



Lippis Report
Research Note

Lippis Report 164:

**Cisco Builds a Modern Network Service Layer for
Virtualized and Cloud Infrastructure**

Any IT business leader knows that the single most important technology driving data center design change is server virtualization to the point that a virtual machine (VM) is now the data center building block. As server virtualization marches on until nearly every physical server has been virtualized, networking in a virtualized environment is being forced to fundamentally change too. By networking, I mean not only layer 2 and 3 forwarding but network services too, such as application controllers, WAN optimizers, firewalls, etc., which are fundamental for mission critical application performance, cost reduction and high application availability especially where service level agreements are required.



**Cisco Re-defines Networking
with Its Unified Network
Services**

[Listen to the Podcast](#)

Adding new applications to a data center has become highly complex, thanks to all the routing paths that need to be set-up to provide connectivity and reach of network services plus the configuration and policy set-up for network services specific to the application. Then, once the application is operational, it's hard to virtualize it and move it via v-motion, et al, while keeping set-up and policies intact, especially routing paths. The current state of rigid networking consumes time and cost, but most importantly limiting the speed and agility in which new applications can be delivered and businesses react to market dynamics. This is a nasty problem, riddled with complexity and associated cross-administrative operational cost limiting the number of applications that can be virtualized until this problem is solved.

An entirely new approach to deploying, provisioning and managing data center network services in a virtualized environment is needed, and Cisco is addressing this need with its Unified Network Services or UNS. Cisco's UNS is not just a suite of its layer 4-7 network service offerings such as ACE, WAAS, etc., but a framework for transparently inserting network services into a virtual server environment for steering traffic to network services on a per-VM basis plus an extensible and integrated policy management architecture. The key word in UNS is "unified," as UNS makes network services available to both physical and virtual servers and their associated applications via steering traffic to network services hosted in appliances/modules/blades or within a VM. UNS promises to help reduce the costs to deploy new applications plus to enable more applications to be virtualized. In short, UNS offers an approach to deploy, provision and manage new applications without the network set-up complexity mentioned above. In addition, it also promises to remove network complexity associated with virtualizing applications and their moves. UNS is a main pillar of Cisco's Data Center Business Advantage architecture, along with Cisco's Unified Fabric and Unified Computing Services. These pillars combine to form the tightly-integrated next generation data center components including the network, storage, application services, virtualization layers and network services.

Cisco's UNS is addressing mobile (v-motion) applications and their associated changing or dynamic network topology requirements by steering traffic to appropriate network services that are centrally controlled via policy. These network services such as firewalls, application controllers, WAN acceleration, load balancing, etc., can be packaged in appliances, modules, server blades and/or other form factors and/or increasingly as a virtualized service. UNS is a modern approach to applying layer 4-7 network services to both non-virtualized applications and VMs, while in the process solving some of the most complex problems associated with virtualized infrastructure.

Dedicated Hardware Services to Virtualized Network Services

Traditional network services are frequently placed in-line or in the flow of traffic, that is firewall, IPS, load balancing, application controllers, WAN acceleration, etc., forming a line of layer 4-7 network services. But as applications are virtualized, their movement may take them out of the path of traffic flow, thus creating difficulty to maintain network services to VMs and their applications. In most data centers, a mix of physical and virtual network services is emerging as well as a mix of virtual servers and physical servers based upon old and new investment. What IT business leaders demand is that their investment in physical and/or virtual network services support both virtualized and non-virtualized applications so they may extract the highest value from their IT dollars. This is a hard problem to solve and requires new thinking in networking which is what UNS is focused upon delivering. In short, UNS allows a mix and matching of physical and virtual network services to support either virtualized or non-virtualized applications through a more flexible approach to networking and policy management. So how do IT architects create this level of flexibility?

In a UNS environment, the physical placement of network services in appliance/modules/server blades, etc., or virtualized form is moot, offering IT architects a new degree of freedom to access these services anywhere in a virtualized infrastructure. A network service can be offered to a VM and its associated traffic, independent upon its form factor, be it a physical appliance, dedicated module or virtualized network service as long as the VM and softswitch send traffic to the appropriate service as the application moves around the data center.

That's important as traffic patterns have shifted from primarily north-south to a mix of east-west and north-south, resulting in the need for network services to offer far greater flexibility in their reach to service VMs and the applications they contain. And as network services are logically wrapped around a VM via policy, they receive the benefit of all moving together, solving one of the biggest virtualization problems in the industry, manually intensive change management. Parallel to making network services accessible independent upon location and its packaging is the added benefit of virtualizing network services as this will decrease the number of hardware appliances in a data center, reducing complexity, total cost of ownership and energy consumption.

Unified Network Services Is a Platform for Inter-Cloud Mobility and On-Demand Provisioning

But perhaps even more important than solving the immediate change management problem is that unified network services deliver a set of attributes that put in place the tools and ability to deliver elastic IT services between clouds—the holy grail of cloud computing. With core network services unified, a degree of flexibility is gained far beyond current technology and offers a platform in which service advertising and registry can occur so that a “provision proxy” can automate network service configuration to meet new IT service delivery needs in near real time; but this is a topic for another day. The important point is that a unified network service is a platform that all large IT firms, cloud providers and enterprises will be investing in over the next business cycle.

