:

Produced by:

Table of Contents

Executive Summary

Over the last couple of years, the hottest topics in networking have been Software Defined Networking (SDN) and Network Function Virtualization (NFV). While both enterprises and service providers have shown great interest in these topics, the vast majority of organizations are still either on the sidelines or in the analysis stage of adoption. The primary goals of the 2015 Guide to Software Defined Networking & Network Function Virtualization (The Guide) are to eliminate the confusion that surrounds SDN and NFV and to accelerate the analysis and potential adoption of these new design and architectural approaches.

The Guide will be published both in its entirety and in a serial fashion. The first document in this series focused on SDN and the second document focused on NFV. This is the third document in the series and it will focus on the combined SDN and NFV ecosystem.

This document has three chapters:

1. SDN Ecosystem
   This chapter identifies the primary classes of vendors that either currently do, or can be expected to provide either parts or all of a SDN solution. Included in the discussion is the value proposition of this class of vendor as well as a set of representative vendors.

2. NFV Ecosystem
   This chapter identifies the primary classes of vendors that either currently do, or can be expected to provide either parts or all of a NFV solution. Included in the discussion is the value proposition of this class of vendor as well as a set of representative vendors.

3. Representative Vendors
   This chapter contains a profile of the sponsoring vendors. The profile focuses on where they fit in the ecosystem, what value they provide and the proof points of that value.

The SDN Ecosystem

One measure of the extent of the SDN ecosystem is that there are currently more than 100 members of the Open Networking Foundation (ONF). This subsection of The Guide identifies the major categories of organizations that are part of the SDN ecosystem and briefly discusses the value proposition of each of the categories. This subsection of The Guide also identifies representative members of each category of organizations that are part of the SDN ecosystem. The representative members that are identified either currently provide the indicated functionality or can be expected to provide the indicated functionality in the near term. As is explained below, in some instances there can be a very wide range in terms of the functionality provided by the members of a given category.

Merchant Silicon/Chip Vendors

Value Proposition: These vendors are in a position to provide hardware support in switching chips for protocols such as OpenFlow and VXLAN. This will have the effect of increasing the speed and scalability of solutions. Longer term there is also the possibility of at least some of these vendors developing cost-effective switch silicon that is optimized for OpenFlow and other controller/switch protocols.

Representative Members:

- Broadcom
- Intel
- Marvell
- Mellanox

HyperScale Data Centers

Value Proposition: Part of their value proposition is that these high-profile vendors either already are or are likely to be early adopters of SDN. As a result, these vendors are having a significant indirect impact on the development of SDN. In addition, vendors such as Google, Yahoo and Facebook are board members of the ONF. As such, these vendors directly influence the work of the ONF in general and of the evolution of the OpenFlow protocol and the northbound API in particular.

Representative Members:

- Yahoo
- Google
- Facebook

Telecom Service Providers

Value Proposition: Part of the value proposition of this class of vendors is similar to the value proposition of hyper-scale data center providers. For example, these vendors either already are, or are likely to be early adopters of SDN in order to support their cloud offerings. In addition, vendors such as Deutsche Telekom, NTT Communications and Verizon are also board members of the ONF.

A preceding chapter of The Guide discussed the interest that IT organizations have in either using SDN in the WAN or in acquiring a service from a WAN service provider that is based on SDN. Responding to that interest, vendors like Pertino are currently using SDN and Network Function Virtualization (NFV)[1] to enable them to offer a new generation of WAN services and Verizon has announced a trial based on using SDN to enable a new generation of data center to data center WAN services. AT&T has announced its interest in using both SDN and NFV to change how it offers services to its customers.

Representative Members:

- Pertino
- Deutsche Telekom
- NTT Communications
- Verizon
- AT&T

Switch Vendors

Value Proposition: Relative to SDN, the majority of these vendors take at least some of the control functionality that has typically resided in their switches and now rely on that functionality being provided by a SDN controller. In addition, these vendors implement protocols in their switches that enable those switches to communicate with an SDN controller. These vendors are increasing reliant on merchant silicon as the basis for major portions of their switching product lines.

Most of the vendors in this category represent traditional switch vendors. An exception to that is Pica8. Pica8 provides a switch that is comprised of its network operating system loaded onto commodity white box, bare-metal switches.

Representative Members:

- Alcatel-Lucent
- Cisco
- Dell
- Extreme Networks
- HP
- Meru Networks
- NEC
- PICA8

Network and Service Monitoring, Management and Automation

Value Proposition: Most, if not all of the providers of SDN solutions will provide at least some ability for the consumers of those solutions to manage the solutions that they provide. The members of this category of the ecosystem don't provide SDN solutions themselves. The vendors listed below either currently provide, or soon will provide management functionality that isn't offered by the providers of SDN solutions and/or they integrate the management of these solutions into a broader management structure.

[1] NFV was explained in the preceding chapter of The Guide

Representative Members:

- NetScout
- QualiSystems
- EMC
- CA

Providers of Network Services

Value Proposition: The members of this category provide network services such as security and optimization that are part of the overall SDN solution. There is the possibility that over time that a large number of independent software vendors (ISVs) will also provide these services.

Representative Members:

- Embrane
- A10
- Radware
- HP
- Riverbed
- Citrix
- Cisco
- Extreme Networks
- NEC

Testing

Value Proposition: The members of this category either provide products that enable equipment manufacturers and others to test SDN solutions or they provide the testing themselves.

Representative Members:

- QualiSystems
- InCNTRE
- Ixia
- Spirent

Standards Bodies and Related Communities

Value Proposition: Some of the members of this category develop use cases, architectures and drive POCs. In some cases, the work of these members helps to clarify the problems that need to be solved and the standards that need to be developed. Other members of this category create standards for protocols such as OpenFlow or VXLAN. These standards form the basis for enabling products from disparate vendors to interoperate.

Representative Members:

- ONF[2]
- IEEE

[2] The ONF is active developing a standards based protocol (OpenFlow) for communicating between a SDN controller and a network element. Its scope of work, however, is broader than just developing OpenFlow.

- IETF
- MEF
- OpenStack
- OpenDaylight

Providers of SDN Controllers

Value Proposition: These vendors provide the controllers that are part of any SDN solution.

Representative Members:

- Big Switch Networks
- NEC
- Nuage Networks
- Netsocket
- HP
- Cisco
- Open Daylight Consortium
- VMware/Nicira

Providers of Telcom Service Provider's Infrastructure/ Optical Networking

Value Proposition: These vendors are providing the infrastructure that enables telecom providers to leverage SDN in their service offerings.

Representative Members:

- ADVA Optical Networking
- Ciena
- Cyan
- Infinera
- ZTE Corporation

Server Virtualization Vendors

Value Proposition: These vendors provide the vSwitches and the hypervisor vSwitch APIs for third party vSwitches that are a key component of SDN and Network Virtualization solutions.

Representative Members:

- Citrix
- Microsoft
- VMware

~ Continued on page 10 ~

AUTOMATE YOUR CLOUD WITH aCLOUD SERVICES ARCHITECTURE

Integrate dynamic services into your Cloud Data Center

www.a10networks.com

Cisco ACI: An Application Centric Approach to SDN

IT Trends and the Advent of Software Defined Networking

IT departments and lines of business are looking at cloud automation tools and software-defined networking (SDN) architectures to accelerate application delivery, reduce operating costs, and increase business agility. The success of an IT or cloud automation solution depends largely on the business policies that can be carried out by the infrastructure through the SDN architecture.

The emergence of SDN promised a new era of centrally managed, software-based automation tools that could accelerate network management, optimization, and remediation. Gartner has defined SDN as "a new approach to designing, building and operating networks that focuses on delivering business agility while lowering capital and operational costs." (*Source: "Ending the Confusion About Software-Defined Networking: A Taxonomy",* Gartner, March 2013)

The Cisco Application Centric Infrastructure (ACI) architecture, Cisco's expanded vision of SDN that encompasses the entire data center infrastructure, supports a more business-relevant application policy language than alternative software overlay solutions or traditional SDN designs. What makes the Cisco SDN policy model application-centric? And what are the benefits? First we need a comparison of ACI to traditional SDN designs.

A Comparison of ACI to Traditional SDN Architectures

Although traditional SDN and Cisco ACI have important differences, both have essentially the same architectural components and concepts for policy-based IT infrastructure automation:

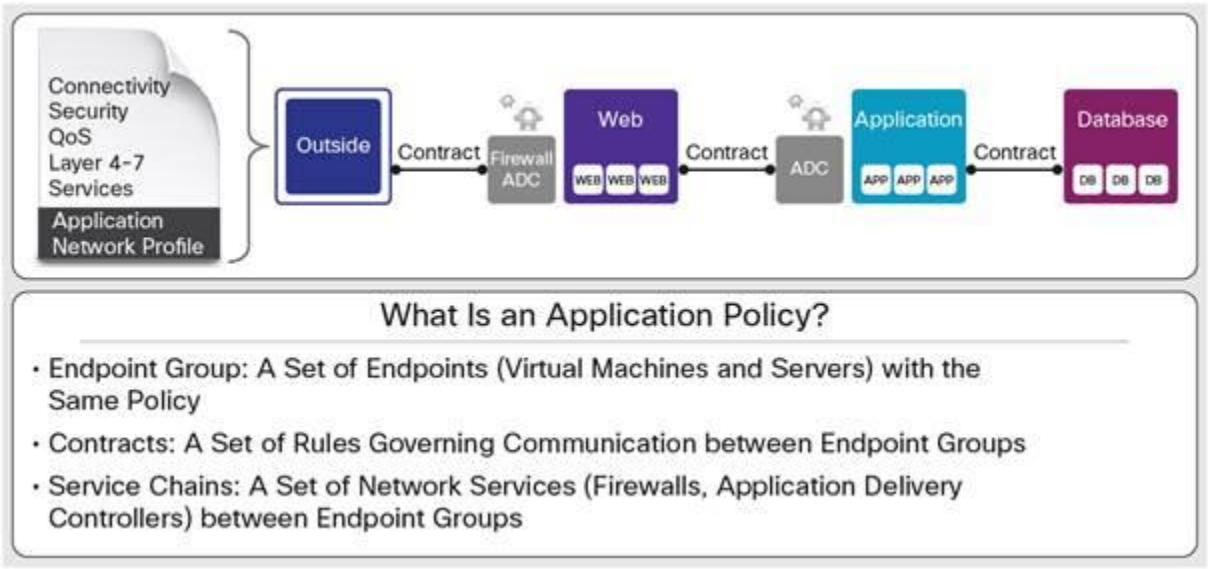
- A centralized policy store and infrastructure controller: In SDN and Cisco ACI, this feature is generally known as the controller (Cisco Application Policy Infrastructure Controller [APIC] for Cisco ACI).
- Programmable, or automated, network devices: All infrastructure devices, such as switches, application delivery controllers and firewalls, must be able to respond to and implement policies according to commands from the controller. This feature may involve agents running on the device, APIs in the devices themselves, or management hooks to the devices that are implemented in the controller.
- A controller southbound protocol to communicate with the managed or controlled devices and to communicate policy information: Initially, the OpenFlow protocol was used in SDN architecture, and vendors released OpenFlow-compliant switches. In Cisco ACI, OpFlex is the primary protocol used, although other mechanisms for integrating devices into the Cisco ACI policy model are supported.
- Northbound controller interfaces for integrating higher-level automation solutions on top of the policy and controller framework, including workflow automation tools and analytics: Modern SDN controllers, as does Cisco APIC, include northbound APIs allowing for the integration of OpenStack or other vendor-specific cloud automation tools (e.g., Cisco UCS Director).

What's unique about ACI is that the policy language (the rules that tell your cloud infrastructure what to do) is not modeled on arcane networking concepts like VLAN's and IP addresses, but on application requirements, and especially how application workloads can and can't communicate, and what kind of services they are entitled to. Policies are applied to classes of applications or workloads (e.g., the web tier of an application), also called endpoint groups (EPG), which can be either physical or virtual workloads (or containers).

An application policy will consist of the EPG's that make up the application, and the contracts and services between the EPG's. This is fundamentally all we need to automate the deployment, provisioning and optimization of our application network anywhere, on any cloud resources we want.

The result is an SDN-automated infrastructure that extends beyond just network devices, to include layer 4-7 application services like load balancers, as well as security devices and policies for IPS and firewall components. Because applications are the best reflection of business activity, an application-centric policy is ideal to align IT with business policies, and to automate policies that reflect real business and application requirements.

Figure – Cisco ACI provisions the entire network infrastructure through application polices managed in a centralized SDN controller, the APIC.



For More Information

For more information, please visit http://cisco.com/go/aci.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-728045-00 05/13

PICA8 OPEN NETWORKING

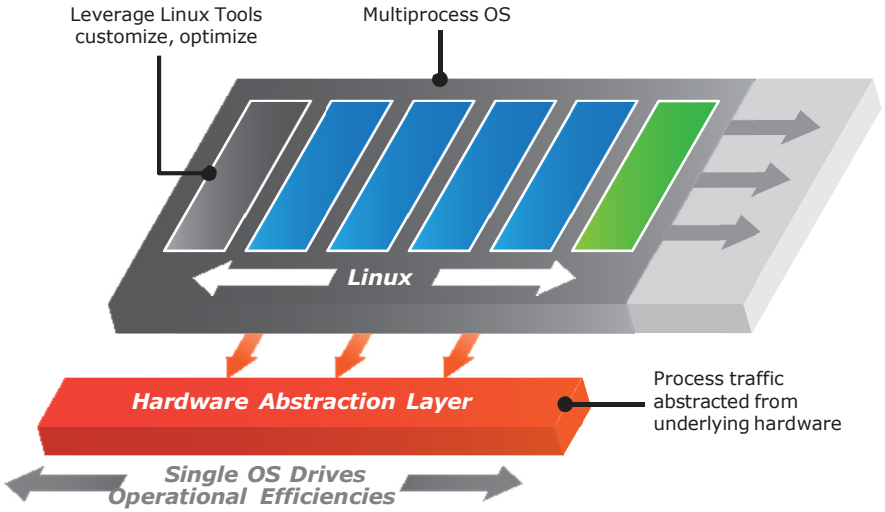
WWW.PICA8.COM

PicOS Overview

PicOS™ is the first bare metal compatible network operating system that:

- Enables customers to seamlessly and easily integrate conventional networking and SDN.
- Provides extensive support for traditional switching and routing protocols that is extendable by SDN and OpenFlow capacity through Pica8's hardware accelerated Open-vSwitch (OVS).
- Offers a unique, comprehensive and flexible configuration management environment from either a Linux shell, a feature-rich command line interface (CLI) or a comprehensive set of APIs (JSON RPC and OpenFlow).

