The 2016 Guide to SDN and NFV

Part 4: Network Functions Virtualization (NFV): A Status Update

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

Platinum Sponsors:

A10®

CISCO

Hewlett Packard
Enterprise

MASERGY
Performance Beyond Expectations

NETSCOUT™
Guardians of the Connected World

Sonus®

Gold Sponsors:

radware

SevOne

Produced by:

Webtorials

Table of Contents

Introduction

Over the last couple of years the hottest topics in networking have been Software Defined Networking (SDN) and Network Functions 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 2016 Guide to SDN & NFV** (The Guide) are to eliminate the confusion that surrounds SDN and NFV and to accelerate the analysis and potential adoption of these new architectural approaches.

The Guide will be published both in its entirety and in a serial fashion. This document is the fourth of the serial publications. It will focus on providing a status update on the development and adoption of NFV. Below is a listing of all of the publications that comprise The Guide:

1. A SDN Status Update
2. The Use Cases and Business Case for SDN
3. The Operational Impediments to Implementing SDN
4. A NFV Status Update
5. Architectural Considerations and Use Cases for NFV
6. The Operational Impediments to Implementing NFV
7. The SDN and NFV Ecosystem
8. An Executive Summary of The Guide

The Guide is based in part on *The 2015 Guide to SDN and NFV* (The 2015 Guide). To limit the size of The Guide, some of the introductory material, such as a description of the basic SDN architecture that was contained in The 2015 Guide has been eliminated. The 2015 Guide, however, is still available online.

The Guide contains the results of a survey that was distributed in December 2015 and January 2016. Throughout The Guide the 144 network professionals who completed the survey will be referred to as The Survey Respondents.

The Relevance of NFV to Enterprise Organizations

The conventional wisdom has been that Network Functions Virtualization (NFV) is associated exclusively with Communications Service Providers (CSPs). Part of the reason for that is the key role that the European Telecommunications Standards Institute (ETSI) has played in the development of NFV. For example, roughly three years ago an Industry Specifications Group (ISG) for Network Functions Virtualization (NFV ISG) was formed under the auspices of the European Telecommunications Standards Institute (ETSI NFV ISG). While the membership has evolved significantly, the initial members of the ETSI NFV ISG were all CSPs such as AT&T, Deutsche Telekom and NTT.

Table 1 contains examples of functions that the ETSI NFV ISG believes can be virtualized.

Table 1: Potential Functions to be Virtualized

Network Element	Function
Switching elements	Broadband network gateways, carrier grade Network Address Translation (NAT), routers
Mobile network nodes	Home Location Register/Home Subscriber Server, gateway, GPRS support node, radio network controller, various node B functions
Customer premise equipment	Home routers, set-top boxes
Tunneling gateway elements	IPSec/SSL virtual private network gateways
Traffic analysis	Deep packet inspection (DPI), quality of experience measurement
Assurance	Service assurance, service level agreement (SLA) monitoring, testing and diagnostics
Signaling	Session border controllers, IP Multimedia Subsystem components
Control plane/access functions	AAA servers, policy control and charging platforms
Application optimization	Content delivery networks, cache servers, load balancers, accelerators
Security	Firewalls, virus scanners, intrusion detection systems, spam protection

Given the leadership role that ETSI is playing combined with the interest that they have in virtualizing functionality such as broadband network gateways and radio network controllers which has no general applicability in enterprise networks, it is easy to see why some people associate NFV strictly with CSPs.

However, while CSPs typically have a broader range of functionality that they are interested in virtualizing than do enterprises, enterprise IT organizations have been implementing virtualized functionality for several years; e.g., virtualized WAN optimization controllers and virtualized Application Delivery Controllers. While ETSI champions the interest that CSPs have with virtualizing network functions, the Open Networking User Group (ONUG) is one of the organizations that has emerged to champion the corresponding interest that enterprises have. ONUG was founded in 2012 and unlike ETSI its members are primarily enterprise companies such as Fidelity Investments, Citigroup and FedEx. In a white paper entitled *Open Networking Challenges and Opportunities*, the group discussed the cost and complexity of managing a large number of Layer 4 - 7 network appliances from different vendors with different management tools. The appliances they mentioned were:

- Server load balancers and application delivery controllers;
- WAN optimization;
- Firewalls;
- SSL/IPSec VPNs and Intrusion Detection and Prevention Systems.

In that white paper ONUG coined the phrase *Network Services Virtualization* (NSV) to refer to the virtualization of functions such as the ones listed above. The paper also stated that the NSV use case "Seeks to leverage the flexibility and low costs of commodity servers to establish a scale-out pooling of virtual and physical appliances, which can be put to use servicing applications." ONUG went on to say "As each Layer 4 - 7 function is virtualized in software, it provides the following benefits:

- Lower CAPEX costs (approximately 30 percent less);
- Rapid service provisioning;
- Reduced risk through service distribution;
- Eased management and reduced operational costs;
- Consistent policies across different Layer 4-7 services and across data center, campus, and WAN networks;
- Programmatic control and ability to offer network functions as a service to developers.

Other potential benefits of NSV include the ability for IT business leaders to deliver on-demand or self-service IT delivery to business unit managers."

There clearly are differences between what ETSI is trying to accomplish with NFV and what ONUG is trying to accomplish with NSV. As mentioned, CSPs hope to virtualize some functionality that few if any enterprise organizations implement and their need for scale far surpasses what is needed by the vast majority of enterprise organizations. In addition, CSPs are notably more likely to have a requirement to link the usage of virtualized network functions to their billing systems than do enterprise organizations. However, if you change at most a few words in how ONUG describes the NSV use case it sounds exactly like what ETSI and others are trying to achieve with NFV. In addition, if you look at the list of appliances mentioned in the ONUG paper, they are all contained in Table 1.

To test the conventional wisdom about the applicability of NFV, the survey respondents were asked to indicate their view of the relevance of NFV to an enterprise IT architecture. Their responses are shown in **Table 2**.