Cisco's Unified Network Services or UNS

In this Research Note, we review Cisco's UNS, the most comprehensive approach to data center and cloud network service deployments in the industry thus far. UNS addresses the on-demand provisioning problem so sought after in virtualized infrastructure. That is when IT leaders need to allocate resources from within or between a private or public cloud on demand and quickly, UNS will respond to a capacity request so that network services are provisioned in the right order, at the right capabilities and within minutes rather than months. In short, UNS's vision is to enable on-demand network service delivery and

on-demand provisioning to accommodate VM container workload mobility within the construct of an Enterprise's IT model or service architecture.

The Virtual Security Gateway

UNS is both a vision of on-demand service provisioning and the products that enable its construct. Within UNS, Cisco has launched its data center firewall called VSG or Virtual Security Gateway, and is on a path of virtualizing its data center service products including the Wide Area Application Services or WAAS, et al, and providing them with consistent policies via its VNMC or Virtualized Network Management Control software. VSG is an example of a virtual service node, as compared to physical ASA security appliances. The key underpinning technology to VSG is the Nexus 1000v and vPATH, which enable traffic to be re-routed or steered to the virtual firewall nodes; more on this below.

Cisco's VSG offers a model of how network services are virtualized and in the process, solves some of the biggest server virtualization problems while delivering added flexibility value. VSG is a proof-point of Cisco's ability to solve the firewall problem within virtualized infrastructure; that is how to provide firewall services to flows destined to and between various VMs. vPATH, a software module within the Nexus 1000v softswitch, steers traffic to VSG, the firewall, which blocks or allows traffic flow to its destination. Further, VSG assures that the correct network security service is applied and a VM's policies follow it as it moves between physical servers. VSG policy is centrally managed through the VNMC umbrella management platform.

Central to UNS is vPATH technology that confers the same VSG benefits discussed above to Cisco's new Virtual WAAS or vWAAS WAN acceleration offering. vPATH is fundamental to UNS as it delivers unification by being the same underlying infrastructure for both VSG and vWAAS. Therefore, by inserting vPATH technology/software into the virtual switch, hypervisors and VM's traffic is re-directed as needed to deliver network services, such as firewall, WAN acceleration, etc.

vPATH

In the case of VSG, through VNMC, policy is created to define what type of traffic needs to be redirected, and then what action to take upon that traffic once it arrives at the firewall. As traffic reaches a server or Nexus 1000v, it is intercepted as it's destined for a particular VM by vPATH, which redirects it to VSG for inspection. VSG then performs its network security service then forwards the traffic, if allowed, to its destination just like a firewall appliance operates.

The closest analogy to describe vPATH's function is network-based application recognition. That is NBAR analyzes traffic and classifies it, and then performs a function such as prioritization. Thus, vPATH intercepts traffic and sends it to VSG while VSG performs its security service and decides if traffic will be forwarded to the destination VM.

Fast Path

vPATH also benefits from a concept called fast path. Fast path is similar to a cut-through method in that once traffic has been forwarded to VSG for firewall services, for example, the remaining traffic flow, it's routed directly to its VM destination. Note that fast path can be utilized for most network services. Fast path obviates the need to route all traffic through VSG once the first packet of the flow has been processed by the firewall. Therefore, all traffic does not require packet-by-packet inspection, speeding up flows and reducing processing and latency.

For example, if the first packet of a flow passes through VSG without alteration, then the rest of the flow should pass uninspected as the security rules are the same. However, this wouldn't be the case for an IPS system, where the entire payload is inspected to assure there is no malware residing in the flow. Fast path will evolve to support various traffic scenarios too.

Network Service Chaining

Cisco's UNS provides a solution to the challenge of providing network services to traffic flows within a virtualized infrastructure that stick to VMs as they move and change physical location in the data center. The next challenge is to provide virtualized network service chaining. Chaining network services is the ability to create a single policy for traffic flows as it ingresses to a VM for multiple network services. For example, a policy may apply firewall, load-balancing, WAN-optimization, etc., to a flow and route that traffic through subsequent services, as opposed to having to create unique policies, intercept each one and route traffic accordingly. Chaining is a huge operational time saver, and it hastens the flow of traffic within the data center. vPATH is one underlying mechanism that can steer traffic to services in the right chain/order.

The UNS Value Proposition

From a data center network design perspective, UNS is developing a set of network service building blocks that brings physical network service appliances and virtual service nodes into virtualized environments along with the tools to apply policies to govern their use. As more and more data centers become virtualized so too will network services. In addition, as physical and virtual data centers will co-exist for many years to come, the ability to offload physical network appliances with virtualized ones as well as pass traffic between them offers a transition path and a means to extend the life of existing appliance investments.

