The VMware NSX Network Virtualization Platform

VMware Solutions: Designed for Early and Ongoing Success

TECHNICAL WHITE PAPER

Table of Contents

Executive Summary

VMware's Software Defined Data Center (SDDC) vision leverages core data center virtualization technologies to transform data center economics and business agility through automation and non-disruptive deployment that embraces and extends existing compute, network and storage infrastructure investments. Enterprise data centers are already realizing the tremendous benefits of server and storage virtualization solutions to consolidate and repurpose infrastructure resources, reduce operational complexity and dynamically align and scale their application infrastructure in response to business priorities. However, the data center network has not kept pace and remains rigid, complex, proprietary and closed to innovation – a barrier to realizing the full potential of the virtualization and the SDDCs.

The VMware NSX network virtualization platform provides the critical third pillar of VMware's Software Defined Data Center (SDDC) architecture. NSX network virtualization delivers for networking what VMware has already delivered for compute and storage. In much the same way that server virtualization allows operators to programmatically create, snapshot, delete and restore software-based virtual machines (VMs) on demand, NSX enables virtual networks to be created, saved and deleted and restored on demand without requiring any reconfiguration of the physical network. The result fundamentally transforms the data center network operational model, reduces network provisioning time from days or weeks to minutes and dramatically simplifies network operations.

NSX is a non-disruptive solution that is deployed on any IP network, including existing data center network designs or next generation fabric architectures from any networking vendor. With NSX, you already have the physical network infrastructure you need to deliver a software defined data center.

Networking is Stuck in the Past

Traditional approaches to networking not only prevent today's organizations from realizing the full promise of the software defined data center, but also subject them to limited flexibility and operational challenges.

The Glass is only Half Full

Server and storage virtualization solutions have dramatically transformed the data center by delivering significant operational savings through automation, capital savings through consolidation and hardware independence, and greater agility through on-demand and self-service approaches to provisioning. As significant as these gains have been, however, much of the potential for these solutions remains untapped. More to the point, these businesses are being held back, by an antiquated network operationaL.

Networking and network services have been stuck in the status quo and are out-of-step with server and storage solutions that can be quickly provisioned but are constrained by networking services that still require manual provisioning and are anchored to vendor specific hardware and topology. This directly impacts application deployment time because applications need both compute and networking resources.

Network provisioning is slow. The current operational model has resulted in slow, manual, error-prone provisioning of network services to support application deployment.. Network operators are dependent on terminal, keyboard, scripting and CLIs to manipulate a multitude of VLANs, firewall rules, load balancers and ACL, QoS, VRF and MAC/IP tables. Complexity and risk are further compounded by the need to ensure that changes to the network for one application do not adversely impact other applications . Given the complexity of this situation, it's no surprise that several recent studies point to manual configuration errors as the cause for more than 60% of network downtime and/or security breaches. The result is that in addition to the frequent, inevitable configuration mis-steps, IT response time to new business requirements is too slow, as rapidly re-purposed compute and storage infrastructure must still wait for the network to catch up.

Workload placement and mobility is limited. The current device-centric approach to networking confines workload mobility to individual physical subnets and availability zones. In order to reach available compute resources in the data center, network operators are forced to perform manual box-by-box configuration of VLANs, ACLs, firewall rules, and so forth. This process is not only slow and complex, but also one that will eventually reach configuration limits (e.g., 4096 for total VLANs). Organizations often resort to expensive over-provisioning of server capacity for each application/networking pod, resulting in stranded resources and sub-optimal resource utilization.

Additional Data Center Networking Challenges

Related challenges data center networking teams face with traditional networking approaches include:

- VLAN sprawl caused by constantly having to overcome IP addressing and physical topology limitations required to logically group sets of resources
- Firewall rule sprawl resulting from centralized firewalls deployed in increasingly dynamic environments coupled with the common practice of adding new rules but rarely removing any for fear of disrupting service availability;
- Performance choke points and increased network capacity costs due to the need for hair-pinning and multiple hops to route traffic through essential network services that are not pervasively available. The increase of East-West traffic in a data center exacerbates this problem
- Security and network service blind spots that result in choosing to avoid hair-pinning and other deploy risky routing schemes
- Increased complexity in supporting the dynamic nature of today’s cloud data center environments.

It’s Time to Virtualize the Network

The solution to these challenges is to virtualize the network. Do for networking the same thing that has been done for compute and storage. In fact, network virtualization is conceptually very similar to server virtualization (see Figure 1).