Table 2: Relevance of NFV to Enterprises

Applicability	% of Respondents
Very Significant	10%
Significant	42%
Moderate	15%
Some	13%
None	1%
Don't know/NA	17%
Other	1%

Half of IT professionals believe that NFV has either significant or very significant relevance to enterprise IT architectures.

The bottom line is that conceptually NFV and NSV have far more points of commonality than differences and the perceived relevance of NFV to enterprises is reflected in **Table 2**. As a result of these factors, throughout The Guide, the acronym *NFV* will be used to discuss the virtualization of network functions, whether those functions are used by CSPs or enterprise organizations or both.

The Relationship between SDN and NFV

The conventional wisdom has been that SDN and NFV were separate initiatives which could evolve independently of each other. However, in 2014 the Open Networking Foundation (ONF) and the ETSI NFV ISG announced the signing of a Memorandum of Understanding (MOU). As part of the announcement of the MOU, the ONF and ETSI stated that "Together the organizations will explore the application of SDN configuration and control protocols as the base for the network infrastructure supporting NFV, and conversely the possibilities that NFV opens for virtualizing the forwarding plane functions."

As part of the announcement, the ONF released a document entitled the *OpenFlow-enabled SDN and NFV Solution Brief*. That document discussed how OpenFlow-enabled SDN can meet the need for automated, open, and programmable network connectivity to support some of the ETSI-defined use cases such as *Network Functions Virtualization Infrastructure as a Service* and *Virtual Network Function Forwarding Graph*.

In a white paper ETSI expressed their belief that NFV and SDN are highly complementary efforts. The ETSI view is that both efforts are seeking to leverage virtualization and software-based architectures to make network infrastructures more cost-effective and more agile in their ability to accommodate the dynamic nature of the workflows demanded by applications and end users. While NFV can be implemented using a non-SDN infrastructure, the ETSI vision is that NFV and SDN will increasingly be intertwined into a broad, unified software-based networking paradigm based on the ability to abstract and programmatically control network resources.

Some of the ways that ETSI believes that NFV and SDN complement each other include:

- The SDN controller fits well into the broader concept of a network controller in an NFV-Infrastructure (NFVI) network domain as defined in ETSI’s NFV architectural framework.

- SDN can play a significant role in the orchestration of the NFV Infrastructure resources, both physical and virtual, enabling functionality such as provisioning, configuration of network connectivity, bandwidth allocation, automation of operations, monitoring, security, and policy control.

- SDN can provide the network virtualization required to support multi-tenant NFVIs.

- Forwarding Graphs can be implemented using the SDN controller to provide automated provisioning of service chains while ensuring strong and consistent implementation of security and other policies.

- The SDN controller can be run as a virtual network function (VNF), possibly as part of a service chain including other VNFs. For example, applications and services originally developed to run on the SDN controller could also be implemented as separate VNFs.

To test the conventional wisdom, the survey respondents were asked to indicate the relationship that their company sees between SDN and NFV and they were allowed to check all that applied. Their answers are shown in **Table 3**.

Table 3: Perceived Relationship between SDN and NFV

Relationship	% of Respondents
They are totally independent activities	8%
They are complementary activities in that each can proceed without the other but the value of each activity may be enhanced by the other activity.	65%
In at least some instances, NFV requires SDN	17%
In at least some instances, SDN requires NFV	12%
Don’t know	18%

Some of the conclusions that can be drawn from the data in **Table 3** are:

The vast majority of IT organizations believe that SDN and NFV are complimentary activities

Only a small percentage of IT organizations believe that SDN and NFV are totally independent activities

The Adoption of NFV

Extent of NFV Adoption

The Survey Respondents were given a set of alternatives and were asked to indicate the alternatives that described their company's current approach to implementing NFV. Their responses are shown in **Table 4**.

Table 4: Current Approaches to Implementing NFV

Approach to Implementing NFV	% of Respondents
We are currently actively analyzing the potential value that NFV offers	25%
We will likely analyze NFV sometime in the next year	24%
We are currently actively analyzing vendors' NFV strategies and offerings	23%
We currently are running NFV either in a lab or in a limited trial	18%
We have not made any analysis of NFV	18%
We expect that within a year that we will be running NFV either in a lab or in a limited trial	17%
We currently are running NFV somewhere in our production network	14%
We looked at NFV and decided to not do anything with NFV over the next year	8%
We expect that within a year that we will be running NFV somewhere in our production network	7%
Other	7%

The data in **Table 4** indicates:

While only a modest number of IT organizations have implemented NFV in a production network, a large percentage of IT organizations are currently in varying stages of analyzing NFV.

The Survey Respondents were asked to indicate the primary factor that is driving their company's interest in NFV. Their responses are shown in **Table 5.**

Table 5: Factors Driving NFV

Factor	% of Respondents
Reduce the time to deploy new services	26%
Greater management flexibility	16%
Better customer experience	14%
Reduce OPEX	11%
Reduce CAPEX	10%
Better network performance	9%
No driver	9%
Other	6%

The data in **Table 5** indicates:

By a wide margin, the primary factor driving interest in NFV is the reduction in the time it takes to deploy new services.

