The 2016 Guide to SDN and NFV

Part 6: Network Functions Virtualization (NFV): Operational Impediments

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

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 sixth of the serial publications. It will focus on the operational impediments to implementing 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.

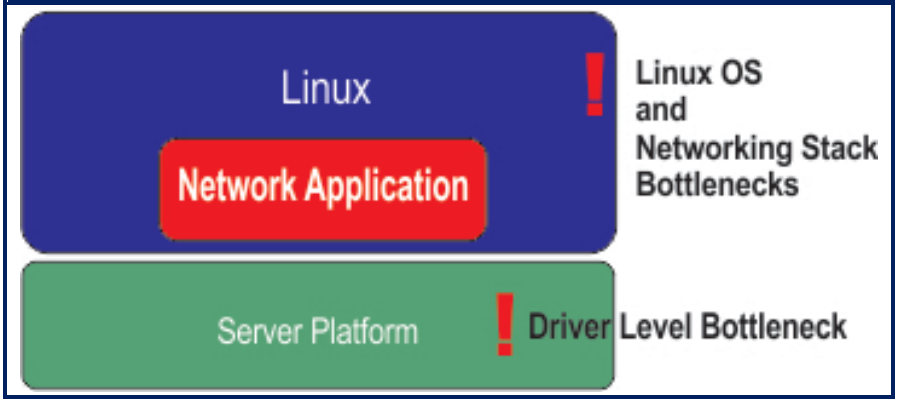
The Guide contains the results of a survey that was distributed in December 2015 and January 2016. Throughout The Guide the 144 network professionals who completed the survey will be referred to as The Survey Respondents.

Performance Limitations

In order to obtain the potential cost and agility benefits of adopting NFV, it must be possible to achieve roughly the same performance in a software-based environment as is possible in a traditional hardware-based environment. However, in many cases that isn't possible without an enabling software architecture because of the bottlenecks that are associated with the hypervisors, virtual switches and virtual machines that are the foundation of the emerging software-based approach to IT. In response to the performance bottlenecks that are associated with NFV, ETSI has authored a document entitled "NFV Performance & Portability Best Practices".

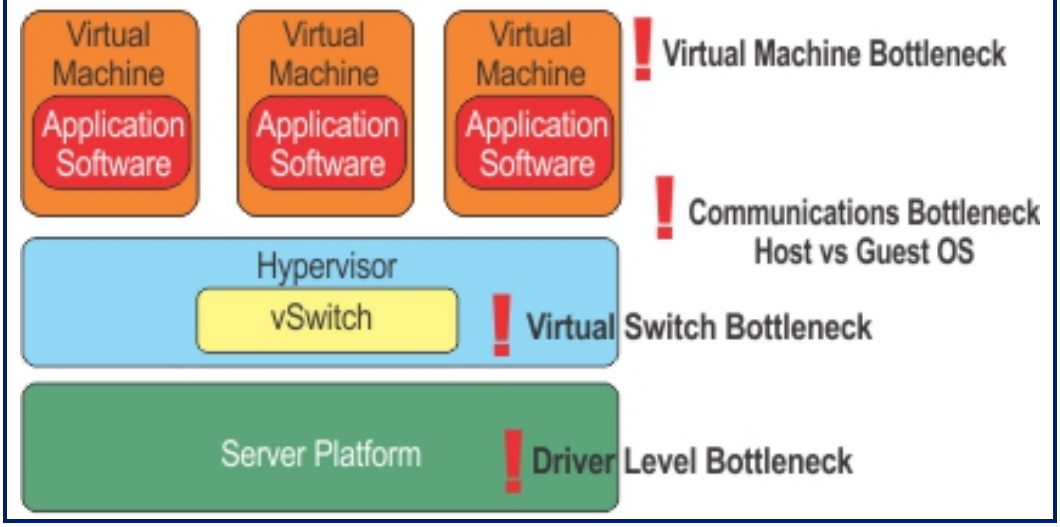
Performance bottlenecks are not unique to virtualized environments. For example, some of the bottlenecks that occur in a physical environment are shown in **Figure 1**.