PicOS runs as an application in user space in an un-modified Linux kernel, thereby leveraging kernel thread protection, and compatible with DevOps tools such as Chef and Puppet that are popular with server and system administrators.



* Only OpenFlow features available in hardware are supported, to ensure optimum performance

PicOS - Three Editions to Leverage

A base configuration starts with the Linux Switching OS package. For additional functionality, select either the Routing or OpenFlow Editions, or the PicOS Bundle depending on your use case.

Features Included	Required PicOS Editions		
	Linux Switching OS	Routing	OpenFlow
• Network operation system using user space standard Debian Linux environment • Leverage vast array of standard Linux tools as a common management and operations framework • Zero Touch Provisioning (ZTP) functionality coupled with ONIE delivers a true bare metal to application environment • Rich Layer-2 protocol stack with MLAG, seamlessly integrating into existing architectures • Full Layer-2 & Layer-3 ACL support • IPv4 & IPv6 Static Routing	✓		
• Rich OSPF and BGP protocol stacks integrating into existing spine / leaf architectures • IPv6 routing protocol support (OSPFv3, MBGP) • Multicast PIM support • NAT (depends on ASIC support) • VXLAN network virtualization (depends on ASIC support)	✓	✓	
• Leading OpenFlow 1.4 support through OVS 2.0 • Deliver true seamless migration to SDN through CrossFlow mode (Layer-2 / Layer-3 and OpenFlow simultaneously) • Leveraging OpenFlow to control MPLS, GRE, NVGRE or VXLAN tunnels, delivering on the promise of open programmability • Support for all major OpenFlow controllers (for example: OpenStack Neutron ML2, OpenDaylight, Ryu)	✓		✓
PICOS Bundle	✓	✓	✓

The NFV Ecosystem

One measure of the extent of the NFV ecosystem is that there are currently more than 90 organizations that are full members of the ETSI NFV Industry Specification Group (ISG), with approximately another 140 organizations listed as participants. This subsection of The Guide identifies the major categories of organizations that are members of the NFV ecosystem and briefly discusses the value proposition of each of the categories.

This subsection of The Guide also identifies representative members of each category of organizations that are part of the NFV ecosystem. The representative members that are identified either currently provide the indicated functionality or can be expected to provide the indicated functionality in the near term. As is explained below, in some instances there can be a very wide range in terms of the functionality provided by the members of a given category.

As a point of reference, an extensive list of NFV-related acronyms can be found in *Network Functions Virtualization (NFV): Use Cases*.

Telecom Service Providers

Value Proposition: Service providers are interested in NFV as a means of improving their ability to deliver services to their customers in a timely, cost-effective, and reliable manner. NFV, possibly in conjunction with SDN, has the potential to enable a new generation of services spanning a wide range of Virtual Network Functions (VNFs) that can generate new revenues from other service providers, enterprises, and residential customers.

Representative Members:

- AT&T
- Cablelabs (representing the cable industry)
- France Telecom S.A.
- Telefonica S.A.
- NTT Corporation

Network Systems and Electronic Equipment Vendors

Value Proposition: This category includes a very wide variety of the components of service provider network infrastructures, and, in some cases, enterprise network infrastructure. In order to accommodate NFV and SDN these vendors will need to take at least some of the control functionality that has typically resided in their products and now rely on that functionality being provided by an SDN controller or NFV management system or orchestrator. These vendors need to implement protocols in their products to support communication with central control entities. In a number of cases, vendors will be called upon to migrate the functionality of their products from dedicated hardware platforms to virtual appliances that can run on industry standard servers.

Representative Members:

- ADTRAN Europe Ltd
- Cisco Systems
- Ericsson
- IBM Europe

- Huawei Technologies (UK) Co. Ltd
- Spidercloud Wireless Inc.

Merchant Silicon/Chip Vendors

Value Proposition: These vendors are in a position to provide hardware support for protocols that support SDN and NFV in switching chips and other semiconductors. This will have the effect of increasing the speed and scalability of infrastructures that support NFV as well as the platforms that support VFNs.

Representative Members:

- Broadcom
- Freescale Semiconductor
- Intel
- Marvell

Virtualized Network Service and Cloud Service Vendors

Value Proposition: The members of this category provide VNFs that can be hosted on either the customer's server platforms or provided in the form of a Virtual Network Function as a Service (VNFaaS). Most of these organizations are focused on the communications service providers either as end users or as providers of services to enterprise and residential end users.

Representative Members:

- Allot Communications Systems Ltd
- Mavenir Systems UK Ltd
- NetNumber Inc.
- Virtela Technology Services Inc.

SDN Controller Software Vendors

SDN can be employed by service providers as a means of implementing a Network Functions Virtualization Infrastructure (NFVI) for cloud IaaS services and as a NFVI within their access and core networks. Some SDN implementations provide flow mapping functions that steer traffic flows to VNFs in the proper sequence.

Representative Members:

- Adara Networks Inc
- ConteXtream Inc.
- NEC

NFVI Providers

Value Proposition: The members of this category provide the virtual networking infrastructure including Virtual Switching (Open vSwitch, Linux Bridge), Virtual Networking (IP Forwarding, Virtual Routing, Filtering, NAT, Link Aggregation, etc.), and Overlays such as VXLAN, VLAN, GRE, etc. for multi-tenancy. The NFVI also includes physical NIC poll mode drivers for outside communication and virtual NIC host drivers (such as Virtio) for communication with VMs.

Representative Members:

- 6Wind
- BTI Systems
- Wind River

Orchestration Software Vendors

Orchestration generally involves the assembly of various software components (e.g., VNFs) and hardware components of the end-to-end infrastructure to deliver and manage a defined service. Orchestrators often employ layers of abstraction that facilitate the automation of provisioning, configuration, optimization, and other repetitive operational tasks. Orchestration is another potential solution for mapping flows through VNFs and can be deployed either in conjunction with SDN or independently of SDN.

Representative Members:

- Anuta Networks Inc.
- Cadzow Communications
- CENX Inc.

Network Monitoring, Management and OSS/BSS Vendors

Value Proposition: The members of this category of the ecosystem will provide management functionality that extends to virtualized infrastructures and VNFs and integrates that functionality into a broader management structure.

Representative Members:

- NetScout
- Amdocs Software Systems Ltd
- Comptel Corporation
- Comverse Network Systems Europe B.V.
- EMC
- MetraTech Corp

Hypervisor Vendors

Value Proposition: These vendors provide the VMs, vSwitches, and the hypervisor vSwitch APIs for third party vSwitches that are a key components of SDN and NFV infrastructure solutions.

Representative Members:

- Citrix Systems Inc
- Oracle
- Virtual Open Systems

Test Equipment Vendors and Test Services

Value Proposition: The members of this category either provide products that enable equipment manufacturers and others to test NFV solutions, or they provide the testing as a service.

Representative Members:

- QualiSystems
- European Advanced Networking Test Center
- JDSU Deutschland GmbH
- Spirent Communications
- Tektronix GmbH Co KG
- Yokogawa Europe B.V.

Standards Bodies and Related Communities

Value Proposition: Some of the members of this category develop use cases, architectures and drive POCs. In some cases, the work of these members helps to clarify the problems that need to be solved and the standards that need to be developed. Other members of this category create standards for protocols such as OpenFlow or VXLAN. These standards form the basis for enabling products from disparate vendors to interoperate.

Representative Members:

- ETSI
- 3GPP
- MEF
- ATIS
- IETF
- OPNFV
- OpenStack
- OpenDaylight
- TM Forum

~ Continued on page 23 ~

Dynamic Cloud, Dynamic Services

Service providers are on a journey to the cloud. Network function virtualization (NFV) and software-defined networking (SDN), when fully implemented, will create highly dynamic networks with an unprecedented level of scale, resiliency and programmability.

The result will be new dynamic services, where the network adapts to users' demands, rather than limits what the user can do. These new services promise to be more flexible and offer a better user experience. However, for service providers to remain viable businesses, it is critical that the migration to this new architecture does not disrupt existing services, and the new services do not cost more to deliver than users are willing to pay.

Alcatel-Lucent and Bell Labs have been with you on this journey from the beginning. From the first telephone, to the invention of the transistor, from the earliest digital telephone systems and cellular networks to today's advanced IP/optical and LTE networks, we have been the industry's leading pioneers. We are also an early leader in adapting cloud technologies to the telecom world, and we have the key solutions to get you started on the next stage of your journey.

The NFV Journey

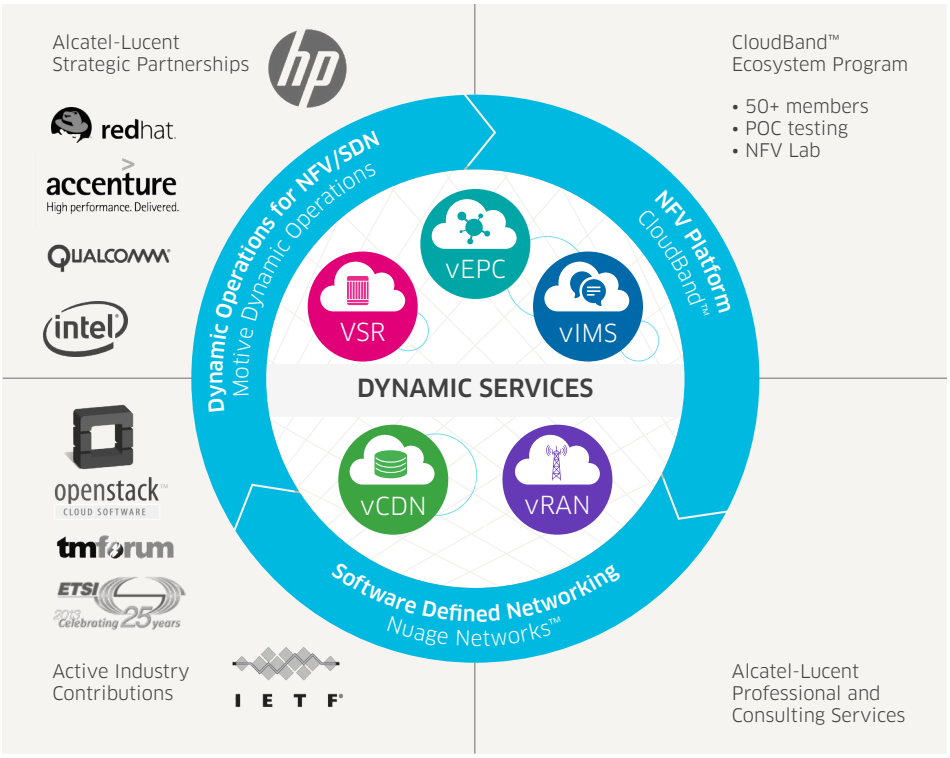
NFV is the start of a multi-year journey; a journey that is being made possible as a result of many technical advances coming together simultaneously. The journey to a fully operational NFV network requires the coordination of three interlinked but separate development paths: virtualization, orchestration and automation. Balancing the investments a service provider allocates to each path has much to do with where they start and their strategy. No path should be considered in isolation.

1. Virtualization

The abstraction of the Telecom functions software from dedicated hardware to run on open commercial-off-the-shelf (COTS) hardware, as well as the need to balance performance and cost reductions, will force service providers to make critical roadmap decisions. Some functions will achieve significant advantages of scale and flexibility from COTS hardware, while other functions, or even the same function, may benefit from the performance advantages of dedicated hardware. This duality is likely to exist for a while, as we pass through a transition phase, but this should not complicate the operational model, provided the same management entities exist. While exact feature parity may not be critical, function performance and robustness cannot be compromised. Service providers should consider the many years of feature development put into the existing functions, and consider carefully how this work will be carried forward into the new mode.

While virtualization of the function is one activity on the path to full NFV, consideration must also be given to how the function will scale. Initially scaling may happen manually, but ultimately, it should be fully automated. Scale and distribution will drive a need for tight inter-virtual machine (VM) communication, and this must be achieved without performance impact.

Alcatel-Lucent's uniquely open approach and ecosystem



The path to full NFV may follow a number of steps as systems evolve:

1. Virtualized software running in a static mode on a defined COTS hardware and software build
2. Virtualized software functions on any COTS or other specialized virtual servers with manually triggered scaling
3. Full cloud implementation with auto scaling, resiliency and open APIs that enable dynamic service activation by third parties, including control of core network functions

When making a decision on which step to take first, the end game should be in sight or it may delay other decisions later on.

2. Orchestration

The orchestration and management of virtual machines needs to be done differently in a telecom network than a typical IT data center. Whether the service provider is offering a mobile app or real-time voice within a Web app (WebRTC) there will be many software routines all interconnected and sharing data across internal and external APIs. Each software module is uploaded onto a virtual machine image within a server. As a result, the telecom domain requires many thousands of virtual machines, which for reasons of resiliency and SLA integrity may be widely distributed. Managing the distribution to assure service performance requires a higher degree of orchestration.

The orchestrator automates the process of preparing and tracking virtual machines within the service provider's network. Each telecom function requires a different virtual machine setup and configuration. Through templates and recipes the orchestrator knows the configuration required to support each application. When a new function and/or more capability is required, an available virtual machine will be located and made available with the correct configuration.

The orchestrator is responsible for the lifecycle management of the virtual machine and its hosted function, including the creation of VM profiles and a wide variety of other functions. A horizontally scalable VNF management function enables the NFV platform to be set up as a Carrier Platform as a Service (CPaaS). The industry still needs to converge on a common scripting tool to create the VNF profiles. The Topology and Orchestration Specification for Cloud Applications (TOSCA) is considered a front-runner.

Quality of service metrics must also be standardized to ensure that when application performance is measured and monitored the performance is considered against a consistent metric and appropriate actions are taken to improve the metric.