As mentioned above, physical data centers are equipped with stacks of appliances offering load balancing, WAN acceleration, firewalls, IPS, etc. Now with service chaining and vPATH, all of these physical and virtualized appliances can be put to work servicing VMs and their applications. Most importantly though is that UNS offers a way to control network services so that VMs, virtual applications and mobile workloads can be scaled up and down plus moved within a dynamic network that allows provisioning services easily. For all intents and purposes, the industry has not had a multi-service chaining mechanism in the physical world. IT operations have done this manually via provisioning VLANs, policy routing, Web Cache Communications Protocol or WCCP, etc. But the old approach is static, and when servers, applications, appliances, etc., move or change, manual intervention is required. The beauty is that chaining network services in a virtualized infrastructure enables elastic scale-up and scale-down much more seamlessly.

Why Unify Network Services

One of the key strategic elements behind UNS is to change the mindset in which IT leaders deploy network services. Traditionally network service appliances were deployed at the edge of the data center or in front of a specific application server. But servers and application are often moved creating the manual re-configuration problem discussed above. Having common accessible network services in private and public data center clouds could offer huge provisioning benefits. For example, there could be, potentially, a vWAAS instantiation in Amazon EC2, Rackspace, GoGrid, etc, which IT leaders who have deployed WAAS in their branch offices could leverage, meaning their WAN would be accelerated thanks to a common WAAS image in the branch and cloud providing that network service independent upon

these two application deployment models. This new network services deployment model attempts to blend the worlds of Cisco's borderless and data center initiatives to the fullest extent.

What's the intrinsic value of making a network service virtualization? In the case of vWAAS, Cisco is able to give IT leaders flexibility of placement and IT delivery. vWAAS is easier to scale up, licensed in a "pay as you grow" model, offers fewer devices to manage with less power and cooling cost plus is overall more flexible in its placement. In addition, vWAAS and WAAS can both offer WAN acceleration services to virtualized applications thanks to vPATH increasing the usefulness and value to both. vWAAS may be deployed by cloud providers too, which could offer IT leaders a WAN acceleration option independent upon application hosting.

Distributed Deployment with Centralized Management

Value is gained by being able to deploy network services in a distributed fashion, thanks to UNS. UNS changes network service deployment from a centralized model to distributed. But while virtualized network services are distributed, its management is centralized, offering operational efficiency and deployment flexibility. Distributed network service deployment with centralized management is the only approach that works as virtualized network services tend to be distributed widely. In fact, large data centers and clouds will see their instantiations of a particular service grown from a few hundred to thousands, if not more. Therefore, centralized management of virtualized network services provide the control knobs to provision, develop policy, steer traffic, etc., for thousands of virtualized network services distributed throughout a virtualized infrastructure. For example, in Cisco's UNS, vWAAS and VSG run in their own VM, either on a single physical server or multiple physical servers, offering a highly distributed network service option.

Other companies, such as A10 and at least five others, are virtualizing their application delivery offering too. And cloud service providers are seeking virtualized network services, which will offer IT business leaders the ability to deploy applications from either private or public clouds with a common set of network services over time. For example, many public cloud providers would like to place load-balancing services on top-of-rack and deploy it in a small-medium-large type format. Further, many would also like to place load-balancing services on a compute platform to give customers the ability to deploy load-balancing pseudo-traditionally. That is to deploy network services where a compute platform would be largely dedicated to that service, or, alternatively, distributed so that it does not necessarily reside top-of-rack, or centralized, but resides "logically" next to a VM or sets of VMs so that as VMs move the network service benefit followings.

UNS: A Product Set or Next Evolution of Networking and Computer Services

Now Cisco isn't the only IT firm developing a unified network service framework, but it is the only company that has all the components to deliver a comprehensive and thoughtful solution. For example, HP, IBM and Oracle do not develop load balancing, application delivery, WAN acceleration or softswitch network services, placing them at a disadvantage. Oracle, HP and IBM usually partner with others for these services such as F5, Riverbed, VMWare, etc., eliminating the opportunity for this level of virtualization and unification development. In HP's case, its networking gear is increasingly made in China which lacks the forward-looking foresight to get in front of this opportunity. IBM usually does a really good job here, but it's limited on these major network service components.

Many of the niche players, such as F5, Riverbed, Infoblox, A10, et al, will and are virtualizing their network service appliances and will do it very well, emerging as feature functional leaders. But these firms' virtualization strategies will lack the broad view of multiple network services and most importantly, how the network nodes (L2-3 infrastructure) or hypervisor can steer traffic to them. To gain a broader UNS view and solution, these firms could organize a consortium to develop a comprehensive UNS strategy and implementation that matches Cisco's UNS. But consortium is driven by committee, which usually moves slowly. Cisco's UNS framework will be emulated by others while key technology layers can be standardized, such as Cisco's proposed VN-Link for traffic steering to physical devices from a virtual/softswitch. Hopefully, an ecosystem can be created that allows all vendors to participate, because UNS is not just another vision and product line, but it's the next evolution of networking and computing services.

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 160,000 times; i-Tunes 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. Mr. Lippis is currently working with clients to design their private and public virtualized data center cloud computing network architectures to reap maximum business value and outcome.

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, Cigitel, 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 firm's 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.