Figure 1: Representative Bottlenecks in a Physical Environment



Unfortunately, as shown in **Figure 2**, as IT organizations adopt a virtualized environment the performance bottlenecks multiply. **Figure 2** demonstrates some, but not all of the bottlenecks that can occur in a virtualized environment. For example, while not explicitly shown in **Figure 2**, VM to VM communications can also result in bottlenecks.

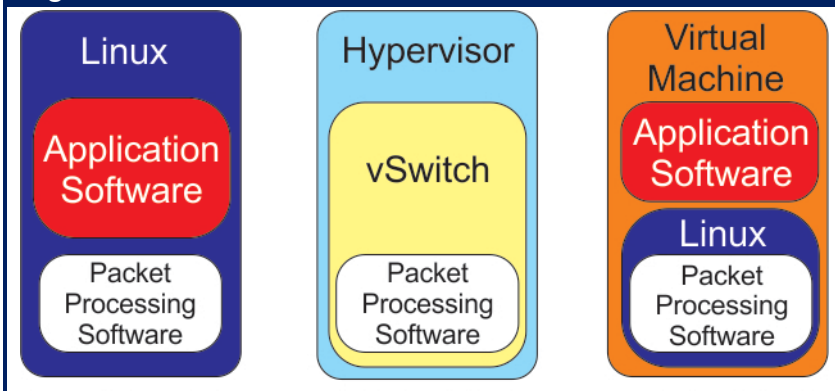
Figure 2: Performance Bottlenecks in a Virtualized Environment



Acquiring solutions that have effective packet processing software that can bypass bottlenecks is one of the primary ways to avoid experiencing unacceptable performance in a virtualized environment. As shown in **Figure 3**, when evaluating the enabling packet processing software, IT organizations should check for the following criteria in order to ensure a cost effective value proposition, and smooth transition to future requirements:

- Equal performance in both physical and virtual environments;
- Transparency: No change should be required to the operating system, the hypervisor, the virtual switch or to the management tools;
- Availability: The solution must work across multi-vendor processors, NICs and hardware platforms.

Figure 3: Breadth of Environments



The evaluation criteria listed above are intended to ensure that the packet processing software can be easily and universally implemented on any version of Linux or on any hypervisor without requiring changes to existing environments.

End-to-End Management

Status of Management

The Survey Respondents were asked to indicate to what extent NFV creates fundamentally new management challenges. Their responses are shown in **Table 1**.

Table 1: Extent of New NFV Management Challenges	
Extent of New Challenges	**% of Respondents**
No new challenges	8%
A few new challenges	41%
A broad range of new challenges	51%

Table 1 indicates that:

There is broad recognition on the part of IT organizations that the adoption of NFV creates new management challenges.

The Survey Respondents were asked to indicate how much progress their organization has already made relative to determining how they will respond to NFV's new management challenges. Their responses are shown in **Table 2**.

Table 2: Progress Towards Managing NFV	
Amount of Progress	**% of Respondents**
None	27%
A little	48%
A lot	14%
We have a well-defined strategy	11%

Table 2 indicates that:

The vast majority of IT organizations have made little or no progress relative to determining how they will respond to NFV-related management challenges.

The Survey Respondents were asked to indicate how much time their organization will spend over the next year working on developing an approach to how they will respond to NFV-related management challenges. Their responses are shown in **Table 3**.

Table 3: Amount of Time to be Spent on NFV Management	
Amount of Time	**% of Respondents**
None	13%
A modest amount	53%
A significant amount	32%
None – already done	1%

Table 3 indicates that:

Over the next year the vast majority of IT organizations will spend at least a modest amount of time working on developing an approach to how they will respond to NFV-related management challenges.