3. Automation

As NFV scales, the operator must simultaneously manage the underlying network infrastructure. To do this cost effectively, it is necessary to automate the network to ensure it is in step with application demand. This is the role of SDN.

SDN is currently deployed in data centers where an overlay control layer is proving critical to meet the networking demands of the rapidly rising number of virtual machines. In these deployments, SDN ensures that network connections can be made as fast as the virtual machines within a server are created. The adoption of cloud computing within telecom networks additionally brings much shorter service lifecycles combined with increased application mobility. For typical telecom services, the location of the host for a service can move very rapidly. Thus the wide area network (WAN) environment is more dynamic than in data-center applications.

Adoption of SDN within the WAN will improve the resource and capacity utilization of the network by automating adjustments based on real-time usage. A fully dynamic network will be achieved by implementing NFV and SDN on top of a converged and programmable IP/optical network fabric to scale and automate application and service performance when and where it's needed.

Alcatel-Lucent has already developed the pieces, partners and ecosystem that operators will need to start down these three interconnected paths. We offer best of breed solutions for the different layers of NFV, using industry-supported open platforms and standards that avoid vendor lock-in. Our professional services organization operates a fully featured test bed environment where our partners, ecosystems of developers and service provider customers can ensure the continuity and resilience that real world deployments will demand.

Find out how we can help you on your journey to virtualization: **www.alcatel-lucent.com/solutions/cloud**

CloudBand

The industry reference NFV platform, CloudBand is a management and orchestration platform for open and massive distribution of virtualized telecom functions. With more than 30 customer trials, including most Tier 1 operators, CloudBand also has over 50 ecosystem members who share experiences, as well as implement and test services.

Virtualized Service Routing

The Alcatel-Lucent Virtualized Service Router (VSR) is a highly flexible, virtualized IP edge router optimized for x86 server environments. The VSR delivers a broad and rich set of virtualized IP edge applications and services. It is built to deliver high performance and elastic scalability, and enables rapid service innovation, extends service reach, opens new markets, and accelerates time to market while lowering operating costs with a homogenized physical infrastructure.

Virtualized IMS

The full portfolio of Alcatel-Lucent IMS solutions is now virtualized and commercially available. It has complete feature parity with native solutions, including the same committed SLAs, OpenStack with HEAT support today, migrating to TOSCA. New service innovations beyond VoLTE are enabled by our IMS APIs and WebRTC in partnership with leading application developers.

Virtualized IP Mobile Core

Alcatel-Lucent has virtualized the IP Mobile Core, including gateways, management, policy and charging, subscriber management and element and network management. It is a proven solution, widely deployed and fully supportive of 2G, 3G and LTE Mobile Core features. Deployed and tested in many NFV trials in conjunction with IMS, it has demonstrated tangible benefits for VoLTE.

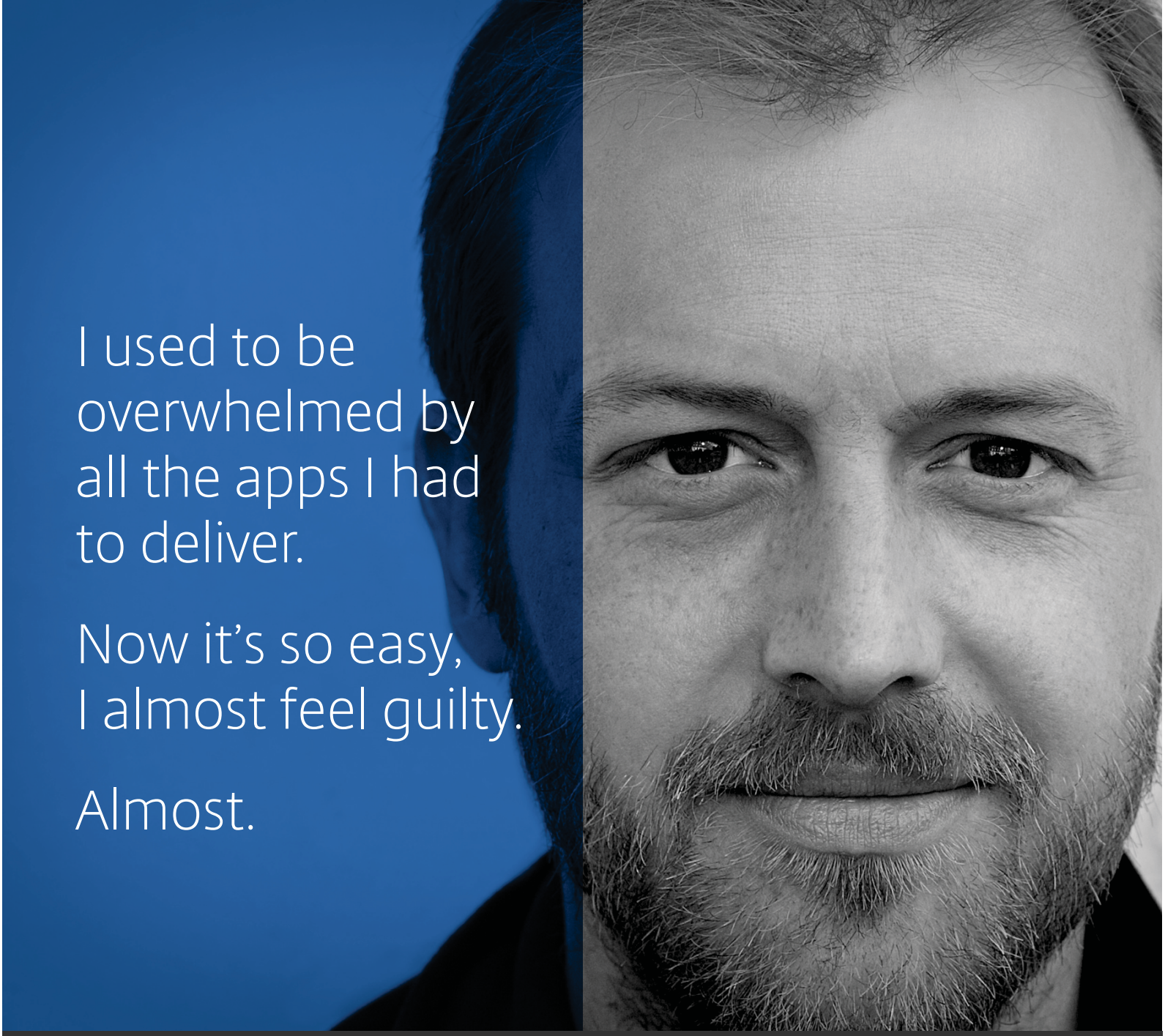
Nuage Networks SDN

Nuage Networks is a leader in SDN. It focuses on modern datacenter requirements for multi-tenancy, full-featured routing and security at scale. The Nuage Networks platform transforms the physical network into a simple to manage, rack-once and wire-once, vendor-independent IP backplane. As a result, network resources within and across datacenters can be treated as an elastic resource pool of capacity that can be consumed and re-purposed on demand.

Motive Dynamic Operations

The new OSS for SDN and NFV, the Motive Dynamic Operations suite brings Motive's rich history with customer experience solutions to the management of SDN automation and NFV abstraction, as well as analytics and professional services – all designed to address different, critical touch points in the relationship between communications service providers and their customers.

Alcatel·Lucent



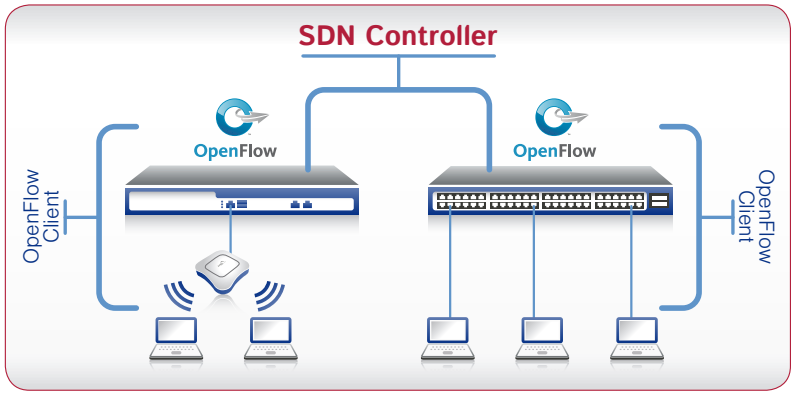
NetScaler with TriScale harnesses the power of software so you can effortlessly customize your app delivery for any business need.

NetScaler with TriScale
SOFTWARE SMART. HARDWARE STRONG.

CITRIX®

www.citrix.com/netscaler

Delivering the promise of SDN across wired/wireless networks



As the enterprise network edge transitions to an all wireless network, software-defined networking (SDN) and OpenFlow are emerging as a way to bring new levels of agility to organizations beyond the data center where SDN first gained traction.

The rapid acceptance of SDN and this new approach to design, build and manage data centers addresses the top challenges experienced by organization related to networks: namely, too many manual processes, and difficulties changing configurations. SDN tackles these challenges in the data center, but SDN can equally address the same issues for the enterprise campus. Without bringing SDN to the edge of the network, its true promise is lost.

Meru is leading the way being the first wireless vendor to receive a Certificate of Conformance through the ONF OpenFlow™ Conformance Testing Program within our wireless LAN controllers to enable third-party control all the way down to the access point. This provides customers with confidence in the products that they adopt will provide multi-vendor support.

Meru is also collaborating with IT giants such as NEC to enable seamless interoperability between the NEC ProgrammableFlow® Networking Suite and Meru 802.11ac intelligent Wi-Fi solutions. NEC and Meru are the world's first vendors to receive OpenFlow Conformance Certification respectively as a wired and wireless vendor - a natural pairing.

Meru has introduced Meru Center, a network application management platform, unifying network applications under a single platform and permits easy activation of pre-installed network tools.

With Meru Center, new SDN applications are delivered via the Meru App Store. This library function hosts a growing set of qualified applications that may be selected and installed on a user's network. Initial Meru SDN applications available will include:

Meru Collaborator
An SDN application that integrates with Microsoft's Lync unified communication solution with the ability to detect QoS (quality of service) issues on a heterogeneous wired/wireless network, deliver prescriptive resolution options and prioritize traffic across multi-vendor wired and wireless networks.

Meru Personal Bonjour
An application that minimizes Bonjour broadcast storms of Apple related devices across unified networks and advertises services only to the correct users according to established policies.

Making SDN a Reality for Wi-Fi

The promise of SDN is that networks will no longer be closed, proprietary, and difficult to manage. Meru is taking a leadership position in the emerging wireless market for SDN, and is committed to delivering the most robust SDN Wi-Fi solution in the market while providing a best-of-breed wireless solution.

With innovative solutions from Meru and a robust SDN ecosystem, organizations can meet the unprecedented demand for Wi-Fi with ease.

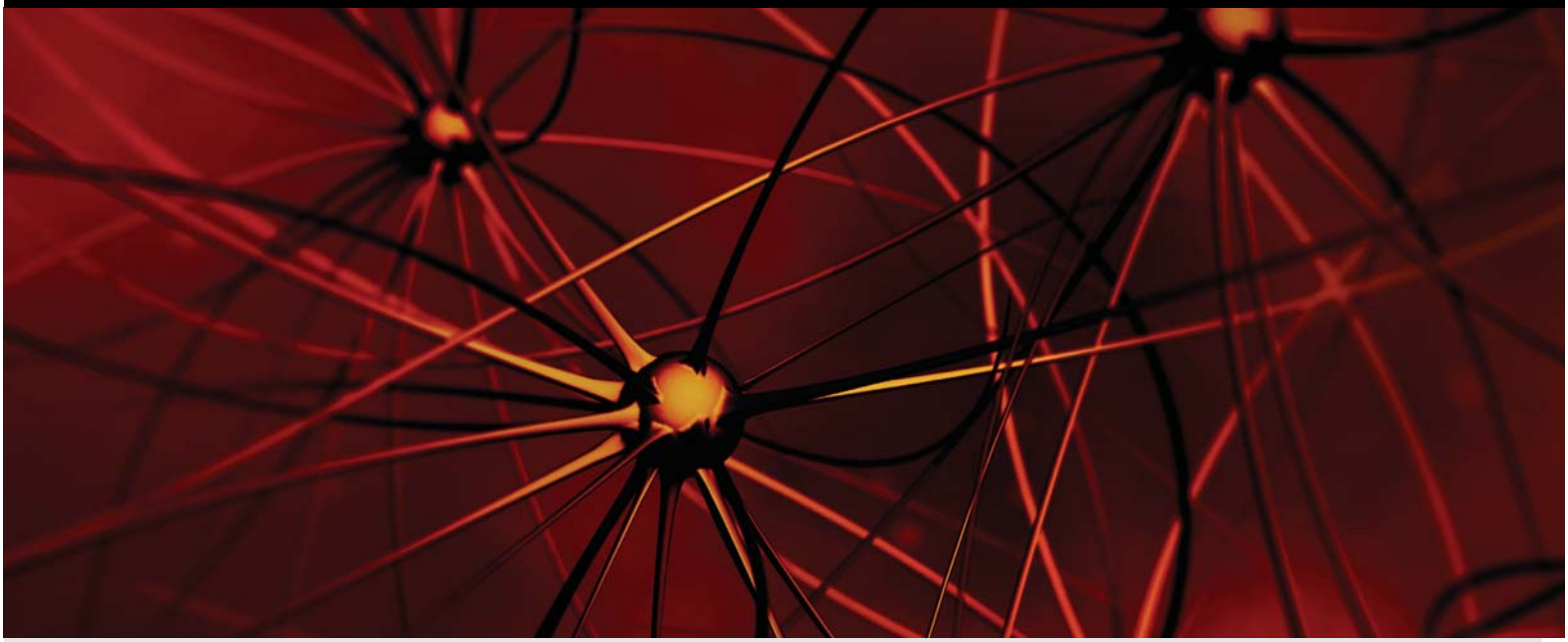
Click for more information

Meru delivers an all-wireless network that fully supports the enterprise, delivering a consistent, interactive experience for all users. No matter what applications they are running. No matter how many other users are on the network. For more information, visit **www.merunetworks.com** or email your questions to: meruinfo@merunetworks.com.

