A Lippis Consulting Industry Paper

A New Open Data Center Fabric Emerges
for
The Age of Software-Defined Infrastructure

By Nicholas John Lippis III
President, Lippis Consulting

October, 2015

Abstract

A number of independent trends are driving a new age of software-defined networking and overall infrastructure. These trends include a new IT delivery model based upon cloud computing, big data analytics, Internet of Things and new IT delivery model. This trend is so massive that no army will stop its progression that's rooted in the separation of network hardware from its high-value software. At the heart of this trend is realization that wide area and data center networking is transitioning to a software model which has implications that stem from how IT organizations are organized to how applications are delivered and maintained. We focus this white paper on the transition to software and the implications upon networking from a perspective of fabric and services, which connects servers and storage to the internet/intranet.

Trends in Modern Data Center Infrastructure

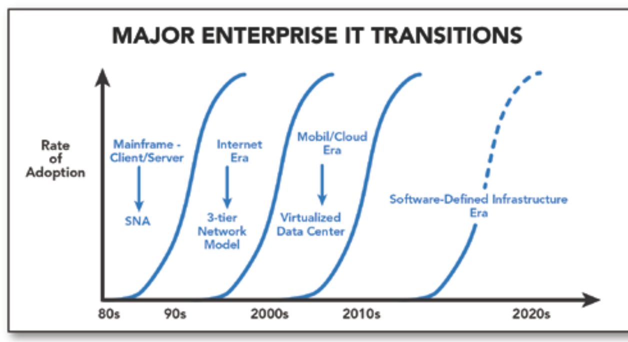
More than ever, the global economy is fundamentally linked to, and its future is tied to, information technology or IT. In particular, this future is one of agile corporations responding to market opportunities and competitive threats. Those corporations, equipped to respond accurately and quickly with IT, will be increasingly rewarded. Corporations capable of rapidly prototyping and deploying applications to address market dynamics will create more business value than those that cannot. In short, these firms are more competitive and responsive. For these firms, IT is not just a strategic asset, but an integral part of the entire corporate experience felt by customers, partners, employees and suppliers. At the heart of this new era in corporate competitiveness is open cloud-based IT infrastructure.

Application development and data center infrastructure are fundamentally changing, thanks to mobile and cloud computing. Applications are being developed for mobile and desktop access, with mobile highly emphasized. New tools, such as containerized microservices, unikernels, library OS, etc., along with virtual machines, offer the right hooks for DevOps teams to rapidly develop, test, deploy, change and maintain applications. But, to fully equip this new IT model, IT infrastructure has to transition to more of a software model than its current, vertically integrated, hardware approach. In short, infrastructure is becoming software-defined.

Applications and associated hosting are being split between private data centers, cloud infrastructure and public cloud hosting facilities in a hybrid cloud model. This change in how applications are being built and consumed started in 2007 with the introduction of Apple's iPhone and in the fall of 2006 with the introduction of Amazon's Elastic Compute Cloud or EC2 for compute and Web Services (AWS) for storage (Amazon S3). Since 2006, data center infrastructure design fundamentally changed from a three-tier internet-based model to virtualized infrastructure and now towards a software-defined cloud infrastructure. All these advances bring faster IT delivery, lower cost and greater agility. But, to gain these advantages, while transitioning brownfield-based applications, a network fabric that supports software-defined infrastructure is required.

Major Enterprise Data Center Infrastructure Transitions over Time

Figure 1 plots major application compute models and their corresponding data center infrastructure architectures over time; starting from mainframe computing to present day private cloud infrastructure to the rise of software-defined infrastructure. Notice how these phases overlap. As one phase starts, the previous phase continues. For example, the virtualization and cloud infrastructure phases are now overlapping and driving a new software-defined infrastructure era.



Case in point, at an Open Networking Users Group, or ONUG, conference in Boston at Fidelity Investments, Chief Network Architects (CNAs) from the largest corporations discussed their Software-Defined Networking (SDN) plans, requirements and experiences. Two key messages from this meeting were network operational expenditure has to fundamentally change and business unit managers are demanding secure self-service IT provisioning. One large bank showed a graphic that plotted the rate of self-service virtual machine (VMs) adds within a business unit, as well as pauses and deletions. The curve was exponential, over a small amount of time—meaning there's a large pent-up demand for secure self-service IT delivery. And, this is just the beginning of the curve considering only 48% of servers are virtualized and a much smaller number of VMs are networked. In short, CIOs are now getting pressure to deliver the same low-cost, fast spin-up and elastic compute model that public cloud services offer, but privately to ensure security.