As discussed in Chapter 3 of The Guide (The Operational Impediments to Implementing SDN), Cloud Orchestration platforms have evolved as a means of automating and facilitating the process of configuring pools of data center resources in order to provide a range of cloud or cloud-like services. As a result, there is a natural affinity between Orchestration and NFV Management.

The Survey Respondents were asked to indicate the approach that their company is taking to orchestration. Their responses are shown in **Table 4**.

Table 4: Approach to Orchestration	
Approach	**% of Respondents**
Developing a strategy but concerned that existing solutions are immature	35%
Don't have a strategy and unlikely to develop one in the near term	16%
Have a well thought out strategy and have begun to execute	15%
Developing a strategy and optimistic it will be completed quickly	14%
Don't know/NA	9%
Have a well thought out strategy but not yet begun to execute	6%
Other	5%

Table 4 indicates that:

There is significant interest in orchestration, but only a very small minority of IT organizations are using an orchestration platform in production.

Management Challenges

Throughout this chapter of The Guide, the phrase *service provider* will refer to both Communications Service Providers and to enterprise network organizations.

As is widely recognized, the adoption of NFV poses a number of significant challenges that must be overcome in order to ensure that IT organizations will be able to implement effective end-to-end management. These challenges include:

- **Dynamic relationships between software and hardware components.** In traditional networks, application software and network function software generally run on dedicated hardware that is statically provisioned by manual processes. With virtualization, software running on virtual machines (VMs) can readily be moved among physical servers or replicated to run on newly created VMs in order to dynamically maintain availability, expand/shrink capacity, or balance the load across physical resources. Many of these changes in the infrastructure can be automated and programmatically activated to conform to configured policies under specific sets of circumstances. Due to the mobility of VMs, topology changes can occur in a matter of seconds or minutes rather than the days or weeks required for changing software/hardware relationships in traditional networks. In order to accommodate and leverage virtualization technologies, end-to-end management systems will need to be re-architected to be capable of implementing automated processes for virtual resource procurement, allocation, and reconfiguration in accordance with a set of highly granular policies designed to ensure the quality of experience for the user of the network services. Effective operations management also requires tools that give operators clear visibility into the relationships between the virtual and physical networks and their component devices. In particular, when performance or availability problems occur, both root cause analysis and impact analysis require bilateral mapping between the physical and virtual infrastructures.

- **Dynamic changes to physical/virtual device configurations.** To accommodate the dynamic nature of virtualized networks, end-to-end management systems will need to be able to adjust the configuration of devices to react to changing conditions in the network. For example, consider the traffic of an important application flow that has a medium priority class. If the network becomes congested, it may be necessary to change the traffic classification to be high in order to continue to meet an established SLA.

- **Many-to-Many relationships between network services and the underlying infrastructure**. In a typical traditional network infrastructure there is 1-to-1 relationship between a network service and a set of dedicated physical resources. In a virtualized infrastructure a network service can be supported by a number of Virtual Network Functions (VNFs) which may be running on one or several VMs. A single VNF may also support a number of distinct network services. In addition, the group of VNFs supporting a single network service could possibly be running on a number of distinct physical servers. As a result, end-to-end management systems need to support a three-tiered network model based on many-to-many relationships among network services, virtualization infrastructure, and physical infrastructure.

- **Hybrid physical/virtual infrastructures.** As virtualization is gradually adopted, service providers will need to be able to integrate virtual environments into their existing end-to-end

traditional/legacy monitoring infrastructures. Therefore, end-to-end management systems developed for the virtual infrastructure will need to be compatible with legacy infrastructure.

- **Performance Monitoring.** Because of the inherent complexity and dynamic nature of NFV, a performance monitoring strategy and methodology must be developed early and applied consistently throughout the service design and development process. This will allow seamless integration of new VNFs into the existing end-to-end monitoring platform and it will also provide development and operations teams with a consistent methodology for service monitoring regardless of what combination of physical and/or virtual functions are used in the delivery of a service. The key will be the ability to consistently and reliably monitor the performance of a service not just the performance of VNFs.