The Survey Respondents were also asked to indicate the three biggest inhibitors to their company broadly adopting NFV sometime in the next two years. Their responses are shown in **Table 6.**

Table 6: Factors Inhibiting NFV

Inhibitor	% of Respondents
The lack of a compelling business case	29%
Concerns about how we would do end-to-end service provisioning that includes physical and virtual resources and which may cross multiple partners' domains	23%
Concerns about security vulnerabilities	23%
The immaturity of the current products	22%
The need to significantly reskill our employee base	22%
The need for sophisticated orchestration capabilities	16%
The immaturity of the enabling technologies	15%
The need to make significant cultural changes in order to fully realize NFV's promise	13%
The difficulty of doing end-to-end service management	12%
The need to make significant organizational changes in order to fully realize NFV's promise	11%
The need to implement a new generation of agile OSS/BSS	10%
The confusion and lack of definition in terms of vendors' strategies	9%
No inhibitors to implementing NFV	9%
Other technology and/or business priorities	8%
The lack of a critical mass of organizations that have deployed NFV	8%
Concerns about how we would evolve from a POC to broad deployment	8%
The time it will take for standards to be developed and implemented	7%
Other	6%
The reluctance on the part of some of our suppliers to embrace a software model	2%
The requirement to make significant changes to our procurement processes	1%

The data in **Table 6** indicates:

The biggest inhibitors to the broad adoption of NFV are:

- ***The lack of a compelling business case;***
- ***Concerns about end-to-end service provisioning;***
- ***Concerns about security vulnerabilities;***
- ***The immaturity of the current products;***
- ***The need to significantly reskill our employee base.***

The Survey Respondents were also asked to indicate how long it would be before their organization had virtualized 25% of its L4 – L7 functionality such as optimization and security appliances. Their responses are shown in **Table 7.**

Table 7: Time Frame for Deployment

Time Frame	% of Respondents
Already have	7%
1 – 2 years	30%
3 – 4 years	32%
5 – 6 years	6%
7 or more years	1%
Don’t know/ Not Applicable	24%

The data in **Table 7** indicates that:

Within a few years, the majority of IT organizations are likely to have made a significant deployment of virtualized L4 – L7 functionality.

Industry Organizations Driving the Evolution of SDN and NFV

Although there is some overlap, the organizations driving the development of SDN and NFV fit into three broad classes. One class is industry groups such as the ONF and ETSI. This class of organization develops use cases, best practices, architectures, frameworks, APIs, vocabulary and POCs. When ETSI establishes an Industry Specification Group (ISG) such as the one it established for NFV (ETSI NFV ISG), the ISG has a two year life cycle. After that they either establish a charter for a new phase of the ISG or they go away. This approach tends to make an ISG very action oriented.

Another group driving the evolution of SDN and NFV are Standards Developing Organizations (SDOs) such as the IETF and the Alliance for Telecommunications Industry Solutions (ATIS). Unlike an ETSI ISG, a SDO typically doesn't have a predetermined life span. As such, they tend to move slowly and focus on technical elegance. There is no doubt that in some situations that technical elegance provides value. There is also no doubt that in many situations the pursuit of technical elegance results in a process that isn't very agile. The IETF is an example of a SDO that is attempting to become more agile as evidenced of the hackfests that it recently conducted.

The third group driving the evolution of NFV is the open source community including organizations such as OpenDaylight (ODL), ON.Lab and the Open Platform for NFV (OPNFV), all three of which are member of the Linux Foundation. The general charter of this class of organization is captured in the initial announcement that the Linux Foundation made about OPNFV. As part of the announcement the Linux Foundation declared that OPNFV will establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and ensure consistency, performance and interoperability among multiple open source components. The Foundation also stated that because multiple open source NFV building blocks already exist, OPNFV will work with upstream projects to coordinate continuous integration and testing while filling development gaps. The bottom line being these groups are developing platforms that over time will become quite feature-rich, and many companies are likely to build their offerings based on these platforms.

It is unclear how the relationship between the SDOs and the open source community will develop. One option is that after a group such as the OPNFV has make progress on creating an open source reference platform for NFV, that one or more SDOs will establish working groups to create standards for some of the key tasks that are part of the reference platform. However, since SDO working groups have historically taken years to create new standards, another option is that whatever functionality is part of the reference platform will become defacto standards.

In order to understand the conventional wisdom relative to the value provided by SDO and open source communities, The Survey Respondents were also asked to indicate the type of organization they thought would have greater impact on the evolution of NFV – SDOs such as the IETF or open source organizations such as OPNFV. Their responses are shown in **Table 8**.

Table 8: Influence of SDOs and Open Source Communities	
Prime Influencer	**% of Respondents**
Open Source Communities	49%
SDOs	27%
Don't know	24%

By almost a 2:1 ratio, IT professionals think that open source communities will have more of an impact on the evolution of NFV than SDOs will.

Key members of the SDN and NFV community

The role that ETSI plays in the evolution of SDN and NFV was described previously in this chapter of The Guide and will be elaborated on in the next chapter (Architectural Considerations and Use Cases for NFV). The role played by OpenDaylight, On.Lab and the ONF was described in Chapter 1 of The Guide (A SDN Status Update). Below is a description of some of the other key organizations driving the evolution of SDN and NFV.

The OpenSwitch Community

In October 2015 the OpenSwitch community was announced. The goal of the community is to develop an open source network operating system (NOS). While there are currently other open source NOSs available, the founders of the OpenSwitch community believe that none of the existing open source NOSs met the requirement for a programmable and scalable NOS that also allows developers to access the source code, rather than just access the NOS through APIs.

Developers and users can download the newly released Linux-based open source NOS, which includes the following functionality and characteristics:

- A fully featured NOS with L2/L3 protocol support;
- An open source cloud database for persistent and ephemeral configuration;
- A system database to support all inter-module communication;
- A universal API approach including CLI, REST, Puppet/Chef, Ansible

The OpenStack Foundation

OpenStack is a cloud computing orchestration project offering free open source Orchestrator software released under the terms of the Apache License. The project is managed by the OpenStack Foundation, a non-profit corporate entity established in September 2012 to promote OpenStack software and its community. Apache CloudStack is another open source Apache Licensed orchestration system. Eucalyptus is a third open source orchestrator with tight technical ties to Amazon Web Services (AWS).

Open Platform for NFV (OPNFV)

As mentioned, the OPNFV mission is to establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and ensure consistency, performance and interoperability among multiple open source components. In June 2015 OPNFV had their first software release, code named Arno. Arno enables end users to deploy virtual network functions (VNFs) on the platform to test functionality and performance. Arno also reflects OPNFV's commitment to testing by providing an automated toolchain that allows upstream projects to do automatic builds and verification as they develop independently.