On-Demand IT Service Delivery Trends Up

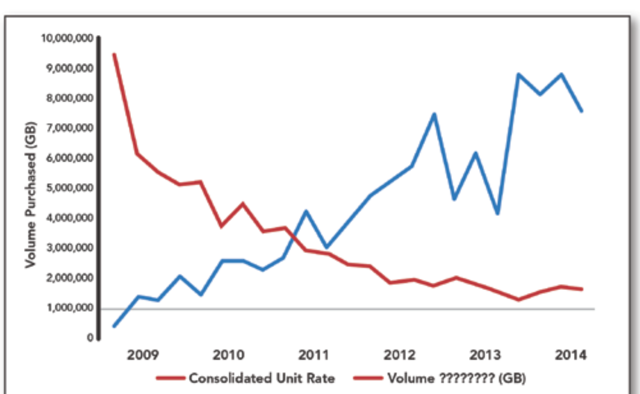
For example, at a recent ONUG meeting, an IT executive from a large financial services firm complained that it took nearly 200 days from the time of server order to application roll out, with network service configuration consuming 42 days or 21% of the time. This does not include application development time—just the time to procure and configure its infrastructure and dependency map.

Compare these 200 days to the seconds-to-minutes needed for VM configuration, and it's no wonder why CIOs are deploying private cloud infrastructure while business unit managers look toward public cloud to speed their application development. But, even with the speed in which VMs are configured, the longest time to market is configuring the network and its associated network services, such as connectivity, policy, control (firewall), load balancing, QoS and building in resiliency. SDN, combined with automation through inventory and intent, can complete the "orchestration stack" and reduce these deployment times by two to three orders of magnitude!

Open networking promises IT executives a choice of vendors and designs with capital plus operational cost relief. But, fundamental to open networking is the enablement of auto configuration and secure provisioning under application control—meaning applications request network services and the network auto configures to accommodate the request. This service sounds simple and is highly desired as a tool to speed up application deployment while shifting to secure, automated IT services by closing the delivery gap. Although enabling auto configuration and provisioning under cloud orchestration control is important to open networking's success, network services are holding up automation.

A few more, important, modern data center trends need to be added to the discussion.

Open Storage: During ONUG Fall 2015, hosted by Credit Suisse, the ONUG Community observed demand for storage was growing at a 25% CAGR (compound annual growth rate) over seven years! See Figure 3. At current growth rates and unit pricing, storage CapEx will increase approximately 50% in three years while some operational costs will rise proportionally. Thus, storage growth is placing a significant impact on networking. In addition, the trend towards distributed server-based storage is positioning Ethernet



networking as the backplane for new scale-out storage architectures.

While storage consumption, spend and flows over data center networking increase, so are operating system instances on both physical and virtual servers on the order of 7% CAGR over the same seven-year period, while data center load or power consumption will increase some 1.3% CAGR over the same period. Virtual desktops are also enjoying a near 8% CAGR over the same seven-year period, mostly thanks to October 22, 2012, Hurricane Sandy. During that disaster, many IT departments lost office space and deployed thousands of virtual desktops over a weekend, proving its value in enterprise computing by allowing IT departments to keep their operations open; that is, not closing for one hour after the storm!

The major challenges IT business leaders face in modern data centers are varied, but mostly include the following:

Restructuring: There is continued pressure on cost, especially in industries that are in the midst of restructuring.

Legacy Application Support: Most large enterprises need to support a large legacy base of applications, usually large capacity, offering no greenfield-forced migrations.

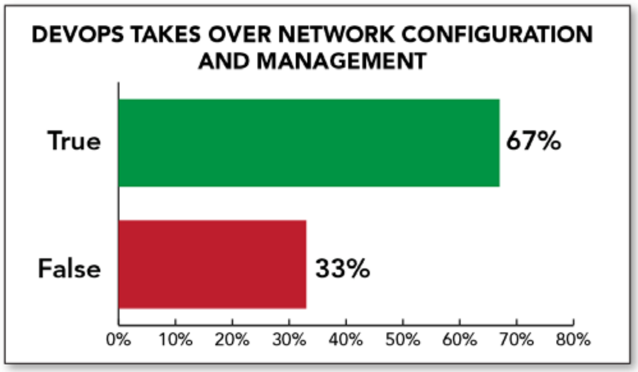
Reduced CapEx: CapEx spending is down approximately 40% from 2007 levels, but is now stabilizing. However, storage cost needs to be contained while data center asset utilization needs to increase.