Meru Networks®
Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089
T +1 (408) 215-5300
F +1 (408) 215-5301
E meruinfo@merunetworks.com

nuagenetworks

@nuagenetworks



The Cloud Network Unbound

Virtualized and automated networking across datacenters and branch offices

Cloud computing is changing the way enterprises access and consume data. To remain competitive, businesses know they must be able to react quickly to market changes. The cloud addresses their need for speed, agility and responsiveness. Unfortunately, today's data communications networks aren't keeping pace. In fact, they're struggling to deliver consistent, on-demand connectivity and things are only going to get more challenging. Fortunately, Nuage Networks has a solution.

Nuage Networks leverages Software Defined Networking (SDN) to unleash the power of the cloud, giving enterprises the freedom and flexibility to:

- Connect sites, workgroups and applications faster, more securely and more cost effectively
- React to change easily
- Respond to growth seamlessly

Nuage Networks makes the network as responsive as your business needs it to be — from the datacenter to remote locations.

Our solutions close the gap between the network and cloud-based consumption models, creating an infrastructure in which network resources are as readily consumable as compute and storage resources. Our approach enables enterprises to transform the way they build and use their networks, which has a profound effect inside and across multiple datacenters and across the wide area network.

Imagine the possibilities when network resources are easily consumable. A Nuage Networks datacenter network is as dynamic, automated and virtualized as the server infrastructure, and supports the needs of applications with instantaneous network connectivity.

Take advantage of a fully virtualized services platform

Cloud-based datacenters have unshackled the IT environment, making it possible for applications to request additional compute and storage on an as-needed basis. Extending the reach of virtualized network services from the datacenter to remote locations further enhances the enterprise's ability to respond to business imperatives at cloud speed. Peak demands can be provisioned "just in time", which lowers operational costs and makes it possible to share compute resources across applications. Geography is taken out of the equation.

Nuage Networks SDN solutions enable you to react to changes in your datacenter or at branch locations with speed, agility, and flexibility. Our solutions seamlessly connect your datacenters and the wide area network, so networking across the whole environment is fluid and responsive to changing business conditions.

By improving efficiency, resiliency and security, our products enable networks to be built and operated at any scale – from a single rack to Fortune 500 scale.

Our SDN solutions work closely together and deployment is flexible, so you can focus on the area most in need of help.

Responsive datacenter networking

Build robust and highly scalable networking infrastructures with the **Nuage Networks Virtualized Services Platform (VSP)**. These new infrastructures will let you instantaneously deliver compute, storage and networking resources securely to thousands of user groups.

Virtual private networking on your terms

The **Nuage Networks Virtualized Network Services (VNS)** enables you to respond faster and with greater agility to changes in your wide are network environment. A self-serve portal allows enterprise end users to self-manage moves, adds and changes, significantly reducing the time and effort required to manage the wide area network.

Nuage Networks SDN solutions are specifically designed to:

Simplify operations for rapid service instantiation	Address changing business requirements with flexible, adaptable services	Support massive scalability and hybrid models with secure, open infrastructure
■ Define network service requirements in clear, IT-friendly language ■ Bring services up using automated, policy-based instantiation of network connectivity ■ Dramatically reduce time to service and limit potential for errors	■ Adapt datacenters and private networks dynamically ■ Detect newly created and updated virtual machines within the datacenter and respond automatically by adapting network services according to established policies, instantly making available new applications to all users regardless of location	■ Benefit from distributed, policy-based approach that allows multiple virtualization platforms to interoperate over a single network ■ Optimize the datacenter network and private network by separating service definition from service instantiation

Nuage Networks SDN solution components

Nuage Networks VSP is the first network virtualization platform to address modern datacenter requirements for multi-tenancy, full-featured routing and security at scale. It is a software solution that transforms the physical network into a simple to manage, rack-once and wire-once, vendor-independent IP backplane. As a result, network resources within and across datacenters can be treated as an elastic resource pool of capacity that can be consumed and repurposed on demand.

Nuage Networks VSP integrates seamlessly with wide area business VPN services. It is also particularly effective when deployed with Nuage Networks VNS for a cloud-optimize network that spans the datacenter right out to your remote locations.

NU•ÂHJ: FROM FRENCH, MEANING "CLOUD"

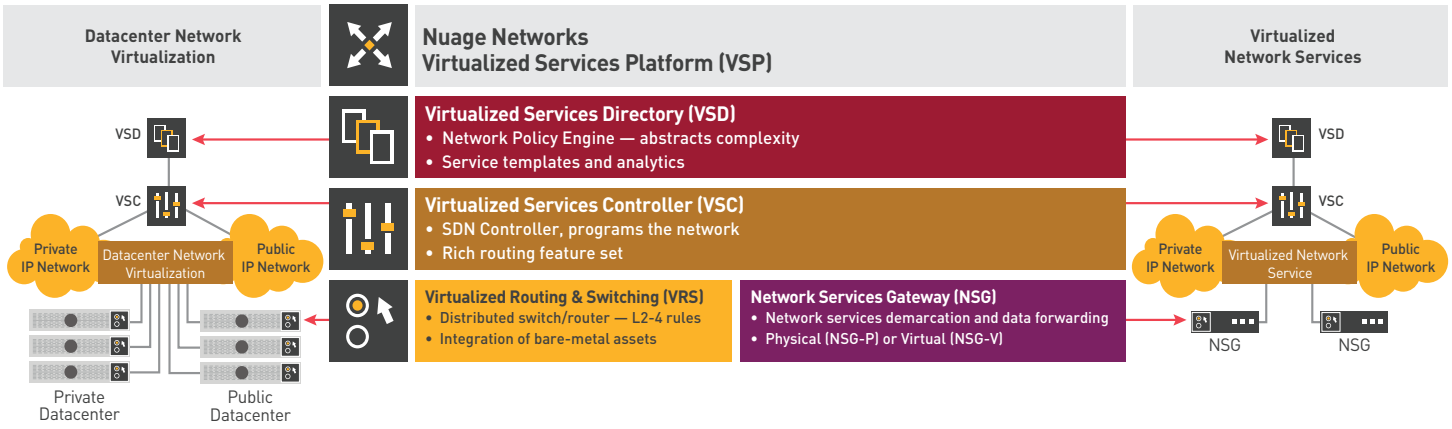
The cloud can be more than what it is. In fact, it needs to be. When we founded Nuage Networks, it was with the idea that it's time for the cloud to come of age. From the beginning we recognized the unique challenges that cloud service providers and large enterprises face delivering and managing large, multi-tenant clouds. While the virtualization of compute and storage has evolved quickly, the network simply has not kept up. The result is that today your cloud is being held back. And so is your business.

When we started Nuage Networks, it was with the mission that we could empower our customers to finally deliver on the true promise of the cloud. We envision a world in which IT and IP are no longer in conflict, but rather work in concert to propel your business and elevate the cloud for every one of your customers. We see a world where innovation isn't hampered by infrastructure, and network resources are as effortlessly consumable as compute and storage.

To make this vision a reality, Nuage Networks brings a unique combination of ground breaking technologies and unmatched networking expertise. This enables us to create solutions that do more than provide incremental improvement. It allows us to introduce radically new thinking and pick up where others have left off, delivering a massively scalable SDN solution that ensures the datacenter and wide area network are able to respond instantly to demand and are boundary-less.

Our mission is to help you harness the full value of the cloud.

Nuage Networks SDN Portfolio



nuagenetworks

Radware's Software Defined Networking Solutions: Enable Network Wide Services via SDN Applications and NFV

Radware SDN applications improve application security, performance and availability by programming the SDN to collect data and optimally forward traffic to deliver network services. The native component of the new network stack introduced by SDN includes the data plane networking devices and the control plane SDN controllers. The Radware SDN applications constructing the SDN application control plane, interact with the SDN controller using dedicated SDN drivers and work together with the Radware systems' using the Radware API to collect data throughout the application infrastructure using specific data collection drivers.

With Radware SDN applications, ADC and security services transform from device-based solutions requiring a static traffic forwarding configuration, to network wide services that intelligently divert traffic to service engines. Network services can scale to support larger networks at lower capital and operational cost. By building SDN applications that continuously interact with the SDN control plane and program the network (and by leveraging the Radware Virtual Application Delivery Infrastructure (VADI) architecture – which enables pooling of disperse resources to operate uniformly) Radware enables an anywhere and everywhere network service paradigm.

Key benefits from the Radware SDN network service infrastructure include:

- **More intelligent application delivery and security decisions** throughout the network break existing network barriers when developing business applications. Every application everywhere is entitled for advanced services.
- **Simpler implementation** of network services allows improved operational efficiency of network management alongside application changes. Not every project needs to become a networking project.
- **Lower overall network service solution costs** – as network service delivery is partially offloaded to the SDN, there is no need to invest in excess network service appliances and capacity. Deploy network services as needed, and use by many tenants and applications throughout the datacenter.
- **Greater scalability** – scale your network services throughout the network. No more limited areas are protected or load balanced. Offer uniform services throughout the SDN.
- **Easier operation** – changing and managing security and ADC functionality becomes simpler as the deployment operates as if it is centralized. Not only does SDN streamline network operations, but Radware SDN applications streamline network service operations. In addition, API to various orchestration systems enables to improve the overall control and automation of network services.

DDoS Protection as a Native SDN Application

DefenseFlow is an SDN application that enables network operators to program the network to provide DDoS protection as a native network service. DefenseFlow features an adaptive behavioral-based DoS attack detection engine and a traffic diversion mechanism that utilizes the programmable characteristics of the software defined network elements for attack cleansing. Designed as part of the Radware SDN application framework, DefenseFlow delivers a security control plane and operates in traditional network environments while enabling to migrate to customer's future, SDN-based networks.

Legacy DDoS protection solutions that make use of scrubbing centers are costly: need hardware detectors in every network location; BGP for traffic diversion; and GRE tunnels to forward the traffic to its designated network object. With SDN, a DDoS protection solution turns into a software application that adds intelligence to the network – no need for additional hardware, BGP or GRE operations.

DefenseFlow equips network operators with the following key advantages:

- **Unprecedented coverage against** all type of network DDoS attacks
- **Best design for attack mitigation**
  - Attack detection is always performed out of path (OOP)
  - During attack only suspicious traffic is diverted through the mitigation device
- **Most scalable mitigation solution – DefensePro mitigation devices can be placed in any location, DefenseFlow diverts the traffic to the nearest mitigation device.**

- **Centralized security control plane including control part of Radware's Attack Mitigation Network (AMN)**

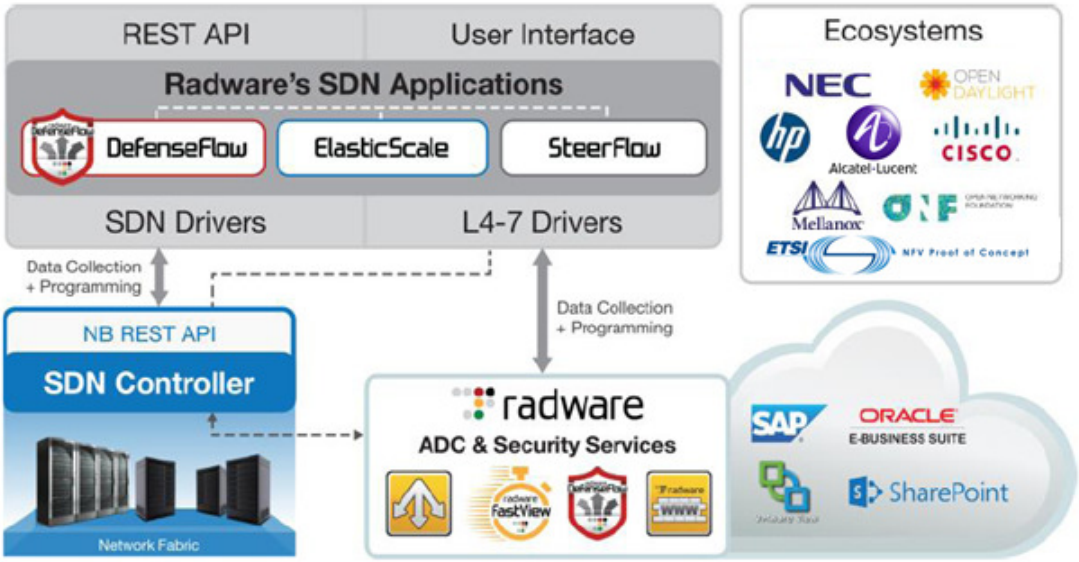
SDN & NFV for a Scalable Application Delivery Network

The Network Functions Virtualization (NFV) initiative was formed in order to enable the standardization of network equipment by leveraging commercially off-the-shelf (COTS) hardware and running advanced network function software on them. Radware is proudly introducing Alteon VA for NFV – the industry's first and only ADC designed from the ground up to run in NFV environments. Targeted mainly at carriers but also at high-end online businesses, Alteon NFV provides unique value proposition including CAPEX/OPEX reduction, eliminate "vendor lock", high performance, high-end scalability and greater network service agility.

Radware's ElasticScale is an SDN application that wraps existing network service virtual appliances, including Alteon NFV, and provides provisioning and traffic distribution logic to consistently deliver network services in an elastic demand environment. ElasticScale can be utilized for service provider internal services, managed services to end customers and can help providers adopt network function virtualization paradigms.

ElasticScale offers network operators the following key features and benefits:

- Ultra scalable traffic steering solution (80Gbps-1Tbps and beyond)
- Based on industry leading, carrier grade Alteon load balancing product line
- Support for leading hypervisors (oXen/KVM/Hyper-V/ESXi)
- Compatible with leading SDN controllers; OpenDaylight, Cisco XNC, NEC pFlow & HP Flare
- Seamless integration with OpenStack and vCloud Director
- Runs over any physical SDN network equipment



Partnering for Success: Our SDN Ecosystem

The SDN eco-system is a critical focus for Radware. Through partnerships with the industry's leading SDN forums and vendors, Radware can ensure customers that our application delivery and security solutions integrate successfully into target architectures. Radware is an active contributor in the following industry and vendor SDN initiatives: Cisco Application Centric Infrastructure (ACI), HP Virtual Application Networks, NEC, Mellanox, Alcatel Lucent, ETSI, Open Daylight Project, and the Open Networking Forum (ONF). Radware is also a member of VMware's NSX partner ecosystem for network functions virtualization (NFV).