TM Forum

In 2014 the TM Forum announced its Zero-touch Orchestration, Operations and Management (ZOOM) project. According to the Forum, the goal of Zoom is to define a vision of the new virtualized operations environment and a management architecture based on the seamless interaction between physical and virtual components that can easily and dynamically assemble personalized services. In addition, the TM Forum has also been active with a wide range of companies to create what the TM Forum refers to as Catalysts, which are short-term collaborative projects led by members of Forum that address operational and systems challenges.

Internet Engineering Task Force (IETF)

Although their efforts are just getting started, the IETF can be expected to play a significant role in the evolution of standards for SDN and NFV. For example, the IETF Service Function Chaining (SFC) Work Group (WG) currently has a number of Internet drafts on the topic of delivering traffic along predefined logical paths incorporating a number of service functions. As described in one of those Internet drafts, the basic concept of SFC is similar to ETSI NFV ISG's Virtualized Network Function (VNF)-Forwarding Graphs.

The Alliance for Telecommunications Industry Solutions (ATIS)

ATIS is a standards organization that develops technical and operational standards and solutions for the Information and communications technology (ICT) industry. ATIS has launched an NFV Forum to make contributions to NFV and SDN technologies. Phase I of the NFV Forum work program includes virtual network operator capabilities as well as other high priority use cases. The forum will focus on technical requirements, a catalog of needed capabilities, and the service chaining necessary for a third party service provider or enterprise to integrate NFVs into a business application. This process will result in creation of specifications that are complementary with existing industry work with an emphasis on facilitating inter-provider NFV. The forum will also engage relevant open source activities and agile software methodologies for the implementation of these capabilities.

The 3rd Generation Partnership Project (3GPP)

3GPP is a collaboration between groups of telecommunications associations. While its initial focus was on 3G as well as the completion of the first LTE and the EPC specifications, 3GPP has evolved to become the focal point for mobile systems beyond 3G. 3GPP standardization encompasses Radio, Core Network, and Service architecture. A number of functions defined in the 3GPP architecture are candidates for implementation as NFVs and have been identified as such in ETSI uses case descriptions. As a result, the 3GPP Telecom Management working group will produce a study Item on the management of 3GPP NFVs. 3GPP is also considering how the work in the ETSI NFV ISG might impact 3GPP at the architecture and system level.

The Metro Ethernet Forum (MEF)

The MEF is the defining body for the global market for Carrier Ethernet (CE). MEF's flagship work is CE 2.0, including specifications and related certification programs for services, equipment and professionals. MEF has announced a new Third Network vision that delivers Internet-like agility and ubiquity with CE 2.0-like performance and security. The Third Network vision is based upon the concept of Network as a Service (NaaS) incorporating service orchestration functions, APIs, a protocol independent NaaS information model and service definitions.

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.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.

AUTOMATE YOUR CLOUD WITH aCLOUD SERVICES ARCHITECTURE

Integrate dynamic services into your Cloud Data Center

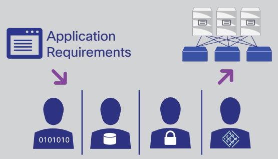
www.a10networks.com

Why Choose Application Centric Infrastructure (ACI)?

Application Deployment at the Speed of Business

Without ACI

New Application



IT administrators work in silos.

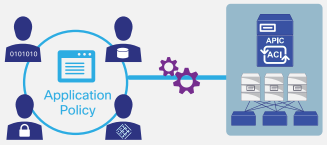
Weeks

There is no shared architectural model.

With ACI

New Application

Simpler



Faster

IT admins work at the application level.

Hours

Efficient

Shared model for policy automation.

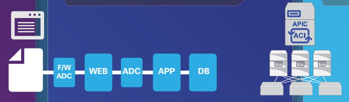
ACI cuts deployment time and effort.

Optimal Design

Application Policy

- Connectivity
- Reliability
- Compliance
- Performance
- L4-L7 Services
- Utilization

Faster Deployment



Application Network Profile

- Test
- Certify
- Adapt
- Provision

Simplified Operations

Application Topology

- Monitor
- Troubleshoot
- Optimize
- Scale Out

What does ACI deliver?

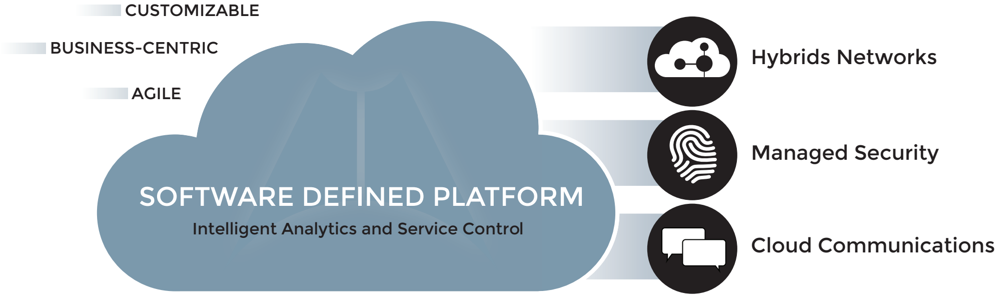
- Automation and Visibility
- Performance and Scale
- Security
- Openness

Redefine the Power of IT with ACI

Learn more at www.cisco.com/go/aci

Masergy’s Software Defined Platform Delivers the Flexibility Enterprises Require

The enterprise WAN is fast becoming the source of serious innovation. Consider it the central nervous system of corporations and their ability to support even the most advanced and demanding business-critical applications. A modern network should be agile enough to adapt to your rapidly changing business needs.



This WAN innovation is being enabled by a Software Defined Networking (SDN) architecture, which enables administrators to rapidly change configurations as performance requirements demand.