Reduced OpEx: OpEx has been reduced approximately 25% since 2011 peak with a need to decrease the cost of DR (Disaster Recovery) testing and improve time to market, as well as application development productivity.

Regulation: In the financial services, and other industries, there's increasing pressure from regulators, driving the need to segregate Development/Production, Servers/VDI (Virtual Desktops).

Infrastructure Life Cycle Shifts toward Software Lifecycle

To address the issues above and opportunities, IT infrastructure is transitioning from hardware- to software-based. Open networking is all about decoupling, or the disaggregation of networking software and hardware, which has two implications: 1) hardware becomes less relevant and, hence, is driven toward commoditization and lower cost, and 2) software now can run of different types of hardware, such as merchant silicon switches or X86 servers, that support integration of embedded functionality, and external controller applications via Application Programmable Interfaces (APIs). These APIs are the gateways to programmable infrastructure, automated configuration and orchestration , as well as tight linkage to an enterprise's software infrastructure and associated lifecycles. The transition towards software-defined infrastructure is rooted in the rise of DevOps within the enterprise market. At a recent ONUG meeting, the community voted "if DevOps would take over network configuration and management" and 67% of voters said they would!



The New Infrastructure Model

The new software-defined infrastructure model leverages commoditized, white box, hardware for servers, network switches and disk drives. Network switches have already made this transition with merchant silicon-based top of rack (ToR) switches being the dominate variety within cloud and service provider data centers, as well as new enterprise data center builds. There are many open switch operating system products, such as ONL, Open NSL, ADP, ONP, SAI, FBOSS and others, that seek to offer choice and options for network architects to mix and match different white box switches and operating systems. While this model is popular in hyperscale firms, such as Facebook, Google, Microsoft, Amazon, et al, its popularity in the enterprise market has not caught fire due to the integration work required. Most enterprise architects choose white box switches with a vendor-supported networking operating system. However, both options, merchant silicon switches with open or closed OS, are being equipped with open programmable interfaces for coding the network infrastructure configuration, feature enablement, etc.

While network hardware is becoming commoditized, the growth of virtual endpoints, such as VMs, containers and microservices endpoints, are growing. Note that virtual endpoint connectivity is required between data centers, as well as branch offices and data centers. Wherever the application reaches, the end user does too, as well as the overlay and its connectivity. Therefore, the need to network these virtual endpoints is growing, which has given rise to virtualized networking, or overlays, in the data center and WAN.

Connectivity is fundamentally changing from physical connectivity to virtual. In addition, virtual flows are created for east-west and north-south traffic, with east-west being the dominant traffic flow. The ability to create flows is important in modern data centers to support applications split across multiple servers as well as connecting virtualized network services such as firewalls, load balancers etc., to applications.

Fundamental to network virtualization is the linking and programming of overlays via cloud orchestration, such as VMware's vCenter, OpenStack, Docker, Mesosphere, Kubernetes, Puppet, Chef, SaltStack, Ansible, CFEngine, Linux, Vagrant, etc., offering speed and agility to configure the infrastructure. Some refer to this model as node-level virtualization. While node-level virtualization does have its advantages, it still requires orchestrating configuration and management complexity at node/port level. Path or flow-level virtualization is best in cases where the end-to-end traffic pattern is known a priori, requiring point-to-point virtual pipes. However, for any-to-any connectivity as observed in today's cloud environment, managing and creating large number of virtual pipes limits scale. Furthermore, such virtual pipes cannot always ensure full usage of the network backplane. The bottom line is that many will deploy both approaches; that is, node- and flow-level virtualization.