Learn More

To learn more about how Radware's SDN solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.

Key Vendors

Below is a profile of the sponsoring vendors that focuses on where they fit in the ecosystem, the value add that they provide and the proof points of that value add.

NetScout

Where do you fit in the SDN and/or NFV ecosystem?

NetScout fits into the SDN ecosystem as one of the leading Service Performance Management (SPM) providers. The SPM vendor landscape in virtual SDN and hybrid environments is very similar to what it is in physical environments. The Application Performance Management players are the same in physical and virtual environments. The Network Performance Management vendors include the traditional players in physical environments as well as the leading SDN / virtualization vendors such as VMware, Microsoft and HP. The bottoms up management approach in virtual/SDN and hybrid environments is conceptually the same as it is in physical environments. The deficiencies of this approach are magnified due to the increase in the overall SPM related big data that needs to be collected, normalized, contextually analyzed and visualized across virtual/SDN and hybrid environments.

For the next few years, the industry will operate in a hybrid environment. Some services will migrate to an NFV/SDN environment while others remain on traditional purpose-build hardware. Even for those services that do migrate to a virtual environment, given the nature of a carrier network, users will still need to traverse functions and services that reside on purpose-built hardware and virtual environments.

For an operator to truly manage and understand the user experience, it will require the ability to have an end-to-end view of the network and services. A view of just the virtual environment or just the traditional environment will not suffice in providing the level of service and experience demanded to truly leverage the agility provided by a virtual infrastructure.

What is your value add?

NetScout believes that its value-add in virtualized and SDN/NFV environments is exactly the same as in physical environments magnified by the extent and breadth of the new challenges.

That value-add includes:

- Pervasive end-to-end visibility into service delivery;
- Reduced MTTR with Proactive Service Triage;
- Enhanced IT Efficiencies through Common Operational View;
- Scalable service delivery management architecture.

NetScout believes that it is uniquely positioned within the industry to be the market leader in monitoring both the hybrid environment as well as the future all-virtual environments. NetScout justifies that statement by pointing out that today it provides a virtual Adaptive Session Intelligence (ASI) probe for VMWare NSX environments. This enables NetScout to extend the monitoring of both enterprise and carrier-scale service delivery infrastructure into both virtual and hybrid environments. This capability is necessary to address the need to monitor services deployed in more complex environments. These environments include physical and virtual

application workloads that exchange greater volumes of traffic between themselves and that also experience higher risk of service degradations. In both a physical and a virtual environment, service degradation often results in a lower quality of end-user experience and may result in increased churn for the service providers.

In a virtual environment there is an additional challenge of collecting management data while having minimal impact on compute and networking resources. This puts significant pressure on monitoring companies to be as efficient as possible with consuming both compute and networking resources in passing monitoring information for performance management. This is another example of where NetScout believes that its ASI technology and the ability to capture, process, and create metadata on packet flow data will be a critical success factor.

What are the proof points?

NetScout claims to have 20,000 of the world's largest enterprises, government agencies, and more than 165 service providers as customers. NetScout believes that the breadth of its customer base combined with their integration with VMware's NSX environment means that NetScout is uniquely positioned to become the leader of SPM in the virtual and hybrid environments.

In the service provider space, NetScout's nGeniuONE platform provides wireless, cable, and wireline network operators with end-to-end network and service performance management. The nGeniusONE platform provides both enterprises and operators a single, monitoring infrastructure for monitoring the hybrid environments of today and the all virtual environments of tomorrow.

NetScout believes that additional proof points of the value-add of its SPM solution in virtual and SDN/NFV environments are based on:

- Shortcoming of existing management tools
    - Existing management tools, such as VMware's vCenter, don't offer end-to-end SPM in hybrid environments.
- Same operational best practices as in the physical environment
    - VMware's vRealize Suite used for cloud operations offers IT the following service troubleshooting tools
    - Syslog – Log analytics using vCenter Log Insight to analyze large volumes of data.
    - NetFlow – class of service, congestion, flows, # of flows (UDP, TCP…)
    - "Deep Troubleshooting" with DPI tools such as Wireshark
    - Manually pinging hypervisors (App VMs, vFW…), check vFW rules (centralized UI – basic ACL using NSX attributes)
    - Configuration management, orchestration, dashboard, capacity mgmt., application awareness (discovery & dependency mapping)
    - These tools are very similar in their scope and functionality to traditional mgmt. tools used in physical environments. Hence SPM solutions have a similar, but significantly augmented, value proposition in virtual and hybrid environments
- Unique agility requirements

Cisco

Where do you fit in the SDN and/or NFV ecosystem?

Cisco believes that its Application Centric Infrastructure (ACI) is an entire open SDN ecosystem unto itself. Cisco markets the SDN/ACI-capable network devices and the SDN controller. Cisco has also defined a policy model and created the communication protocols and interfaces between devices, controller and orchestration platforms. Cisco has stated that its open, extensible environment includes over 60 ecosystem partners, including ACI-compliant network, security and services devices, monitoring, analytics and DevOps solutions, as well as cloud automation platforms.

What is your value add?

Cisco's application-centric approach to SDN:

- Extends beyond network devices to include L4-7 services, security, and eventually servers and storage;
- Includes a policy model which is defined in terms of application requirements and which reflects business activity and requirements, making it easier to align IT with business strategy;
- Applies application policies equally across physical and virtual environments, so the solution is not just an overlay network that has to be managed separately from the physical infrastructure.

What are the proof points?

The proof points include:

- A number of case study videos
- Other case studies
- Awards

A10

Where do you fit in the SDN and/or NFV ecosystem?

IT organizations are evolving their IT strategy by adopting various cloud computing models and SDN architectures for their internal private data centers in order to achieve automation, business agility, and dramatically reduce operational costs. These organizations need an equally automated and agile L4 - L7 network services architecture to ensure that application networking and security policies are fully integrated within these emerging cloud data center architectures, and to deliver equal automation and cost of ownership benefits.

As part of the industry's SDN ecosystem, A10 Networks delivers a portfolio of products and solutions that enable seamless integration with cloud orchestration platforms and SDN network fabrics through API calls to dynamically provision application and security policies per tenant. As part of the industry's NFV ecosystem, A10 Networks delivers virtualized network functions on its vThunder virtual appliances. Automation through OpenStack and integration with on-demand licensing makes it possible to turn up new services for customers as they are needed, and tear them down once they're no longer needed. In addition to flexibility, the A10 appliances allow customers to optimize performance so they can maximize their investment in resources

What is your value add?

Integration with leading SDN networks ensures that network and security policies are applied on any of A10's appliances for automated L4 - L7 services provisioning. Overlay and SDN fabric integration ensures automated provisioning of network segmentation and security policies on a per tenant basis. In addition, A10's NFV solutions allow virtualization of L4 - L7 services so they can be chained together to create customized communications services quickly and as needed.

What are the proof points?

There are several case studies that demonstrate A10's value proposition. This includes:

- http://www.a10networks.com/resources/files/A10-CS-80103-EN.pdf
- http://www.a10networks.com/resources/files/A10-CS_Micron21.pdf
- Additional proof points will be available in Q1 2015

Alcatel-Lucent

Where do you fit in the SDN and/or NFV ecosystem?

Alcatel-Lucent (including Alcatel-Lucent's venture Nuage Networks) offers a comprehensive SDN and NFV solution architecture which is comprised of the Cloudband™ management system, Nuage Virtualized Services platform, Motive Dynamic operations and solution specific virtualized software. Alcatel-Lucent's design goal is to enable scaling of networks with virtualized networking and communications solutions including LTE packet core, VoLTE IMS architectures, virtualized CDN, virtualized RAN, virtualized routing as well as tuneable and scalable packet optical and routing solutions.

What is your value add?

Within the SDN and NFV portfolio, Alcatel-Lucent's focus is on relevant virtualization of its existing networking and communications portfolio and providing the core networking infrastructure to support virtual functions, with its Nuage Networks division for SDN control, Cloudband, a platform for NFV service orchestration, and Motive for dynamic operations of virtualized operations.

Alcatel-Lucent stated that all of its products are developed within an open standards based philosophy and are sold as best of breed solutions on their own or combined within the broader Alcatel-lucent framework. The key relevant products within the Alcatel-Lucent NFV portfolio are:

- vRAN with NFV offering virtual network functions for control, performance and delivery optimization at the RAN level. Alcatel-Lucent's first vRAN platform is already in commercial service with its vRNC solution, which facilitates advanced RNC requirements for geo-redundancy, hitless software upgrades, load balancing, and dynamic reconfiguration.

- Nuage Networks VSP interconnects multi-tenant infrastructures and hybrid clouds with an enterprise's existing Ethernet Layer 2 or IP Layer 3 VPN. A distributed, policy-based approach separates the evolution of compute and networking technologies. This separation allows multiple virtualization platforms to interoperate over a single network. For large scale and high traffic volume environments, the Nuage Networks 7850 VSG provides gateway functionality with native support for 1GE, 10GE and 40GE connections.

- For NFV, the CloudBand Management System orchestrates, automates, and optimizes virtual network functions across the service provider's distributed network and data centers. The CloudBand Node is a turn-key, all-in-one compute and storage node system. It includes hardware and software designed for efficient remote operation of distributed clouds.

- For next generation OSS/BSS solutions, the Motive Dynamic Operations provides Service & unified resource engine (SURE). SURE allows service providers to make their operation systems as agile as their virtualized network and data center, providing a unified view of the network and cloud infrastructure.

What are the proof points?

Alcatel-Lucent states that it has the capacity to scale its business quickly, and that is has an end-to-end offering from an SDN Controller, NFV orchestration platform with routing, optics, and virtualized appliances such as the LTE Packet Core, and VoLTE IMS solutions. The company claims that it can leverage its size and its expertise in broadband and wireless access solutions.

Alcatel-Lucent is highly active in promoting the notion of SDN and NFV, including:

- An ecosystem of partners as integral parts of its architecture, with 50 members including 6Wind, HP, F5 Networks, Intel, RedHat, VMWare, Contextream and others.
- Deployments in various countries (including Verizon, AT&T, NTT, DT and Telefonica) and more than 30 trials.

Alcatel-Lucent says that it is differentiated by taking a holistic end-to-end approach by combining its SDN and NFV solutions with operational support systems, a broad range of network solutions, strategic partnerships and professional transformation services.

Meru Networks

Where do you fit in the SDN and/or NFV ecosystem?

Meru Networks stated that it is taking a leadership role in developing and deploying best-of-breed wireless LAN solutions that are SDN enabled. According to Meru, its solutions can integrate with any wired vendor that also supports the OpenFlow solution. This capability allows customers to manage and control their wired/wireless network as a single unified network.

What is your value add?

The Meru SDN solutions provide:

- ONF certified OpenFlow wireless network solutions;
- End-to-end application QoS enabling enforceable service-level agreements (SLAs);
- Single-pane-of glass management of the unified wired and wireless network, with policy automation;
- Support for multi-vendor solutions through the ability to mix-and-match best-of-breed solutions.

What are the proof points?

- Meru Networks is the first WLAN vendor to receive the Certificate of Conformance through the ONF OpenFlow™ Conformance Testing Program (June, 2014);
- Meru Networks is the first vendor to complete qualification with Microsoft Lync® for 802.11ac wireless networking solutions (Aug 2014);
- Meru Networks is the winner of the October SearchNetworking Network Innovation Award for its achievements in the wireless software-defined-networking (SDN) space. (November 2014).

6WIND

Where do you fit in the SDN and/or NFV ecosystem?

6WIND stated that it enables NFV by accelerating Linux based networking environments to provide over 10X network performance improvements compared to standard Linux software architectures. As a result, service providers benefit from bare metal performance in their virtual environments.

The two products that 6WIND delivers for NFV are:

Solution 1: Data Plane Acceleration using 6WINDGate packet processing software

Description: Data plane performance enhancements that enable OEMs to build accelerated applications in bare metal and virtual environments. By leveraging a fast path architecture outside of the Linux kernel, 6WINDGate is deployed transparently with no change to OpenStack, the OS, hypervisor or virtual switch. 6WINDGate delivers the following features:

- High performance Layer 2-4 packet processing software for generic servers with a choice of multicore processors including Broadcom, Cavium, Intel and EZchip/Tilera;
- Cryptographic acceleration (software and hardware acceleration for built-in or external crypto engines);
- Fast path-based data plane solution on Intel leveraging DPDK and extensions (multi-vendor 10G and 40G NICs, smart NICs and more);
- Accelerated IPsec and IKE stack supporting over 190 Gbps over tens of thousands of tunnels on Intel servers;
- Accelerated TCP/UDP stack supporting over 100 million concurrent sessions and session setup rates of 5 million sessions per second;
- High capacity firewall and NAT;
- Wide tunneling support: GTP, PPP, L2TP, GRE, MPLS, VXLAN, etc.

Virtual Network Functions (VNFs) that can be built with 6WINDGate packet processing software include: routers, firewalls, Carrier Grade NAT, IPsec Gateways, EPC, HTTP-based applications and more.

Solution 2: NFV Infrastructure using 6WIND's Virtual Accelerator

Description: The 6WIND Virtual Accelerator runs within the hypervisor domain with a hardware-independent architecture that allows new and existing VMs to be integrated quickly onto x86-based servers. As a transparent virtual infrastructure acceleration solution, 6WIND Virtual Accelerator is provided as a simple software package so that customers do not have to replace or modify existing software such as Open vSwitch (OVS), Linux, Hypervisors and OpenStack.

Features include:

- Network hardware independence for seamless hardware updates, including 10G to 40G to 100G ports;
- Wire speed performance required to enable high density, compute intensive VMs on a single server;
- Flexible virtual switching support for Open vSwitch and Linux Bridge with no modifications;

- Complete virtual networking infrastructure with VLAN, VXLAN, Virtual Routing, IP Forwarding, Filtering and NAT;
- Native Virtio support for VMs based on different OSs;
- High bandwidth for VM to VM communications required for Service Chaining;
- No modification to OpenStack for orchestration.

What is your value add?