Putting theory into practice, Masergy’s Software Defined Platform accelerates IT transformation by providing the foundation for an open, automated and programmable network fabric. Our Software Defined Platform is the foundation for our three essential solutions: hybrid networking, managed security and cloud communications.

SDN enables us to build intelligent analytics, automation and service control into all of our solutions.

Here are some of the many benefits of our Software Defined Platform:

- A high-availability, highly resilient hybrid network environment that provides an optimal client and application experience
- A secure, hybrid WAN architecture that permits dynamic traffic engineering across both private and public domains, delivering seamless performance and consistent manageability
- Administrators are afforded full visibility into business-critical applications and the ability to prioritize traffic based on performance, security and business policy needs
- Remote sites and branch offices can be added to the corporate network quickly and with little-to-no on-site administration

SOFTWARE-DEFINED SOLUTIONS THAT ADAPT TO THE DEMANDS OF YOUR BUSINESS

VIRTUALIZATION

Network Function Virtualization (NFV) as a central tenant of our Software Defined Platform. NFV is poised to transform the world of networking as part of a larger shift from rigid, legacy networks where hardware and software are proprietary and tightly integrated, to modern networks that are software-driven and programmable. This gives network architects and administrators a new way to design, deploy and manage network capabilities.

Masergy has implemented NFV in its recently introduced Managed Network Functions f(n). We offer a family of fully managed, distributed network functions that can be delivered in the way that best suits your needs, whether that's on premises, in the cloud, or virtualized via software.

The solution offers Virtual Functions f(n) that lets companies add routing and firewall capabilities in software on their existing Masergy network interface device, eliminating the need for proprietary network appliances and on-site administration.

Our Premise Function f(n), is a complete lifecycle management solution for enterprises, which covers essential on-premises networking functions, including routers, firewalls and session-border controllers. And a third component, Cloud Functions f(n), help companies deliver essential network functions as cloud services over the Masergy network.

> *"Masergy was able to custom design our hybrid network to meet our unique application performance requirements. It's outcome-based approach and ongoing superior support have convinced us we selected the right partner for our needs."*
>
> Patrick Tisdale, CIO – McKenna, Long & Aldridge, LLP

FLEXIBLE BY DESIGN

SDN transforms enterprise networks into modular, scalable assets that can be assembled and rearranged as business needs require. It also reduces IT complexity through automation.

Masergy is helping customers accelerate their IT transformation efforts, providing the foundation for an open, automated and programmable environment. This, in turn, frees up IT staff to focus on strategic, business-driven innovations and less time "keeping the lights on."

MASERGY
Performance Beyond Expecations

For more information, please visit https://www.masergy.com

Compared with legacy approaches, Masergy's NFV offers three compelling advantages:

1. **Extended Flexibility:** Masergy's Managed Functions f(n) gives enterprises complete control over their distributed network resources–plus the ability to scale up new services and decommission outmoded network capabilities as business needs change.
2. **Rapid Deployment:** NFV lets organizations add, remove, configure and modify network services in real time. Rather than ordering and shipping network appliances to branch offices and remote locations, it lets you take advantage of innovative new services and deploy them over your network via software updates.
3. **Lower Costs:** Our managed Network Functions f(n) reduces CAPEX because an organization no longer needs to purchase specialized hardware in many instances. And OPEX drops because of the way NFV lowers the need for dedicated hardware, support personnel and equipment maintenance.

Contact us for a free consultation.

Corporate Headquarters (USA):
2740 North Dallas Parkway, Suite 260
Plano, TX 75093 USA
Phone: +1 (214) 442-5700
Fax: +1 (214) 442-5756

European Headquarters (UK):
29 Finsbury Circus
Salisbury House 5th Floor
London, EC2M 5QQ UK
Phone: +44 (0) 207 173 6900
Fax: +44 (0) 207 173 6899

NETSCOUT

Extending Service Assurance into SDN and NFV Environments

SOLUTION BENEFITS

NETSCOUT's Adaptive Service Intelligence™ (ASI) technology empowers enterprises and service providers to fully realize the benefits of SDN and NFV CapEx and OpEx efficiencies by reducing deployment risk.

- Accelerates migration to virtualized infrastructures with confidence.
- Provides service visibility without compromising user and customer experience.
- Protects and enhances performance of traditional, non-SDN/NFV, deployments.

Solution Core Functionality

NETSCOUT's nGeniusONE™ Service Assurance platform and ASI technology deliver real-time, actionable traffic-based intelligence capabilities.

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

Challenges

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 lower cost. 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 SDN and NFV CapEx and OpEx efficiencies, enterprises and service providers need a comprehensive service delivery monitoring capability which offers end-to-end visibility across physical, virtual, and hybrid environments. To be truly beneficial, the tool needs to offer rapid service triage capabilities to reduce the mean time to resolution (MTTR), 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 IT and Operations teams, and lacks the ability to provide an end-to-end 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 disparate 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 significantly increased mean time to resolution, drastically extended service outages, reduced quality of end-user experience or loss in worker productivity.

Solution Overview

NETSCOUT® offers rapid 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 using one cohesive, consistent set of metadata, based on packet flow data, for service provider and enterprise services. This metadata is generated by the patented Adaptive Service Intelligence technology running on NETSCOUT's physical and virtual 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 points across the service delivery infrastructure using physical and virtual appliances. The packet flow data collection and aggregation is passive and noninstrusive and can scale to collect any required volumes of data across physical, virtual, and hybrid environments.

The nGeniusONE Service Assurance platform aggregates, correlates, and contextually analyzes the metadata gathered from NETSCOUT's physical and virtual Intelligent Data Sources. It then creates real-time holistic views of service performance, establishes performance baselines, and facilitates service-oriented troubleshooting workflows.