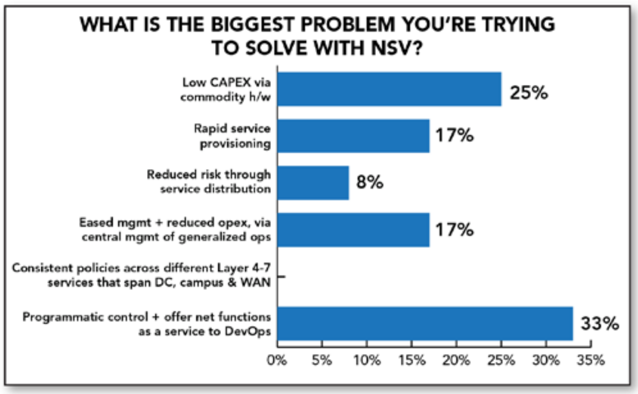
As overlay deployments rise, so does the need for full-stack engineers who understand networking, as well as how to code in Python, Ruby, Jenkins, JavaScript, GO, Linux, etc. From a skill set and IT staffing point of view, it's pretty clear from the above that the CCIE skill set is becoming less and less relevant in today's IT job market as software-defined infrastructure build out expands.

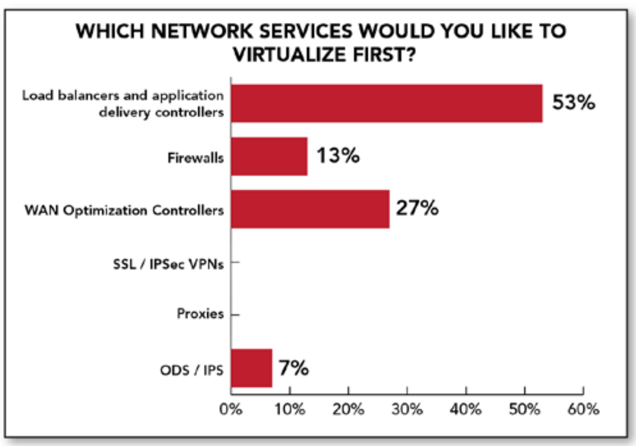
Software-Defined Infrastructure

The above discusses commoditized hardware and overlay software, linked to cloud orchestration, as key components of a software-defined infrastructure (SD-I) architecture. Another aspect of SD-I is network appliances, such as firewalls, load balancers, WAN optimization, IPS, etc., are also transitioning from hardware-based appliances to software models that are chained together to create virtualized dependency maps for specific applications. At ONUG, this mapping was called Network Service Virtualization or NSV. Service providers have an initiative called Network Function Virtualization, or NFV, which seeks to do the same for the many hardware-based network functions or appliances that make up service provider networks.

NSV provides three core components to a software-defined network by removing the many hardware appliances stacked within data centers and branch offices into a software model that is less expensive to manage, does not consume separate power and is accessible to DevOps, as well as cloud infrastructure teams, so they can add services to their applications via "service chaining."

During ONUG Spring 2015, the community voted upon what problem NSV solved and which network service they wanted to virtualize first. The data below shows "service chaining," the ability to have programmatic control plus offer network functions as a service to DevOps, was paramount followed by practical cost savings. In terms of which network service to virtualize first, load balancers and application delivery controllers ranked first followed by WAN optimization controllers that are first in line to be folded into a software-defined network infrastructure.





NEC's ProgrammableFlow® Networking: An investment in providing options and choices in the building of a Software-Defined Infrastructure

Since 2011, IT business leaders have installed NEC's ProgrammableFlow® Networking Suite in both large and small production networks in a wide range of geographies around the world. The NEC ProgrammableFlow® Networking Suite deployments range from the predominate mobile phone operator in Japan, NTT Communications Global Cloud, to a 28-building school system in the U.S. NEC ProgrammableFlow® Networking Suite was one of the first, commercially available, SDN solutions to enable full network virtualization, allowing enterprises, data centers and service providers the ability to deploy, control, monitor and manage secure multi-tenant network infrastructure.

ProgrammableFlow SDN automates network administration for business agility and provides a network-wide programmable interface capable of unifying the deployment and management of network services throughout the entire IT infrastructure value chain. This open network architecture separates hardware from software resulting in centralized and streamlined network administration.

With its SDN offering, ProgrammableFlow Networking Suite, NEC offers a software-defined network fabric with the following attributes:

Stable –Centralizes and automates network control, eliminates fragile and complex protocols, including manual, error-prone processes inherent to conventional networks.

High Performance –Provides reliable Layer 2 and Layer 3 multipath networks capable of supporting network interfaces up to 1 terabit. ProgrammableFlow's distributed virtual routing function eliminates bottlenecks associated with traditional network design, providing optimal, line rate traffic forwarding throughout the network.

Open–Support for OpenFlow 1.3 and 1.0 standards, while being the first OpenFlow provider certified by the Open Networking Foundation, acknowledging NEC's commitment to open standards.