- **Network services spanning multiple service providers.** Some of the VNFs comprising a virtualized network service may be hosted in the clouds of multiple collaborating providers. One major challenge in a multi-cloud environment is managing end-to-end service levels and SLA compliance. Since visibility into portions of the end-to-end path that are external to a service provider will always be limited, some form of aggregated external SLA data will have to be developed and imported from partner providers and the Internet. This requires a flexible and extensible end-to-end management architecture that provides consistent data collection and management interfaces across all on-net and off-net resources and technologies. Multi-cloud environments also require new approaches in managing end-to-end security.

- **IT and Network Operations collaboration.** These organizations will need to cooperate effectively to establish new operational processes that meet the demands of end-to-end management of hybrid physical/virtual infrastructures. This will require an effective DevOps organizational model for the development of network services based on NFV. One of the challenges will be to share the responsibilities for the various tasks involved in rolling out a new service. A key aspect of this cooperation will involve the selection and management of component VNFs, as well as testing and deploying the end-to-end management capability for the network service in question.

- **Hybrid environments**. For the foreseeable future, some services will be based on existing physical network functions while others will be based on VNFs and some others will be based on a hybrid environment made up of both. In a hybrid environment both types of function must have management interfaces built on a common information model (see below) in order to support agile DevOps-style service creation as well as the dynamic management and orchestration. In a hybrid environment it's crucial that management is policy-based and uses control loops to ensure quality of service.

- **Shared information model**. Where dynamic network service configurations are required, the management interfaces presented by both virtual and physical infrastructure elements need to lend themselves to automated plug and play integration. Information models drive consistency in the design of data payloads in automated interfaces by capturing behavior, defining standard interface communications patterns and specifying information representations; e.g., metrics representation and semantics for reporting SLA and QoS performance.

- **Policy based architecture**. Taking full advantage of the dynamic mature of virtualization requires an end-to-end management system that can perform as an autonomic system to support real time operational processes. A policy management architecture is the basis for automated management and orchestration. Policies can be based on hierarchical system of

rules designed to deal with the complexities of a hybrid environment and to manage the relationships among users, services, SLAs, and device level performance metrics. For example, if the CPU utilization of a physical server hosting a VNF becomes excessive, the VNF may be moved to a server with lower utilization if that is in accordance with the SLA.

Management Direction

ETSI is working to drive how NFV will be managed. Towards that end, ETSI has established a management and orchestration framework for NFV entitled Network Function Virtualization Management and Orchestration. Some of the key concepts contained in that framework were summarized in another ETSI document. According to that document:

> *"In addition to traditional Fault, Configuration, Accounting, Performance, and Security (FCAPS) Management, the NFV Management and Orchestration framework introduces a new set of management functions associated with the lifecycle management of a VNF. The NFV ISG has focused on detailing these new sets of management functions, which include, but are not limited to: on-board a VNF, instantiate a VNF, scale a VNF, update a VNF, and terminate a VNF. A difference also worth highlighting relates to fault and performance management - in a virtualized environment this is the responsibility of different functional blocks at different layers. As a result, the correlation of faults, alarms and other monitored data such as performance metrics and resource usage, and the consequent fault resolution needed to operate the service in a reliable manner, will typically be distributed.*
>
> *Network Service Orchestration functions are responsible for coordinating the lifecycle of VNFs that jointly realize a Network Service. Network Service orchestration functions include on-boarding a Network Service, management of resources used by the Network Service, managing dependencies between different VNFs composing the Network Service, and managing the forwarding graphs between the VNFs. During the Network Service lifecycle, the Network Service orchestration functions may monitor Key Performance Indicators (KPIs) of a Network Service, and may report this information to support an explicit request for such operations from other functions.*

Expanding on the functional blocks and reference points identified by the NFV Architectural Framework, the NFV Management and Orchestration framework defines requirements and operations on the interfaces exposed and consumed by functional blocks associated with the different management functions; e.g. VNF lifecycle management, virtualized resource management. The objective of such an approach is to expose the appropriate level of abstraction via the interfaces without limiting implementation choices of the functional blocks. The document provides an extensive description of interfaces, which is the basis for future work on standardization and identification of gaps in existing systems and platforms."