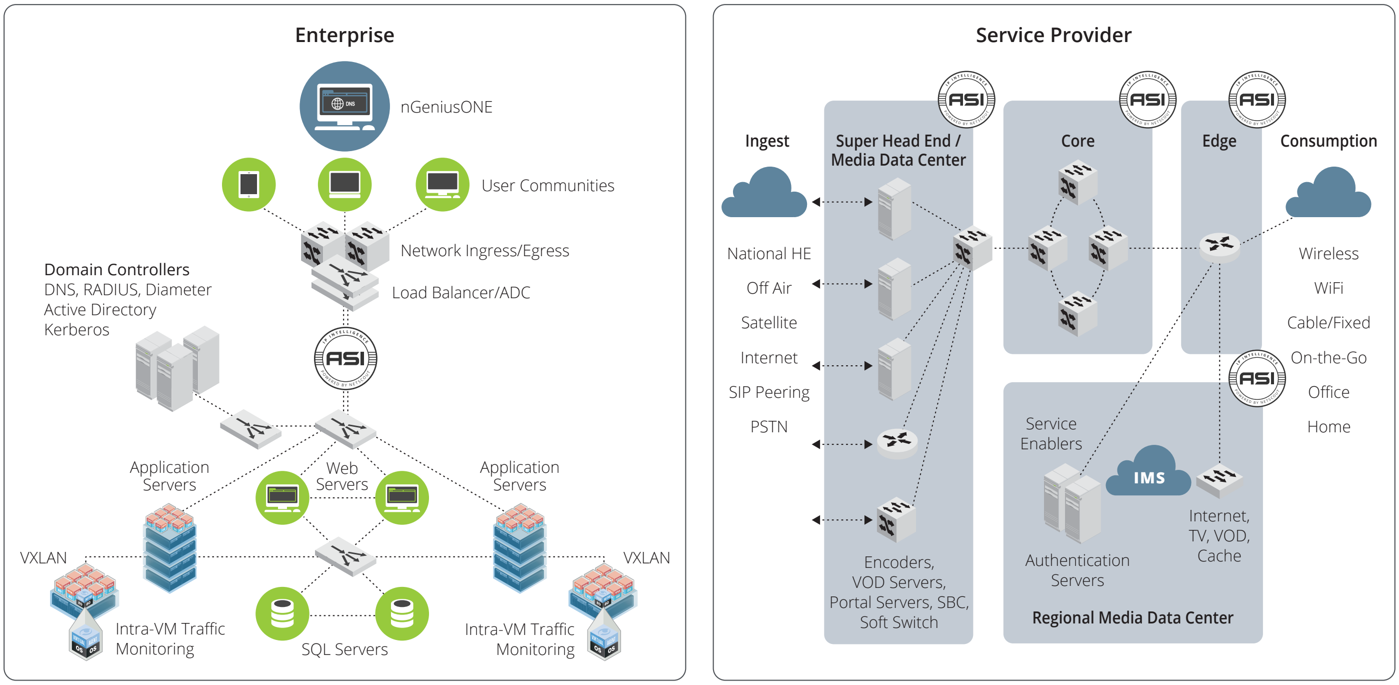


Figure 1: Service Instrumentation in Enterprise and Service Provider Environments.

Core Technologies

NETSCOUT's unique ability to gain a pervasive end-to-end visibility into the service delivery environment, and enable rapid service triage is centered on NETSCOUT's ASI technology, utilizing packet flow data, and providing scalable packet flow access.

Adaptive Service Intelligence (ASI)

Adaptive Service Intelligence is patented technology which uses rich packet-flow data to generate highly scalable metadata that enables a comprehensive real-time and historic view of service, network, application, and server performance. This powerful packet inspection and data mining engine runs on NETSCOUT's Intelligent Data Sources generating metadata based upon actual session traffic in real time as the packets cross physical or virtual links. NETSCOUT's ASI technology is the foundation of a highly scalable service delivery monitoring architecture which seamlessly collects, normalizes, correlates, and contextually analyzes data for all services: voice, data, and video.

Leverage 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 Packet Flow Switches and TAPs provide the foundation for a scalable monitoring architecture needed for service assurance. NETSCOUT's nGenius Packet Flow Switches (PFS) filter, aggregate, and distribute the targeted data to NETSCOUT's Intelligent Data Sources in a transparent, selective, and efficient manner. 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.

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 integrating NETSCOUT's ASI technology into a virtual machine (VM), functioning as a virtual Intelligent Data Source. NETSCOUT's VM either analyzes the intra-VM traffic in a self-contained virtualized mode or redirects the traffic to an external NETSCOUT Intelligent Data Source for analysis.
- **Traffic between VMs that reside in different hypervisors** is monitored by NETSCOUT 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 Comparison

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.
Rapid Service Triage	Reactive and time-consuming triage result in poor user experience, and extended service downtime impacting multiple users.	Rapid service triage helps resolve service degradation in real time before large numbers 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 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 return on investment in performance management by gradually expanding the solution over time.

About NETSCOUT Systems, Inc.

NETSCOUT Systems, Inc. (NASDAQ:NTCT) is a market leader in real-time service assurance and cybersecurity solutions for today's most demanding service provider, enterprise and government networks. NETSCOUT's Adaptive Service Intelligence (ASI) technology continuously monitors the service delivery environment to identify performance issues and provides insight into network-based security threats, helping teams to quickly resolve issues that can cause business disruptions or impact user experience. NETSCOUT delivers unmatched service visibility and protects the digital infrastructure that supports our connected world. To learn more, 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

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

Radware SDN applications improve application security, performance, and availability by integrating ADC and security intelligence with SDN to optimally analyze and forward traffic enhancing network services. Radware SDN applications integrate with the SDN application control plane and interact with the SDN controller to work with the Radware technologies throughout the application infrastructure.

Radware SDN-enabled ADC and security services transform applications from device-based solutions to become network wide services that intelligently divert traffic to service engines. Radware enhances SDN functions by leveraging our Virtual Application Delivery Infrastructure (VADI). This enables an EveryWare network service paradigm where applications are available anywhere and everywhere.