Secure–NEC's Virtual Tenant Network (VTN) technology enables isolated and secure virtual networks. Each VTN has its own network policy, eliminating complexity and trade-offs associated with traditional network security design.

As mentioned above, the main focus of NSV is to move as many network service hardware appliances as possible to software. The following key attributes of ProgrammableFlow are uniquely suited for NSV orchestration.

Selective Appliance Routing

Defining flexible conditions on how traffic should be forwarded to different types of appliances is straightforward. For example, an administrator can decide, via rules, whether to forward a given traffic flow to a firewall or whether to add a particular appliance, such as an intrusion detection system, along the flow path.

Appliance or Service Composition

Chaining or sequencing multiple rules or virtual filters (vFilters) can accomplish appliance or service composition. For example, an administrator can define a set of filters with corresponding actions to define a forwarding path for a particular flow that consists of a firewall, an intrusion prevention system and a load balancer before reaching a destination host.

Appliance Availability

ProgrammableFlow's ping-based monitoring feature in the controller can be used in conjunction with conditional routing to improve appliance availability. For example, if a given appliance becomes unavailable, the network fabric can detect the fault and assist in redirecting the traffic flow to a standby or backup appliance.

Selective Traffic Steering

Selective traffic steering refers to an application scenario where traffic is steered towards a given egress port of the fabric based on certain matched conditions. An example scenario is when policies are set to steer traffic through the right WAN interface. Such policies can be reactive as well. For example, if WAN access becomes unavailable, the traffic needs to be steered through a backup interface.

Dynamic Intelligent ACLs

The vFilters defined in ProgrammableFlow solution can be leveraged to define Access Control Lists (ACLs) with varying degrees of complexity. Simple ACLs can be based on direct packet header matching to decide whether to drop or pass packets. Complex ACLs can consist of complex predicates defined on multiple packet header fields. The ACLs can be deployed dynamically on the virtual network. The controller takes responsibility of pushing the associated flow table entries to all the switches in the fabric.

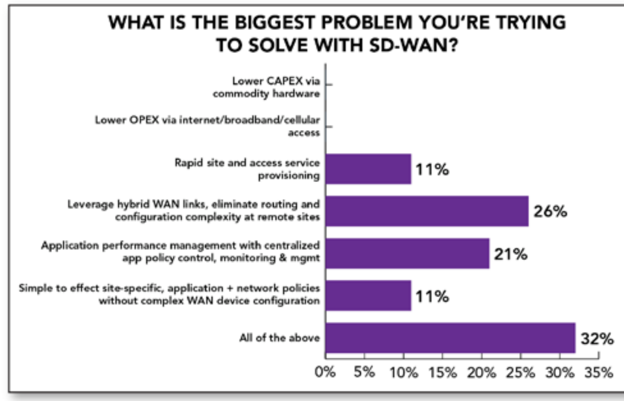
Appliance Layer Compaction

In traditional Layer 2 data center design, appliances, such as firewalls and load balancers, are deployed as separate layers, thereby creating multiple layers at the logical level. With the use of conditional routing, appliances can be connected to any switch port and traffic can be explicitly routed to specific appliances using appropriate condition definitions. In other words, there are no physical connectivity constraints associated with attaching the appliance.

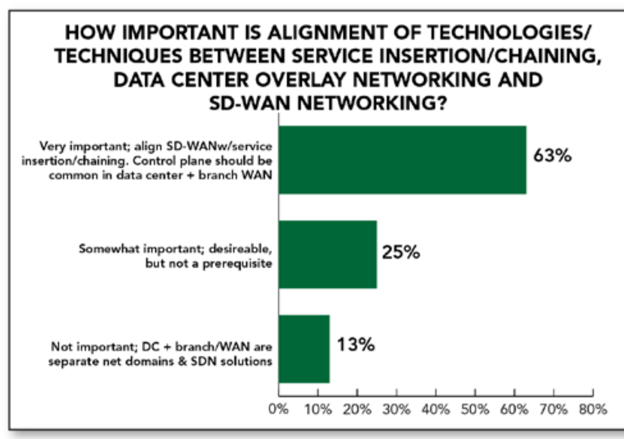
Two unique attributes of the NEC ProgrammableFlow® Networking Suite fabric are the ability to span architecture enterprise wide, wide area and data center, and programmability. At ONUG Spring 2015, there was much discussion and interest in Software-Defined Wide Area Network or SD-WAN. The poll below captures key problems IT business leaders seek to solve via SD-WAN. The top two problems the ONUG community seeks to solve with SD-WAN are:

1) Leverage hybrid WAN links, eliminate routing and configuration complexity at remote sites.