Scalability: With 6WIND's data plane acceleration and NFV Infrastructure, performance scales linearly with the number of processor cores. This means that fewer processor cores can be used for networking tasks so that more cores can be saved for the actual VNFs. At Dell World 6WIND recently demonstrated 240 Gbps aggregate bandwidth running an IP Forwarding VM. Another demonstration showed over 200 Gbps throughput with 80% of the processing cores left to run Virtual Network Functions.

Hardware Independence: As an independent software vendor, 6WIND supports multi-vendor NICs from vendors such as Intel, Mellanox and Emulex so that there is not vendor hardware lock-in. This network hardware independence enables seamless hardware upgrades including 10G to 40G to 100G ports.

Performance: NFV is cost effective if performance can be achieved in virtual environments at least similar to physical environments. 6WIND enables 200 Gbps of virtual switching, 190 Gbps of IPsec and over 100 million concurrent TCP connections, to give a couple examples of performance that is not sacrificed with virtualization.

What are the proof points?

High Performance Virtualized SBC with Metaswitch and 6WIND

In November 2014 Metaswitch Networks announced a test with Perimeta, its virtualized session border controller (SBC), with 6WIND Virtual Accelerator for NFV Infrastructure. The background for this test is that conventional cloud environments built for IT workloads are not designed to provide the high rates of packet throughput needed to support virtualized network functions such as session border controllers. This has the effect of limiting the number of concurrent media sessions that can be supported by a virtualized SBC on a given amount of hardware.

For example, Perimeta SBC software running directly on current generation Intel architecture servers can relay about 60,000 concurrent bi-directional audio sessions using 6 CPU cores. However, the same software, running in a virtual machine in a conventional cloud configuration, using Open vSwitch (without specialized tuning) and using the same number of CPU cores can only manage 700 sessions.

By substituting 6WIND Virtual Accelerator, the results are much better. Virtual Accelerator helps increase the media capacity of a virtualized Perimeta SBC, running on 6-CPU cores, to 36,000 sessions, a more than 50 times improvement over Open vSwitch. In this configuration, 2 CPU cores are dedicated to running 6WIND Virtual Accelerator while 4 CPU cores are forwarding media. At 9,000 sessions per CPU core, the 6WIND Virtual Accelerator solution delivers 90 percent of the capacity per core of Perimeta SBC running on bare metal.

Dell

Where do you fit in the SDN and/or NFV ecosystem?

Dell stated that it enables the Open Networking Ecosystem. As Dell points out, the world has changed, the cutting edge is no longer found in proprietary solutions and closed ecosystems. Yet while open infrastructure technologies have already delivered exponential cost efficiencies and paradigm shifting innovation in some of the world's largest data centers, these technologies remain difficult to access for service providers and effectively impossible to access for most enterprises. Dell stated that it stands alone in its bold embrace of open technologies and that Dell's focus is on making the latest innovations from open ecosystems available to all consumers without vendor lock-in. Dell believes that this approach fundamentally changes the economics and accessibility of open, web-scale technologies.

What is your value add?

Dell stated that its solutions leverage open technologies with open interfaces throughout all layers and that this enables them to deliver the simplicity of vertically integrated solutions with the openness, flexibility and economics of web-scale technologies. For carriers investing in NFV, Dell offers pre-engineered NFV infrastructure bundles with validated reference architectures for leading VNF offerings, management & orchestration solutions and full support for popular Linux and OpenStack distributions without proprietary hardware or software requirements. For enterprises investing in private cloud solutions, Dell supports Microsoft, VMware and OpenStack environments equally without forcing customers into a vertically integrated & closed solutions. Dell Networking offers integrations with Microsoft, VMware, Openstack, Cloudstack, Puppet, Chef and other ecosystem solutions without additional licensing fees.

All advanced software interfaces including Perl/Python/Puppet/Chef/Shell/REST/Openflow and other API's are included in the base license for Dell Data Center switches with full support and no additional fees for use with either Dell or 3rd party management software, controllers or applications. Dell's embrace of open hardware and software ecosystems allows the company to offer the broadest and most flexible array of technology solutions with industry-leading performance, economics and efficiency.

What are the proof points?

Dell Networking has added over 3,000 new customers and continues to outpace the market in growth. Dell stated that its extensive list of available case studies with marquis customers and cutting edge use cases provides a testimony of the efficacy and performance of their solutions. Dell Networking products have received numerous awards from leading technology publications, events and analysts and have received superior ratings in performance reviews from leading independent testing firms including Miercom, The Lippis Report and others.

EMC

Where do you fit in the SDN and/or NFV ecosystem?

EMC provides data center management software that delivers comprehensive monitoring, diagnostics and Service Assurance across software-defined networks, integrating natively between virtual network infrastructure and the physical hardware, providing detailed real-time topology mapping from physical port through the tenant. These capabilities are the foundation for EMC's NFV management strategy, extending the functionality across physical and virtual network boundaries providing enterprise and service providers the tools they need to effectively manage these emerging virtual network functions across heterogeneous network infrastructure.

What is your value add?

EMC Service Assurance Suite provides complete operational visibility across storage, compute and networks providing detailed fault correlation, root cause and impact analysis across large, complex data center infrastructure. Service Assurance increases availability by providing detailed performance analysis and event correlation to address issues before service is impacted, enabling network operations teams to determine the specific root cause of network issues, minimizing any potential downtime.

What are the proof points?

In April 2014, EMC Service Assurance Suite was selected by Enterprise Management Associates as the network management product offering the best scalability in their annual Enterprise Network Availability and Monitoring System radar report.

As an additional proof point, Compucom saved over $550K in the first 12 months of operation because of 80% faster root cause analysis of system and network problems, cutting their discovery time for their 15,000 node network from 2 weeks to 30 minutes with EMC Service Assurance Suite. They also saw a 4x reduction in trouble ticket reduction in the first year after deploying the EMC solution.

Citrix

Where do you fit in the SDN and/or NFV ecosystem?

Citrix stated that it has always believed in software-based networking and offering its customers complete freedom of choice between platforms and features. Citrix claimed that its NetScaler VPX product line is the leader in the virtual ADC space and has the exact same binary as their hardware appliances. Citrix added that its virtualized products are the fastest growing products within their NetScaler product line, both in terms of revenue and net new customers and that they are positioning the NetScaler SDX as an open and elastic platform that consolidates network services into a unified service delivery layer accessible as a whole by an application through open APIs.

Citrix believes that the network needs an application control layer. SDN enables a programmable networking model that allows Citrix to disseminate deep and broad application intelligence into the network, making the network a unified Layer 2– Layer 7 intelligent application fabric. Based on that belief, Citrix stated its goal of seamlessly integrating its technology into SDN environments as an always-on, elastic service that can be consumed on demand. Towards that end, Citrix is building the NetScaler Control Center, which is a common multi-tenant platform that orchestrates NetScaler services across both physical and virtual appliances. The Control Center will allow customers to use all NetScaler appliances as an aggregate pool of capacity.

Citrix acknowledged that most vendors of L4 - L7 services have already made their solutions available as virtual appliances. They also stated their belief that advanced L4 - L7 services play a vital role in lending application intelligence to NFV environments through intelligent traffic steering between various virtualized services and enabling seamless availability, scalability, and performance of those services. These advanced L4 – L7 services can also provide the ability to integrate into the application orchestration environment as well as open APIs to drive configuration programmatically.

Citrix's view is that the core value of its products and technology should remain the same across both physical and virtual form factors. The choice of a physical appliance is primarily for performance and scalability reasons, which is generally addressed through a scale-out architecture in NFV environments which Citrix supports through its TriScale clustering technology.

What is your value add?

Citrix believes that NetScaler is very well positioned to play a critical role in the SDN value chain. Citrix stated that value for customers lies in networks having a deep understanding of applications and Citrix believes that's where NetScaler's application intelligence becomes an indispensable asset. Citrix extracts application information and they disseminate that information through the network using the programmable interfaces that SDN offers. The company believes that by tightly integrating with SDN environments they become a core part of the fabric and that they can interact with the switching layer to augment network intelligence with functionality such as application visibility, application-based QoS, advanced security and application-aware routing.

In NFV environments, NetScaler's value add goes beyond just large-scale load balancing of an operator's infrastructure. Citrix's stated that its orchestration capabilities, open APIs, and TriScale technology form the key enablers for the agility and scalability needed in environments like the Evolved Packet Core. NetScaler's native intelligence of various signaling protocols such as SIP and Diameter allows for optimization of virtualized voice and AAA services in both mobile and fixed line operator networks. Purpose built functions such as CG-NAT and NAT64 enable a seamless transition to IPV6, while NetScaler's content and front-end optimization capabilities allow providers to offer a rich end-user experience for their mobile customers. Finally, NetScaler's layer 7 intelligence and traffic steering capabilities enables intelligent chaining of virtualized services that can be customized per subscriber

Citrix is an active participant in the OpenDaylight community and is working to shape the direction of SDN by working closely with Cisco and many other industry leaders to forge innovation in the areas of Group Policy (i.e., an advanced policy abstraction model to describe all networking), OpFlex (i.e., a declarative policy protocol that enables highly scalable solutions), and Network service header (NSH) for intelligent traffic steering and service chaining.

What are the proof points?

There are a number of NFV-related Proof of Concept (POC) trials being sponsored by organizations such as the European Telecommunications Standards Institute (ETSI). In addition, there are a number of additional private trails underway. Some of these trials are focused on enabling the operator to develop expertise necessary to conduct full life-cycle management of the virtualized applications that reside between the mobile packet gateway (PGW) and the Internet—a domain commonly referred to as either the Gi-LAN (3G) or the SGi-LAN (LTE). As the predominant application in the Gi-LAN and SGi-LAN, the Citrix ByteMobile Adaptive Traffic Manager (ATM) is part of these network virtualization trials.

Citrix is partnering with operators to develop a solution that: a) is readily integrated with an operator's chosen NFV management and operations (MANO) framework; and b) meets NFV requirements such as rapid service provisioning. The Citrix ByteMobile ATM function must scale in parallel with broadband data traffic growth and an NFV implementation will enable the automated scaling of this function within the S/Gi-LAN domain. To achieve this end, Citrix offers a complete virtualized application stack that includes the virtual Adaptive Traffic Manager and the Citrix NetScaler VPX virtual application delivery controller. In preparation for expected operator demand, Citrix has conducted lab demonstrations of this application stack using both XenServer/CloudPlatform and KVM/OpenStack as hypervisor /virtual infrastructure manager.

Nuage Networks

Where do you fit in the SDN and/or NFV ecosystem?

Nuage Networks Virtualized Services Platform (VSP) is a Software Defined Networking architecture that acts as a non-disruptive overlay for all existing virtualized and non-virtualized network resources. VSP works across Cloud Management Software packages (such as OpenStack, CloudStack, and VMware), across hypervisors, across vSwitch architectures (embedded into a hypervisor or standalone as part of an Open Source platform such as OpenFlow), across legacy network gear, across converged network hardware / software approaches, across network software platforms, and across datacenters and WANs.

In contrast to controller-based SDN approaches, Nuage Networks VSP is completely hardware-independent. Platform components run in virtual machines, in hypervisors, or in Docker servers. Further, in contrast to server virtualization-based SDN approaches, Nuage Networks VSP is completely independent from hypervisor versions.

A fundamental component of Nuage Networks VSP is network virtualization to eliminate the need for applications and Virtual Machines (VMs) to deal with complexities of the physical network layer, including both datacenter and branch office WANs via the Nuage Networks Virtualized Network Services (VNS) use case. Building on the virtualization layer, replacing hardcoded addresses and relationships with intelligent network policies enables applications and VMs to move fluidly and rapidly as needed. Lastly, NFV capabilities such as Service Chaining of virtual functions enables the automation of complex configuration tasks such as defining cascading firewalls for a multi-tier web application or eliminating network appliances at the branch location.

In summary, Nuage Networks VSP occupies a unique place in the SDN market. Nuage Networks' VSP is able to seamlessly operate as an overlay on the incumbent network vendors and technologies and also virtualization and programming constructs such as Docker. By seamlessly removing all constraints in the datacenter network through the WAN with a comprehensive network policy framework, Nuage Networks VSP makes the network completely programmable and instantly available to the business applications and end users.

What is your value add

What differentiates Nuage Networks:

- Non-disruptive network virtualization solution that's agnostic to the existing network equipment and topology, choice of compute management platform or hypervisor deployed.

- Unified Fabric – from the Datacenter to the WAN: With the Nuage Networks Virtualized Network Services (VNS) the solution efficiently virtualizes and unifies the entire network fabric across datacenters and out to the very edge of the WAN within a single policy domain.

- Intelligent Automation: By providing intelligent policies that are interpreted where needed at each network end point – such as within the hypervisor, the rack switch, or the WAN edge, the Nuage Networks solution provides unique efficiencies in CapEx and OpEx as well as provide a consistent set of network and security policies across the data center and WAN environments.

- Service Provider Scale with full control: Leveraging the operating system that today runs roughly a quarter of the Internet, the Nuage Networks solution provides the scale that F500 Enterprises, major Service Providers, and Governments demand.

- Open Approach: The Nuage Networks solution is unique in simultaneously supporting any Cloud Management System (e.g. OpenStack, CloudStack, and VMware), any Hypervisor (e.g. Docker, VMware, KVM and Xen), and any networking vendor (e.g. Alcatel-Lucent, Cisco, and Juniper).

- Leading-edge Capabilities: In addition to supporting new programming constructs such as Docker, the Nuage Networks solution enables the self-service capabilities needed to both enter new markets and to compete effectively with public cloud giants.

What are the proof points

In around 18 months of sales activity, Nuage Networks has been implemented at scale within the networks of leading global companies, including financial services and healthcare companies, cloud providers, telecommunications providers, and infrastructure providers across the three key worldwide theatres (NA, EMEA and APAC).