Key benefits of the Radware SDN network service infrastructure include:

- **Intelligent application delivery and security –** Optimal application service delivery
- **Easy implementation -** Improved operational efficiency of network management
- **Lower overall network service solution costs** – Deploy network services as needed
- **Greater scalability** – Scale network services throughout the network
- **Easier operational control** – Streamline network operations

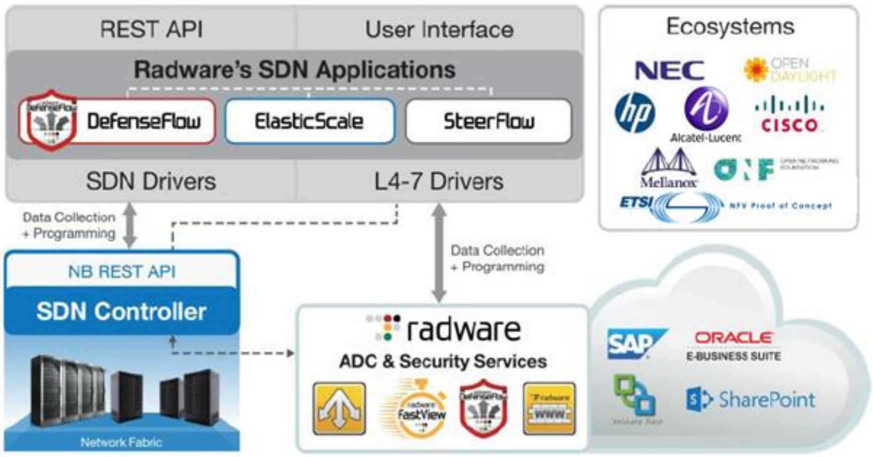
DDoS Protection as a Native SDN Application

DefenseFlow is an SDN application features an adaptive, behavioral-based DoS attack detection engine and a traffic steering mechanism taking advantage of the software defined network elements for attack mitigation. DefenseFlow delivers a necessary security control plane for SDN-based networks.

SDN & NFV for a Scalable Application Delivery Network

Radware offers Alteon VA for NFV – the industry's first and highest performing ADC designed from the ground up to run in NFV environments. Alteon NFV provides a unique value proposition consisting of CAPEX/OPEX reduction, vendor agnostic technologies, high performance, enhanced scalability, orchestrated elasticity, and improved network service agility.

Radware's ElasticScale is an SDN application that wraps existing network service virtual appliances, including Alteon NFV to consistently deliver network services in an elastic network environment. ElasticScale can be utilized to help providers adopt network functions virtualization paradigms.



Partnering for Success: Our SDN and NFV Ecosystem

The SDN and NFV eco-systems are a critical focus for Radware. Through partnerships with the industry's leading SDN and NFV consortiums and vendors, Radware ensures customers that our application delivery and security solutions integrate successfully into target architectures.

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.

Sonus SBC SWe—Virtual Session Border Controller

Service Providers and Enterprises Leverage NFV from Customer Premises to the Cloud

In the migration to private and public Cloud environments, Network Function Virtualization (NFV) is being adopted as one of the most disruptive changes in telecommunications since the transition to all-IP networks. NFV focuses on new methods for deployment and delivery of telecom services over a software-based network infrastructure. Through NFV, applications that were previously coupled to proprietary hardware can now be instantiated on generic commercial off-the-shelf (COTS) computing hardware.

Designed to operate in virtualized public and private cloud environments, the Sonus SBC SWe is the industry's only software-based SBC that delivers unmatched scalability using the same code base, resiliency, session management, media processing, transcoding, and security technology of a hardware-based SBC.

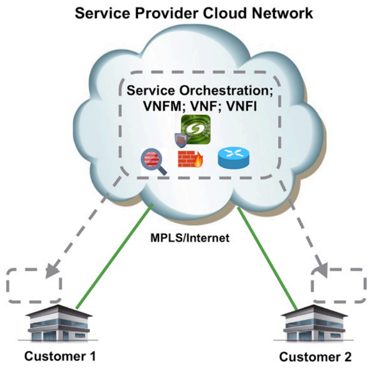
Sonus provides a migration path to private and public Clouds that can begin at multiple points within a service provider or enterprise network. Because there are many possible paths—from the traditional vertically integrated, custom-hardware-centric way of building networks, to the more flexible, software-defined, and highly elastic future way of building networks—Sonus is committed to working with each service provider or enterprise to achieve the best possible deployment model for their specific network.

Deploying SBC SWe as Virtual CPE (vCPE)

When deployed as a virtual CPE (vCPE), the Sonus SBC SWe enables service providers and enterprises to take advantage of shorter and more flexible deployment cycles for new services and cost savings from virtualization. A perfect application for a virtualized SBC, the emerging vCPE market is based on leveraging the value of NFV and orchestration for network edge services at the customer premises. Deployment models could include a service provider that manages the CPE, a Cloud-based service provider, or an enterprise that wants to retain ownership and control.

Service Providers Offer SBC-as-a-Service (SBCaaS)

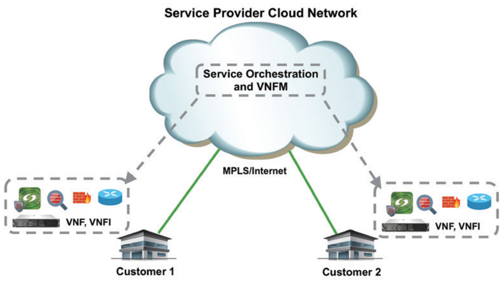
With NFV, service providers can deliver 'SBC as a Service' to enterprise customers by moving to a more efficient business model leveraging their virtualization and cloud infrastructure. Hosting SBCaaS eliminates the need to install, deploy, and maintain SBCs at the customer premises. Because NFV enables the rapid instantiation of an SBC, SBCaaS makes it far easier to serve enterprises that have seasonal business or high variability in traffic level, by adding or reducing capacity with a pay-as-you-grow model. Enterprises benefit because they eliminate SBC capital expenses and associated operational expenses. Additionally, the need to carry and manage spare physical inventory, to deal with space, power, and equipment installation issues, and possible CPE obsolescence are also eliminated.