2) Application performance management with centralized application policy control, monitoring and management.



While most of the industry has focused on network virtualization, or overlays, and SD-WAN as two separate markets, with separate vendors, there is a growing interest in leveraging the same controller to support both SD-WAN and data center overlays. At the same ONUG Spring 2015 meeting, 63% of the ONUG community voted that it's "*Very important to align SD-WAN w/ service insertion/chaining, that is the control plane should be common in the data center and branch/WAN.*"



Service chaining is fundamental since it provides a DevOps interface into the network fabric, allowing applications to be supported by virtualized and non-virtualized network services. To bridge brownfield and greenfield infrastructure, to enable full utilization of previous investments and newer software-based network services, a partner ecosystem is required around the software-defined network fabric. NEC ProgrammableFlow® Networking Suite fabric ecosystem includes Dell, Palo Alto Networks, F5, Riverbed, NoviFlow, Meru and others. Having these ecosystem partners provides choice and alternatives to IT architects and DevOps groups while providing a means to utilize these IT assets via service chaining.

Service chaining enables dynamic, automated and programmatic inserting of networking services into the path of applications. When most traffic flowed north-south in and out of data center, it was easy to attach a network service to an application by simply placing a hardware network service appliance in the path of the application flow. That is, network engineers would physically cable appliances, such as firewalls, IPS, load balances, etc., together in the application path. Service chaining seeks to logically chain networking services together, on-demand via software, to support north-south and east-west flows. An added benefit of service chaining is the minimization of service interruption as hardware appliances are reduced. Thus, service chaining may leverage both physical and virtual appliances.

NEC Open Data Center Fabric Use Cases

Two examples below offer a means to bring the NEC ProgrammableFlow® SDN solution to life. The first example shows how authentication can be simplified in the most demanding of DMZ environments. The second example illustrates combining of data center fabric, SD-WAN and service chaining into a unified solution.

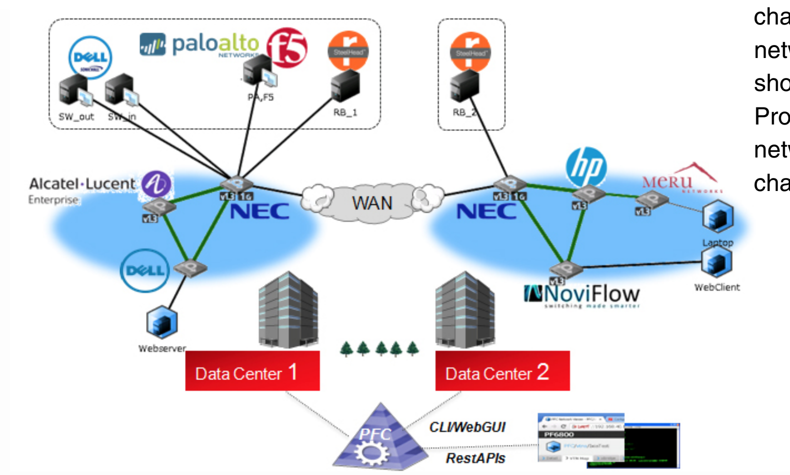
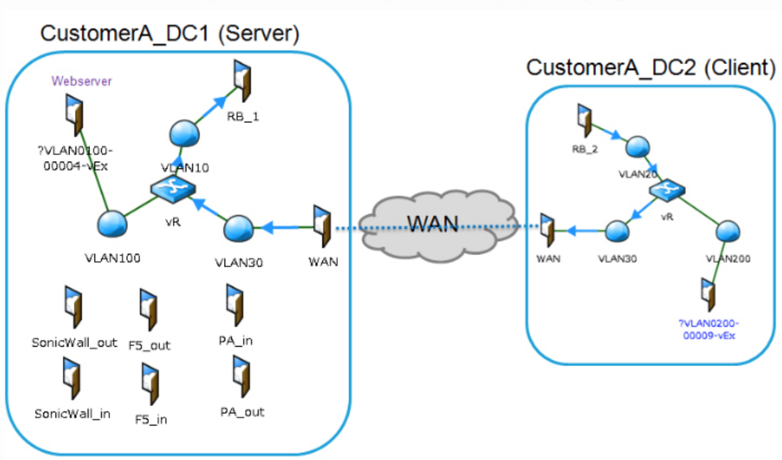