The best proof points for any solution are when customers leverage it to create entirely new ways to do business. Select examples include:

- **New Software Defined Cloud model**: Numergy, the national cloud provider for France, has created a new architecture that will allow all network and value-added services to be software defined, based largely on Nuage Network's capabilities. See http://www.nuagenetworks.net/press-releases/numergy-selects-nuage-networks-software-defined-networking-solution-new-cloud-infrastructure/

- **New Cloud Distributed Hosting model**: A service provider in EMEA (EVONET) has created a virtual Platform Optimized Design (vPOD) architecture that provides Cloud efficiencies along with the flexibility of offering either shared or dedicated resources distributed among datacenters. Nuage Networks VSP provides the interconnection within and among all vPODs and among all datacenters. See http://vimeo.com/98173520.

- **New Cloud Service model**: OVH, the number one hosting provider in Europe, has introduced a game-changing OpenStack-as-a-Service offering with Nuage Networks VSP. See http://www.nuagenetworks.net/press-releases/ovh-sdn-nuage-networks/

- **Unified Healthcare model**: UPMC, a $10 billion integrated global health enterprise, has unified their 450 sites and 2 datacenters to provide services to 62,000 employees with Nuage Networks. See http://www.nuagenetworks.net/press-releases/upmc-selects-nuage-networks/

Pica8

Where do you fit in the SDN and/or NFV ecosystem?

Pica8 is one of the pioneers of open networking in part based on PicOS™, the first Linux-based network operating system that enables customers to easily integrate conventional networking with software-defined networking (SDN) using commodity bare metal switches. Pica8 is challenging 20 years of the traditional proprietary approach to networking by providing an open switching system, which users can personalize to meet the needs of their application environment.

As traffic demands skyrocket and data centers must scale, traditional networking has proven increasingly inefficient. Current architectures, comprised of disparate network devices, are difficult to provision and to customize. Pica8 believes that SDN resolves these challenges because it abstracts the network data plane from the control plane, enabling users to easily address all network services through myriad external programming interfaces. The result is that a company's data center network can now be customized and personalized.

PicOS provides extensive support for traditional switching and routing protocols and Linux. PicOS offers a comprehensive and flexible configuration management environment from either a Linux shell or feature rich command line interface (CLI). PicOS runs as an application on an un-modified Linux kernel. This enables familiar system administration and automation tools such as CFEngine, Chef or Puppet to run natively and seamlessly.

PicOS delivers SDN solutions through Pica8's adoption of Open-vSwitch (OVS). Pica8 can provide PicOS, switching hardware through a growing list of Hardware Ecosystem Partners, or both in a fully integrated package leveraging ONIE as part of an end-to-end data center SDN solution. Pica8 also provides a Starter Kit that Pica8 stated enables deployment in hours rather than months.

PicOS interoperates with leading network virtualization products such as VMware's NSX (Nicira), Midokura and PLUMgrid.

What is your value add?

As customers progress down the path of SDN, one thing that is clear in the early rollouts is that there are no cookie-cutter deployments. Everyone has a different application, a different use case, and a different rate of adoption. Pica8 believes that the network should be flexible and easy enough to help any customer on their journey.

To that end, Pica8 offers CrossFlow Networking, where customers get the flexibility and granularity of OpenFlow-based network policy on the same device that's running traditional Layer-2 / Layer-3 protocols for efficient packet forwarding. CrossFlow Networking users can use OpenFlow to fine tune the switching or router tables in a switch. This allows users to inject OpenFlow rules for specific applications and policies, while also preserving the networking topology that's built on tried and true Layer-2 and Layer-3 protocols.

Benefits of CrossFlow Networking:

- Save money by reducing CapEx. With CrossFlow, users don't have to purchase a different set of networking equipment for their OpenFlow implementation.

- Save time by reducing the complexity of different modes of operation between Layer-2, Layer-3 and OpenFlow.

- Deliver business logic and policy into the network by simplifying the integration of SDN into the existing network.

More and more customers are deploying SDN in new use cases and in real networks. According to Pica8, these customers are discovering that some SDN implementations have significant limitations relative to the scalability of the solution. Pica8 enables large-scale OpenFlow based networks through software innovation with PicOS™, their operating system for open switching.

Pica8 accomplishes this in part by combining the switching and routing memory in the switch. Another technique that Pica8 has implemented that enables scalability is optimizing the memory allocation across these tables to drastically increase the number of flow entries that their switches can support. Pica8 claims that they can support over 200,000 flows — enough for even the largest of networks.

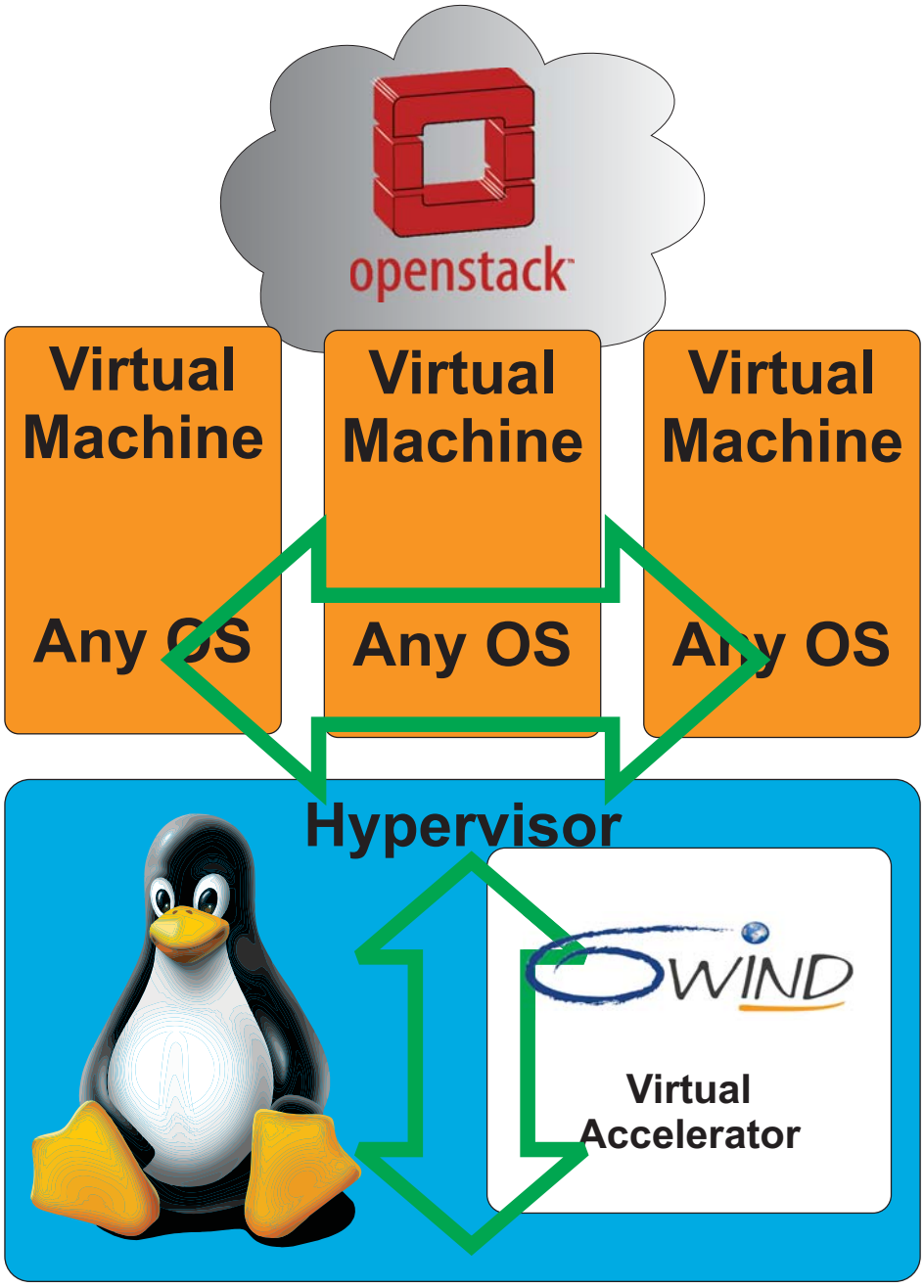
Pica8 enables seamless SDN integration with CrossFlow Networking, and supports networks of any scale with PicOS. If you want to deploy OpenFlow at scale in your production network, take a look at Pica8.

What are the proof points?

Pica8 has over 350 customers worldwide, including web services companies, global carriers, and leading research labs. Their corporate headquarters is located in Palo Alto, California, and their R&D facility is in Beijing, China, with sales and support offices worldwide.

6WIND Virtual Accelerator

Enable NFV And Virtual Networking



Transparent OpenStack orchestration support

High bandwidth for VM performance, density and communications

Complete virtual networking infrastructure

Support for Open vSwitch and Linux Bridge with no modifications

Network hardware independence for seamless hardware upgrades

6WIND

Wire Speed Virtual Switching
From Common Hardware

www.6WIND.com

Enterprise SDN and Carrier NFV: Distant Cousins or Twins?

It's not unusual to hear SDN and NFV mentioned together as part of a broad, conceptual discussion about network virtualization. But in practical use, the two represent entirely different worlds—SDN having been born out of the needs of large enterprises principally focused on data center virtualization, and NFV being embraced by telcos and communication service providers for virtualizing service delivery.

One major reason enterprise and carrier technology, including SDN and NFV, are treated as fundamentally different is that the IT goals driving enterprises and carriers are noticeably dissimilar. Add to that the historic differences in vocabulary, infrastructure, and scale between the two camps, and it's not surprising most IT professionals still think of these worlds as wholly unrelated.

But as IT evolves toward virtualization and convergence, the fact is that undeniable similarities have started to emerge. In fact, there are common infrastructural elements striking enough to raise the question: should we think of enterprise SDN and carrier NFV as distant cousins, or are they actually more like twins?

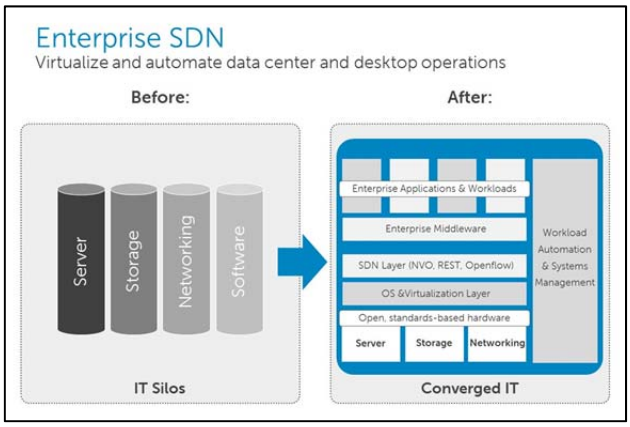
OPERATIONAL NEEDS DRIVE ENTERPRISE SDN ADOPTION

Data centers have been virtualizing server and storage functions using software and hypervisors from VMware, Microsoft Hyper-V, and Red Hat/OpenStack for years now. Virtual machines (VMs) give enterprise data centers the flexibility and agility they need to scale and operate efficiently on a day-to-day basis while also reducing the amount of physical infrastructure required.

Naturally, IT teams have begun applying the same philosophy to networking, seeking the greatest level of virtualization, automation, and programmability possible to simplify their back-end operations.

In many cases, this involves the deployment of virtual switching technology (aka vSwitches) and networking them along with physical switches to create more efficient workflows for applications and workloads.

Right now, there are three common approaches to virtualizing networking infrastructure and and introducing greater levels of programmability and automation.



1. Network virtualization overlay (NVO)
NVO stitches the data center's vSwitches together by building tunnels (VXLAN, NV-GRE, etc.) through the physical switch infrastructure, requiring no additional effort at the physical switch level.

2. Controller-based solutions (ex: Openflow)
Controller-based solutions change what takes place in the physical switch by establishing a protocol among the deployed physical switches and a controller. The controller can then be used to program all the switches in any way desired for policy control.

3. Programmable solution (ex: REST)
Other IT teams prefer to use programmatic or scripting languages, such as Puppet or Chef, to interface with their infrastructure and automate operations. Rather than a controller that speaks to multiple devices, they implement a programmatic language to define and implement policies across the infrastructure. .

Each of these approaches has arisen from challenges that are inherent in operating large-scale data centers. Meanwhile, carriers have their own reasons for virtualizing their infrastructure.

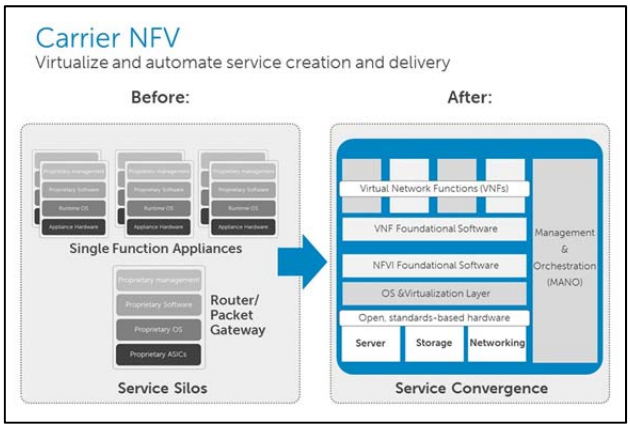
SERVICE DELIVERY GOALS DRIVE CARRIER NFV ADOPTION

Traditionally, when a carrier delivers IP services, data packets are sent from customer site or device to a carrier's router or switch, and then daisy-chained through a set of boxes performing additional service-related functions.

Just as it sounds, this process of service creation and delivery has been very physical in nature, involving many pieces of equipment, cables, and

moving parts and requiring similarly large number of staff for rollout and support.

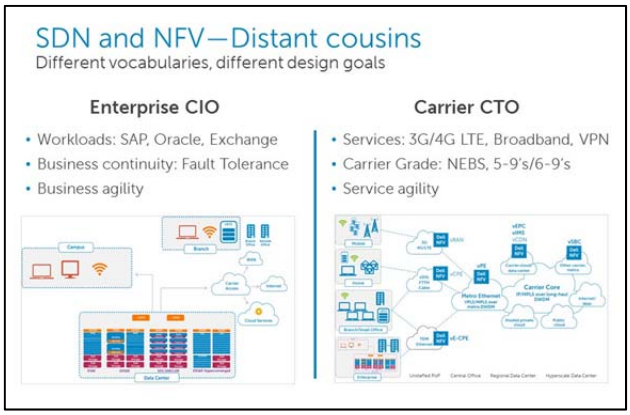
Carriers globally are now turning to virtualization and in particular NFV as a way to simplify and automate service delivery infrastructure, while also introducing greater agility for new service creation and delivery. For carriers, then, the drivers for virtualization are to improve both CAPEX and OPEX structures, making existing service delivery more cost effective, and enabling new, high-margin, services quickly.