Impact on Organizations and Jobs

The Survey Respondents were also asked how much of an impact they thought that NFV will have on the structure of their company's IT organization over the next two years. Their answers are shown in **Table 5**.

Table 5: Impact of NFV on Organizational Structure	
Impact	**% of Respondents**
Very Significant Impact	9%
Significant Impact	27%
Moderate Impact	19%
Some Impact	19%
No Impact	8%
Don't Know	18%

The data in **Table 5** indicates:

Roughly a third of IT organizations believe that over the next two years that the adoption of NFV is likely to have a significant or very significant impact on the structure of their organization.

When The Survey Respondents were asked what the impact would be, their answers included that NFV will:

- Reduce the time it takes to deploy new offerings;
- Force realignment between departments;
- Drive changes to security models;
- Result in a reduction in the amount of labor that is required;
- Result in the assignment of new roles once the efficiencies are realized;
- Drive the need for cross domain management;
- Cause a change in their approach to application development.

The Survey Respondents were also asked how much of an impact they thought that NFV will have on the required skill base of their company's employees. Their answers are shown in **Table 6**.

Table 6: Impact of NFV on Employee Skills	
Impact	**% of Respondents**
Very Significant Impact	7%
Significant Impact	34%
Moderate Impact	26%
Some Impact	19%
No Impact	5%
Don't Know/Other	10%

The data in **Table 6** indicates:

Over the next two years the adoption of NFV is likely to have a significant or very significant impact on the skill base of roughly 40% of all it professionals.

When The Survey Respondents were asked what the impact would be, their answers included that NFV will:

- Drive the need for employees to develop enhanced skills;
- Increase the time it takes to train new employees;
- Create the need for employees to have a knowledge of software tools;
- Drive the need for cross training of team members;
- Drive the need for combining IT and networking skills;
- Cause companies to replace employees who don't adapt;
- Increase the need to transition from traditional network skills to cloud and systems skills;
- Result in DevOps skills replacing traditional networking skills.

DevOps

One of the implications of the ongoing virtualization of all forms of IT functionality is the adoption of a DevOps model. The point of adopting DevOps is to establish tight collaboration between a number of the phases of the application development lifecycle, including application development, testing, implementation and ongoing operations. With that goal in mind, some of the key characteristics that are usually associated with DevOps are that the applications development team continuously writes primarily small incremental pieces of code that are tested on an architecture that reflects the production architecture.

Those key principles that characterize DevOps are:

- **Collaboration**
  A key aspect of DevOps is to create a culture of collaboration among all the groups that have a stake in delivery of new software.

- **Continuous integration and delivery**
  With continuous integration, software changes are added to a large code base immediately after development so that new capabilities can be continuously delivered to the entire release chain for testing and monitoring in production-style environments.

- **Continuous testing and monitoring**
  With DevOps, testing is performed continuously at all stage of the release process and not just by the QA organization. Developers do testing and provide test data and procedures that can be used by collaborating groups downstream in the process. The operations group is also typically involved in the test and monitoring processes. Part of their value add is that operations groups can specify load patterns to make testing by other groups more in line with actual usage conditions.

  In addition, operations groups perform continuous monitoring to identify problems with the services being delivered so that they can be fixed in near real-time. Monitoring relies on an appropriate set of tools. The same tools that monitor the production environment can also be employed in development to identify performance problems prior to production deployment.

- **Automation**
  With DevOps all stages of software delivery are highly dependent on automated tools. Automation is essential because it enhances agility and provides the productivity required to support the continuous nature of integration, delivery, testing, and monitoring of many small increments to the code base.