Figure 2-2: Service Chaining over the WAN (Physical Topology)



DMZ Authentication Simplification

Service chaining three appliances, as traffic flows pass through a DMZ, can be significantly simplified with the NEC ProgrammableFlow®. An example, DMZ consists of three hardware appliances: a load balancer and two firewalls. The hardware appliances are used in conjunction with virtualized network software. This combination of hardware and network virtualized services are service chained to the respective applications. The NEC ProgrammableFlow® controller simplifies security authorization by exploiting flow networking characteristics to move traffic to the right network service before it arrives at the appropriate application.

SD-WAN Service Chaining for Inter-Data Center Applications

As noted above, NEC ProgrammableFlow® supports service chaining for both SD-WAN and data center. In this scenario, the ProgrammableFlow controller inserts a WAN optimization service across the WAN in different physical data centers.

The figure highlights new kinds of architecture approaches that are possible with NEC ProgrammableFlow® and its ecosystem partners. The physical topology depicts service chaining over a WAN connection in a ProgrammableFlow network. The ability to place location independent appliances shows the advantage of this architecture. The ProgrammableFlow controller steers traffic to the appropriate network virtualized service resulting in dynamic service chaining.

Industry Recommendations

The transition toward a software-defined infrastructure is not daunting, but IT business leaders need to start pilots now to gain IT skills, understand benefits, limitations and knowledge to plan deployment at scale. It's highly suggested to bring business unit managers into the discussion early to ensure business value creation, as well as buy-in. Most successful pilots start in one of two areas: wide area or data center. As most enterprises have requirements for both, it may be advantageous to seek suppliers that support both use cases in their product set.

Consider suppliers that support a software-defined infrastructure business and product model committed to continued investment in product and service development, as well as a commitment to grow an ecosystem of partners that enable legacy and cloud applications to share the same infrastructure. As nearly all large and small enterprises support legacy and new cloud-based applications, it's suggested that a supplier's ability to embrace both worlds, and its ability to create a bridge toward transition at the IT business leader's pace, be taken into consideration. For example, the ability to leverage previous network service appliance investments is a goal for most IT business leaders; therefore, vendors that support a hybrid model of physical and virtual appliance approaches are best.

About Nick Lippis

Nicholas J. Lippis III is a world-renowned authority on advanced IP networks, communications and their benefits to business objectives. He is the publisher of *the Lippis Report*, a resource for network and IT business decision makers to which over 35,000 executive IT business leaders subscribe. Its Lippis Report podcasts have been downloaded over 200,000 times; ITunes reports that listeners also download the *Wall Street Journal*'s Money Matters, *Business Week*'s Climbing the Ladder, *The Economist* and *The Harvard Business Review*'s IdeaCast. He is also the cofounder and conference chair of the Open Networking User Group, which sponsors a bi-annual meeting of over 500 IT business leaders of the largest enterprises. Mr. Lippis is currently working with clients to design their private and public software-defined infrastructure architectures with open networking and storage technologies to reap maximum business value and outcomes.

He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, the state of Alaska, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cisco Systems, Hewlett Packet, IBM, Avaya and many others. He works exclusively with CIOs and their direct reports. Mr. Lippis possesses a unique perspective of market forces and trends occurring within the computer networking industry derived from his experience with both supply- and demand-side clients.

Mr. Lippis received the prestigious Boston University College of Engineering Alumni award for advancing the profession. He has been named one of the top 40 most powerful and influential people in the networking industry by *Network World*. *TechTarget*, an industry on-line publication, has named him a network design guru while *Network Computing Magazine* has called him a star IT guru.

Mr. Lippis founded Strategic Networks Consulting, Inc., a well-respected and influential computer networking industry-consulting concern, which was purchased by Softbank/Ziff-Davis in 1996. He is a frequent keynote speaker at industry events and is widely quoted in the business and industry press. He serves on the Dean of Boston University's College of Engineering Board of Advisors as well as many start-up venture firms' advisory boards. He delivered the commencement speech to Boston University College of Engineering graduates in 2007. Mr. Lippis received his Bachelor of Science in Electrical Engineering and his Master of Science in Systems Engineering from Boston University. His Masters' thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.