THE LANGUAGE BARRIER

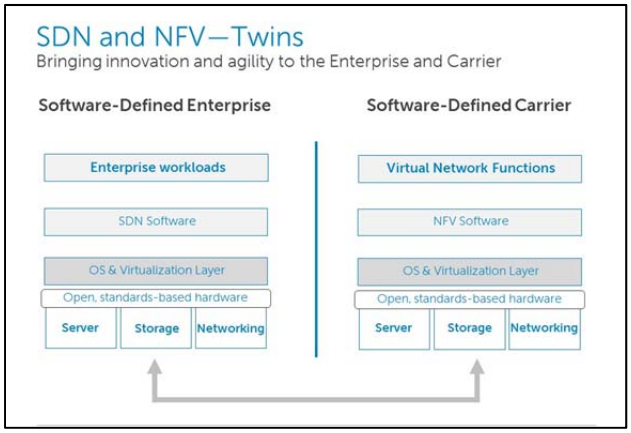
To further compound these differences, enterprise SDN and carrier NFV generally fall under the purview of different executive roles—typically the CIO at enterprises and the CTO for carriers.

There are also fundamental differences in the vocabulary surrounding each. Instead of *workloads*, carriers are concerned with *services*, and instead of *business continuity*, carriers are interested in *carrier-grade* 5-9's and 6-9's *technology*.



DISTANT COUSINS OR TWINS?

Considering this laundry list of differences, you might wonder how we can propose that enterprise SDN and carrier NFV are actually twins. It's not until you look at their technological DNA that you start to see the remarkable similarities.



As the above image shows, beneath the disparate business goals and terminology, the infrastructures that support enterprise SDN and carrier NFV are practically identical.

At its core, in both enterprise SDN and carrier NFV, exists x86 server-centric DNA that forms the foundation of the converged infrastructure for compute, storage and networking. Yet, just as twins share the same DNA but can have very different personalities based on environmental factors, enterprise SDN and carrier NFV are really only distinguishable at the application level (e.g. enterprise application vs. carrier VNF)

COMMON TRAITS FOR THE FUTURE

The full implications of this shift in perspective remain to be discovered, but a couple of opportunities immediately arise when we recognize the structural similarities of enterprise SDN and carrier NFV:

1. Carriers who are new to network virtualization can learn best practices from Web 2.0 and large enterprises who have already made significant strides in that area and apply in context..

2. Organizations that operate both production and provisioned infrastructure—enterprise-style for their own operations and carrier-style to provide services—can cross-pollenate, leveraging common technology assets, best-practices, and purchasing power.

While the vocabulary and topologies may never fully converge, the thinking can, having the potential to open new doors for positive collaboration and greater operational efficiencies. Recognizing the common traits behind enterprise SDN and carrier NFV is the first step.

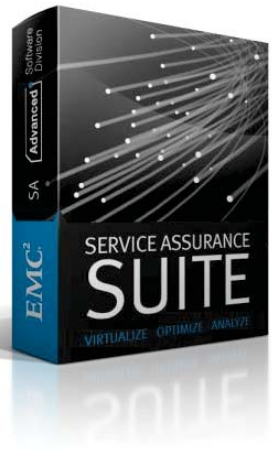
Software-Defined Networking

Are your management tools prepared?

Software-Defined Networking (SDN) and Network Virtualization (NV) are quickly becoming priorities because of the promise to dynamically manage traffic loads while lowering costs in response to changing business requirements…

Are you prepared for this evolution?

EMC understands these challenges. Designed to manage physical, virtual and cloud environments, the EMC Service Assurance Suite helps IT operations teams manage infrastructure across each phase of this evolution.



Empower your IT operations team to visualize, analyze, and optimize your service-delivery infrastructure. Learn more at www.emc.com/sa.

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, email us at asd@emc.com or call 866-438-3622.

EMC²

Extending Service Performance Management into SDN and NFV Environments

Solution Benefits

- Holistic end-to-end visibility into physical, virtual, and hybrid service delivery infrastructure
- Proactive service triage helps resolve problems in real time and assures a positive customer/user experience
- Comprehensive service performance management platform across voice, data, and video services and applications
- Ultra high scalability assures service delivery across any size of service provider and enterprise infrastructure

Problem Overview

While the strategic importance of delivering IP-based services is constantly increasing, enterprises and service providers are being pressured to find ways to deliver these services faster, with higher quality, and more cost effectively. To achieve these goals, enterprises and service providers are gradually migrating their data center workloads onto a virtual infrastructure.

To realize the full potential of virtualization CapEx and OpEx efficiencies, enterprises and service providers need a comprehensive service delivery monitoring tool which offers end-to-end visibility across physical, virtual, and hybrid environments. To be truly beneficial, the tool needs to offer proactive service triage capabilities to reduce the mean-time-to-resolution, by identifying the root cause of service degradations and outages in real time.

Unfortunately, the traditional bottom-up triage methodology based on multi-vendor silo-specific Network Performance Management (NPM) and Application Performance Management (APM) tools is ineffective. It does not offer service level triage capabilities to key organizations, and lacks the ability to provide a view of the overall service.

The bottom-up triage methodology relies on disparate sets of data collected from multiple silo-specific tools, which makes it virtually impossible to gain an end-to-end holistic view of the service performance. Furthermore, these datasets lack the insight on the interrelationships and dependencies between service delivery components and therefore inhibit service triage activities. The overall result of relying on the bottom-up triage methodology is drastically increased service unavailability, reduced quality of end-user experience and loss in worker productivity.

Solution Overview

NetScout offers efficient service triage based on pervasive end-to-end visibility across physical, virtual, and hybrid service delivery environments. The triage is performed proactively by detecting service degradations in real time and is based on one cohesive, consistent set of metadata, for service provider and enterprise services. This metadata is generated by the patented Adaptive Session Intelligence™ (ASI) technology running in both virtual environments as well as nGenius® Intelligent Data Sources, and offers meaningful and contextual view of all interrelationships and dependencies across all service delivery components in physical, virtual, and hybrid environments.

NetScout's pervasive and scalable data collection is established by instrumenting strategic access points across the service delivery infrastructure using physical and virtual appliances. The packet flow data collection and aggregation is passive and non-intrusive and can scale to collect any required volumes of data across physical, virtual, and hybrid environments.

The nGeniusONE™ Performance Management platform aggregates, correlates, and contextually analyzes the metadata gathered from the nGenius Intelligent Data Sources in both physical and virtual environments. It then creates real-time holistic views of service performance, establishes performance baselines, and facilitates service-oriented troubleshooting workflows.

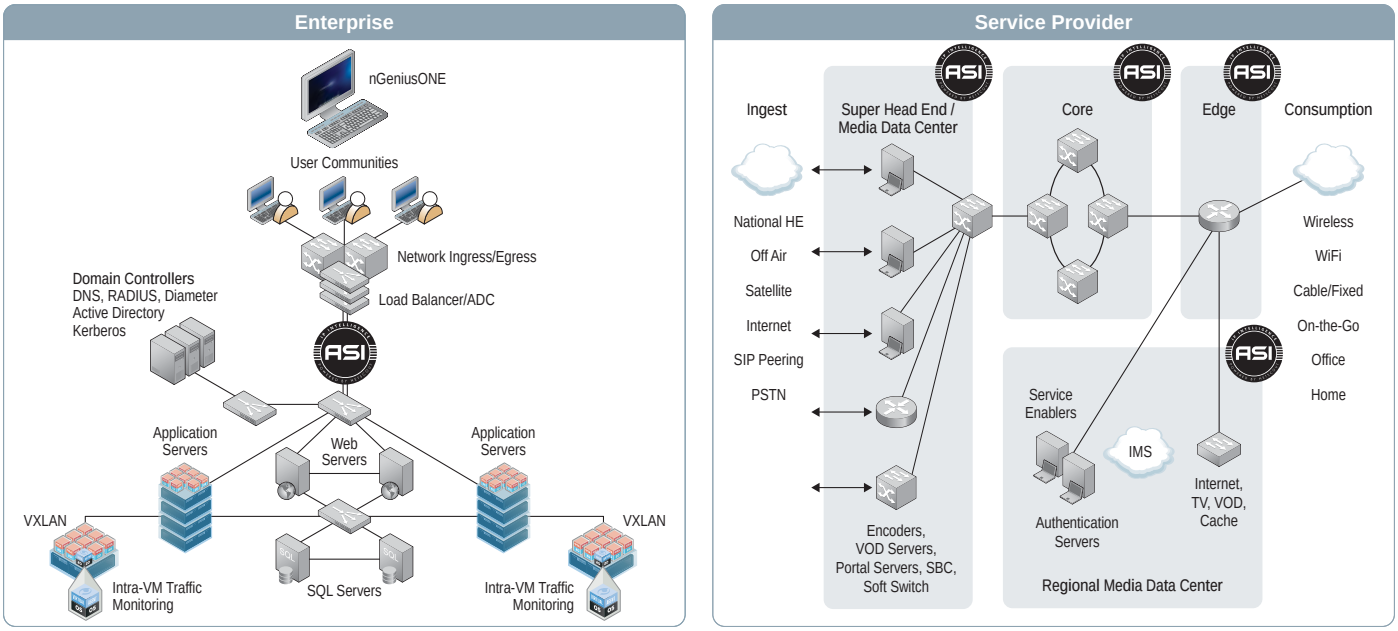


Figure 1: Service Instrumentation in Enterprise and Service Provider Environments.

Core Technologies

NetScout's unique ability to gain a pervasive end-to-end visibility into the service delivery environment, and offer proactive service triage is attributed to the following architectural principles and technologies:

- Utilize Packet Flow Data
- Provide Scalable Packet Flow Access
- Adaptive Session Intelligence (ASI)

Utilize Packet Flow Data

NetScout uses packet flow data as the foundation for generating highly scalable metadata that enables a comprehensive real time and historic view of all service components including physical and virtual networks, n-tier applications, workloads, protocols, servers, databases, users, and devices.

Provide Scalable Packet Flow Access

NetScout physical and virtual TAP network monitoring devices provide comprehensive and reliable access to packet flow data and establish strategic service visibility points across the entire service delivery infrastructure. The nGenius Packet Flow Switches (PFS) filter, aggregate, and distribute the targeted data to the nGenius Intelligent Data Sources in a transparent, selective, and efficient manner.

Adaptive Session Intelligence (ASI)

ASI is patented technology which uses a rich packet-flow data Deep Packet Inspection (DPI) engine to generate highly scalable metadata that enables a comprehensive real time and historic view of service, network, application, and server performance. This powerful deep packet inspection and data mining engine runs on nGenius Intelligent Data Sources, generating metadata based upon actual session traffic in real time as the packets cross physical or virtual links. The generated metadata provides important metrics such as application traffic volumes, application server response times, server throughputs, aggregate error counts, error codes specific to application servers and domain, as well as other data related to network and application performance. The ASI technology is the foundation of a highly scalable service delivery monitoring architecture which seamlessly collects, normalizes, correlates, and contextually analyzes data for all business services.

Service Delivery Monitoring in SDN Environments

NetScout has partnered with VMware, the global leader in virtualization and cloud infrastructure, to provide service delivery monitoring solutions in VMware NSX™ environments. These solutions enable NetScout to gain full visibility into applications traversing NSX environments in the following use cases:

- **Traffic between the VMs on the same hypervisor** is monitored by embedding NetScout's ASI patented technology into a virtual machine (VM) probe, which resides on the same hypervisor as the monitored VMs. NetScout's VM either analyzes the intra-VM traffic in a self-contained virtualized probe mode or redirects the traffic to an external nGenius Intelligent Data Source for analysis.
- **Traffic between VMs that reside in different hypervisors** is monitored by the nGenius Intelligent Data Sources that decode the VXLAN encapsulation and access the original packet flow data between the VMs.
- **Multi-tier East-West and North-South Data Center traffic** is monitored by collecting data from a combination of multi-tier physical and virtual service delivery environments, correlating, and contextually analyzing all the interrelationships and dependencies across all monitored service delivery components. These include n-tier applications, workloads, protocols, servers, databases, users, and devices.

Solution Benefits

NetScout's ability to provide end-to-end visibility into multi-tier physical, virtual, and hybrid service delivery environments combined with proactive service triage, helps address the key problems associated with silo-specific, component-based, bottom-up performance management approaches.

Attribute	Bottom-Up Triage Problems	NetScout's Solution	IT Benefits
End-to-End Visibility	• Point visibility into individual service delivery components from a variety of multi-vendor silo-specific tools. Lacks the necessary insight into interrelationships of service delivery components.	• Holistic end-to-end visibility into service delivery infrastructure using one cohesive, consistent set of data, for service provider and enterprise services delivered in physical and virtual environments.	• Optimize experience of user communities and customers. • Comprehensive solution from a single vendor. • Full visibility into services running in physical, virtual, and hybrid environments.
Effective Service Triage	• Reactive and time consuming triage results in poor user experience, and extended service downtime impacting multiple users.	• Proactive service triage helps resolve service degradation in real time, before a large number of users are impacted.	• Increase service uptime and end-user productivity. • Support more services with existing IT resources. • Reduce time wasted in war rooms.
Scalability	• Lacks scalability required to assure delivery of modern business services for service providers and enterprises.	• Scales to assure service delivery across any size of service provider and enterprise infrastructure.	• Optimize your investment in performance management by gradually expanding the solution over time.

About NetScout Systems, Inc.

NetScout Systems, Inc. (NASDAQ:NTCT) is the market leader in application and network performance management solutions that enable enterprise and service provider organizations to assure the quality of the user experience for business and mobile services. Used by 92 percent of Fortune 100 organizations and more than 165 service providers worldwide, NetScout's technology helps these organizations proactively manage service delivery and identify emerging performance problems, helping to quickly resolve issues that cause business disruptions or negatively impact users of information technology. For more information about NetScout, visit www.netscout.com.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by
Webtorials
Editorial/Analyst
Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
Steven Taylor

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.