- **API centric automated management interfaces**
  Software Defined Environments (SDEs) are an emerging core capability of DevOps that allow organizations to manage the scale and the speed with which environments need to be provisioned and configured to enable continuous delivery. SDEs use technologies such as API-centric automated management interfaces that define entire systems made up of multiple components. These interfaces are based on information models that define the characteristics, configurations, roles, relationships, workloads, and work- load policies, for all the entities that comprise the system.

All of the basic principles of DevOps are applicable in a network operations (NetOps) setting. However DevOps is generally applied to discreet services that are frequently delivered over the web on a best effort basis. The network environment is different than that and as a result virtualized network services development creates challenges that are not addressed by DevOps. One such challenge is that since Virtual Network Functions (VNFs) such as optimization and security are chained together to create an end-to-end service this creates strong dependencies between the VNFs. For example, if a service provider updates an optimization VNF they need to ensure that it is fully compatible with the security VNF(s). As a result much stronger version control and compatibility testing is needed than would be typical for enterprise applications.

Other challenges created by network services development that must be addressed by NetOps that were not addressed by DevOps include:

- Since for the foreseeable future the vast majority of environments will be a combination of hardware-based and software-based functionality, the NetOps methodology must accommodate services that depend on network functions running on dedicated hardware platforms as well as VNFs.

- Virtualized services will often be created by integrating services from multiple suppliers. This will require NetOps methodologies and best practices to support concurrent synchronized development and integration across the domains of multiple partners.

- Unlike what happens when delivering an application over the Web, NetOps will need to support dynamic and automated management of service performance and SLAs. This can only be achieved by a policy model that supports end-to-end SLA targets.

- Again in contrast to what often happens when delivering an application over the Web, NFV services are often mission critical. This creates a need for high levels of resilience and rapid fallback capabilities.

- Virtualized services will cover a very wide range of network functions and technologies. As a result, consistent frameworks and interfaces are needed in order to achieve the goal of minimizing or eliminating the need for manual intervention of any sort when incorporating VNFs into a network service.

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.

AUTOMATE YOUR CLOUD WITH aCLOUD SERVICES ARCHITECTURE

Integrate dynamic services into your Cloud Data Center

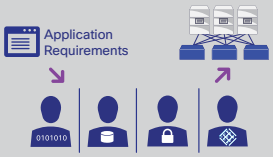
www.a10networks.com

Why Choose Application Centric Infrastructure (ACI)?

Application Deployment at the Speed of Business

Without ACI

New Application



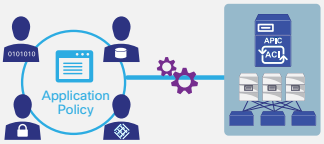
IT administrators work in silos.

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.

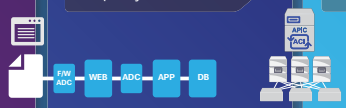
ACI cuts deployment time and effort.

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

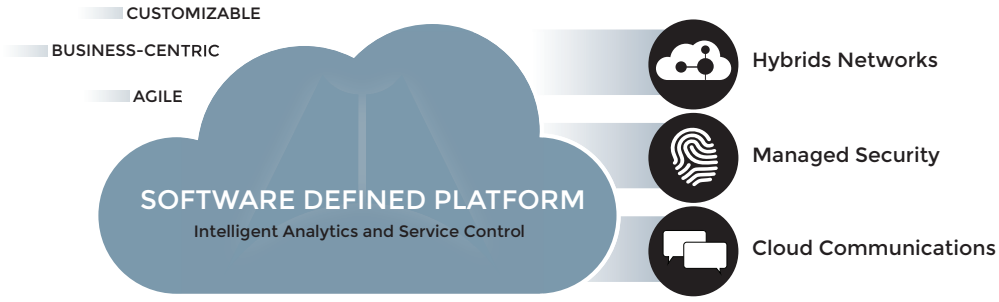
cisco

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

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.