Service Provider Cloud Network
Service Orchestration; VNFM; VNF; VNFI
MPLS/Internet
Customer 1
Customer 2

Service Provider SBC-as-a-Service

Virtual SBCs Deployed as Service Provider-owned Managed CPE

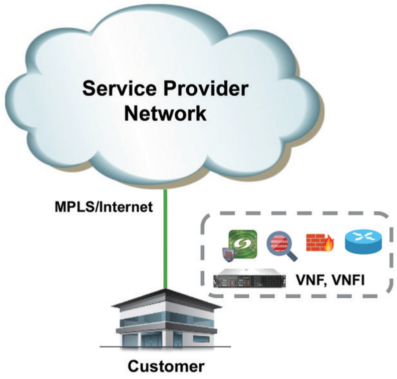
Service providers can choose to include a virtual SBC as part of a 'Managed CPE' service, in which low-cost COTS servers on the customer premises are used to host Virtual Network Functions (VNFs), and only the management and service orchestration of the virtualized SBC is conducted from their cloud environment. Orchestration and automation eliminate costly and manual turn-up/turn-down processes, and seamlessly and dynamically scale resources. In this mixed model, new services can be deployed quickly, and since the SBC is a collection of virtual functions, a service provider's upfront CPE costs are contained using COTS servers.


Service Provider Cloud Network
Service Orchestration and VNFM
MPLS/Internet
VNF, VNFI
VNF, VNFI
Customer 1
Customer 2

Service Provider-Owned Managed CPE

Enterprise-owned Virtual SBCs Deployed on Customer Premises

When a premises-based SBC is a necessity for an enterprise, the Sonus SBC SWe can be virtualized on common hardware platforms to contain operational costs. The portability and flexibility of the SBC SWe solution make it the ideal choice for enterprises that have invested in virtualization technology, require prepackaged solutions in a box, require remote network deployments, or are supporting opportunities such as entering a new geographic market where deploying a hardware solution would be impractical or cost prohibitive.



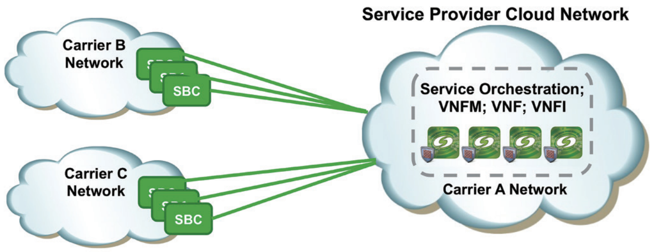
Enterprise-Owned Virtual SBC on Premise

Deploying SBC SWe as a Virtual Interconnect SBC

Interconnection peering points between service providers can be characterized as having dynamic traffic demands—which applies to mobile operators, fixed network operators, and cable providers, and especially to hub/wholesale service providers. Since each service provider is trying to optimize the cost of their interconnection points, traffic patterns are dynamic because they frequently make routing changes on the fly based on least-cost routes and quality-of-service conditions.

Because of this dynamic traffic demand, it's difficult to optimize the SBC capacity required at these interconnection points with a fixed hardware-based solution. This typically leads to overprovisioning of capacity, increasing both capital expense and operational expense. With a virtualized interconnect SBC, it is possible to overcome this limitation.

Deploying virtualized interconnect SBCs in a Cloud environment provides elasticity—the ability to have on-demand instantiation and/or reconfiguration of SBC VNFs to match dynamic traffic demand. A significant advantage of the Cloud environment is the ease and speed at which a new "logical" instantiation of an SBC can be deployed. Given the ability to perform scaling on-demand, service providers can deploy SBC VNFs in their network and scale a single instance or multiple instances independently from very low to very high session counts. With NFV orchestration, this on-demand scaling will be automated and touchless.


Service Provider Cloud Network
Carrier B Network
SBC
Service Orchestration; VNFM; VNF; VNFI
Carrier C Network
SBC
Carrier A Network

Virtualized Interconnect SBC

Load balancing and high availability are also key to addressing dynamic traffic demands of interconnect SBCs. Load balancing enables efficient scaling by allocating work load across a resource pool. In a Cloud environment, with only virtual resources, this is essential for the scalable deployment of SBCs. With a well-designed load balancing strategy, virtual resources are optimized to fine-tune the overall status of the application processing.

Real-time applications in a virtualized, cloud-based environment have the same high availability requirements for service, subscriber, and call resiliency as they do in traditional network environments. High availability requires an architecture where critical state information in an SBC is backed up in another node, ready to handle the traffic in the event of failure. Any change in the network is transparent to all peers, and no action is required to achieve this seamless transition.

About Sonus Networks

Sonus brings the next generation of Cloud-based SIP and 4G/VoLTE solutions to its customers by enabling and securing mission-critical traffic for VoIP, video, IM, and online collaboration. With Sonus, enterprises can intelligently secure and prioritize real-time communications, while service providers can deliver reliable, secure real-time services for mobile, UC, and social applications. Sonus offers an award-winning portfolio of hardware-based and virtualized Session Border Controllers (SBCs), Diameter Signaling Controllers (DSCs), Cloud Exchange Networking Platform, Policy/Routing servers, and media/signaling gateways. Visit www.sonus.net or call 1-855-GO-SONUS.

The content in this document is for informational purposes only and is subject to change by Sonus Networks without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Sonus Networks assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Sonus Networks, Sonus Networks has no obligation to develop or deliver any future release or upgrade, or any feature, enhancement or function.