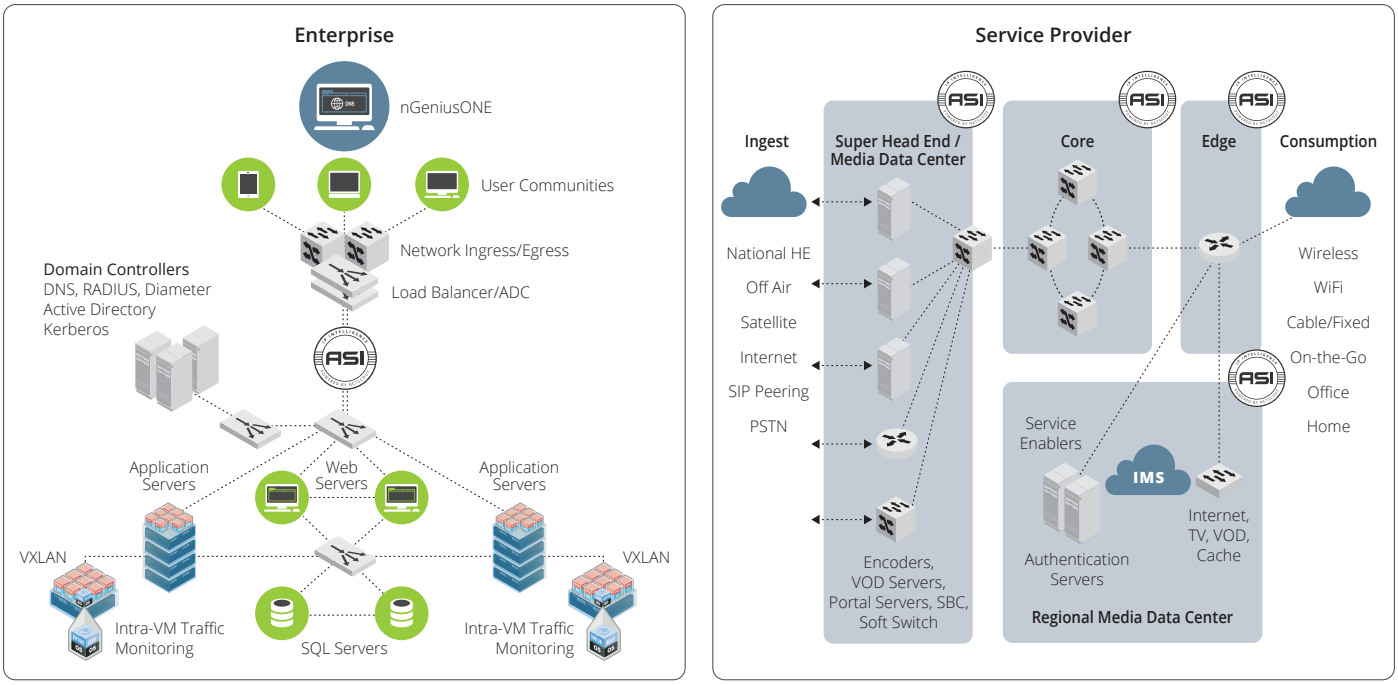


Figure 1: Service Instrumentation in Enterprise and Service Provider Environments.

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

ADV_001-1500 11/2015

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

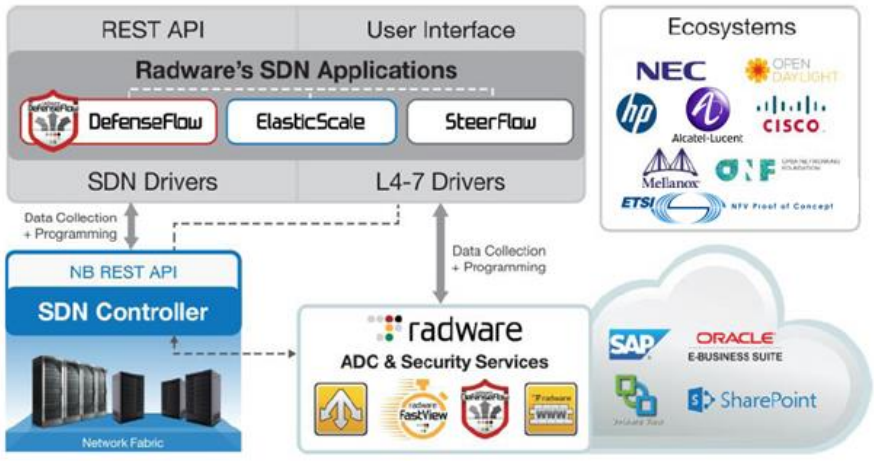
DDoS Protection as a Native SDN Application

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.

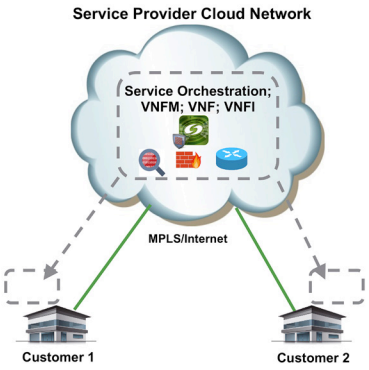
Sonus provides a migration path to private and public Clouds that can begin at multiple points within a service provider or enterprise network. Because there are many possible paths—from the traditional vertically integrated, custom-hardware-centric way of building networks, to the more flexible, software-defined, 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)

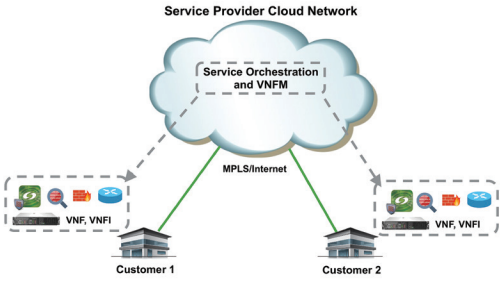
With NFV, service providers can deliver 'SBC as a Service' to enterprise customers by moving to a more efficient business model leveraging their virtualization and cloud infrastructure. Hosting SBCaaS eliminates the need to install, deploy, and maintain SBCs at the customer premises. Because NFV enables 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 SBC-as-a-Service

Virtual SBCs Deployed as Service Provider-owned Managed CPE

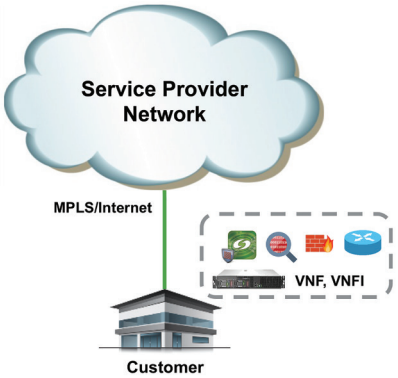
Service providers can choose to include a virtual SBC as part of a 'Managed CPE' service, in which low-cost COTS servers on the customer premises are used to host Virtual Network Functions (VNFs), and only the management and service orchestration of the virtualized SBC is conducted from their cloud environment. 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-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.



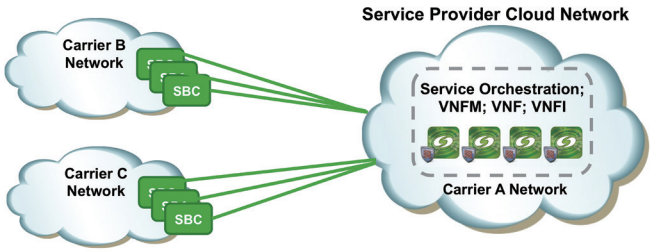
Enterprise-Owned Virtual SBC on Premise

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.



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.

Sonus™
Cloud communications made smarter