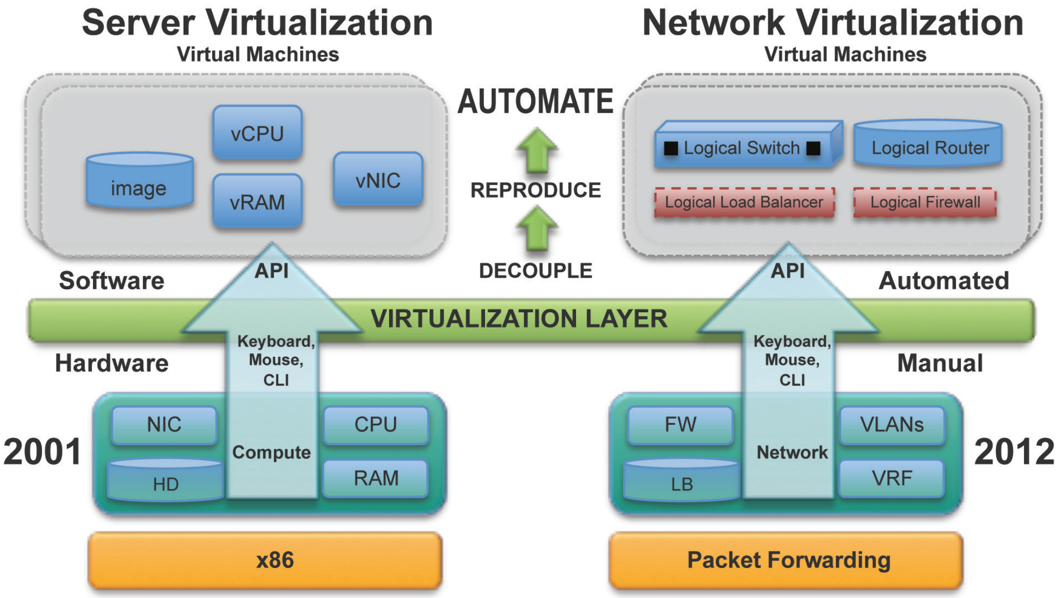
With server virtualization, a software abstraction layer (server hypervisor) reproduces the familiar attributes of an x86 physical server (e.g., CPU, RAM, Disk, NIC) in software, allowing them to be programmatically assembled in any arbitrary combination to produce a unique virtual machine (VM) in a matter of seconds.

With network virtualization, the functional equivalent of a “network hypervisor” reproduces the complete set of Layer 2 to Layer 7 networking services (e.g., switching, routing, access control, firewalling, QoS, and load balancing) in software. As a result, they too can be programmatically assembled in any arbitrary combination, this time to produce a unique virtual network in a matter of seconds.

Not surprisingly, similar benefits are also derived. For example, just as VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand.

More importantly, network virtualization provides a strong foundation for resolving the networking challenges keeping today's organizations from realizing the full potential of the software defined data center (see text box "Why the Software defined Data Center Makes More Sense")

Figure 1: How Network Virtualization Parallels Server Virtualization.



Why the Software defined Data Center Makes More Sense

The software defined data center (SDDC) approach to building next generation data centers has several compelling advantages over emerging hardware defined data center (HDDC) alternatives. First and foremost, SDDC is proven. Indeed, building advanced, software-based intelligence into their applications and platforms is what has enabled Google and Amazon to deliver the largest, most agile and efficient data centers in the world today. Another major advantage of SDDC is that innovation occurs at the speed of software releases, instead of being tied to ASIC and hardware-upgrade cycles of three to five years, or more. Moreover, adopting new innovations no longer requires forklift hardware upgrades. Best of all, a software defined data center works with the physical infrastructure you already have and can be deployed non-disruptively alongside your existing configurations at whatever pace your organization chooses.

Introducing VMware NSX – The Platform for Network Virtualization

VMware NSX is the market leading implementation of network virtualization from VMware. By delivering a completely new operational model for networking that breaks through current physical network barriers, NSX enables data center operators to achieve orders of magnitude better agility, economics, and choice.

With NSX, virtual networks are programmatically created, provisioned and managed, utilizing the underlying physical network as a simple packet forwarding backplane. Network and security services in software are distributed to hypervisors and “attached” to individual VMs in accordance with networking and security policies defined for each connected application. When a VM is moved to another host, its networking and security services move with it. And when new VMs are created to scale an application, the necessary policies are dynamically applied to those VMs as well.

NSX is completely non-disruptive solution:,

- Deploys on hypervisors connected to any existing physical network infrastructure and supports next-generation fabrics and topologies from any vendor;
- Requires no changes to existing applications and workloads
- Allows IT departments to incrementally implement virtual networks at whatever pace they choose (without any impact to existing applications and network configurations)
- Extends visibility to existing networking monitoring and management tools to deliver increased visibility into virtualized networks

The net result is a transformative approach to data center networking that – among its many other benefits – matches the velocity demands of today’s businesses by reducing service delivery times from weeks to seconds.

How VMware NSX Works

The following diagrams reveal the fundamentals of how NSX works. They also set the stage for further exploring the technical characteristics, capabilities, and value propositions that define the NSX solution.

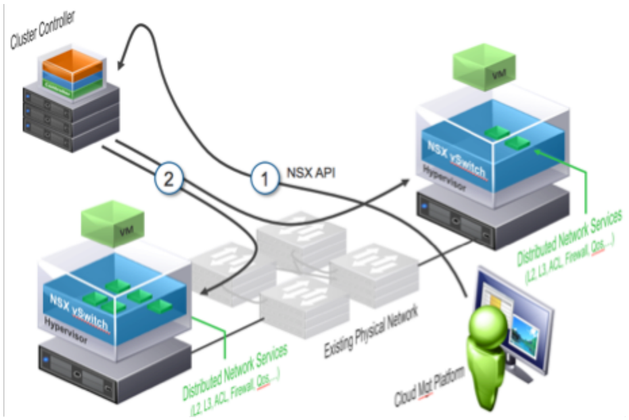

Cluster Controller
1
NSX API
2
VM
NSX vSwitch
Hypervisor
VM
NSX vSwitch
Hypervisor
Distributed Network Services
(L2, L3, ACL, Firewall, Qos...)
Distributed Network Services
(L2, L3, ACL, Firewall, Qos...)
Existing Physical Network
Cloud Mgt Platform

Figure 2: NSX is a multi-hypervisor solution that leverages the vSwitches already present in server hypervisors across the data center. NSX coordinates these vSwitches and the network services pushed to them for connected VMs to effectively deliver a platform – or “network hypervisor” – for the creation of virtual networks.

Similar to how a virtual machine is a software container that presents logical compute services to an application, a virtual network is a software container that presents logical network services – logical switches, logical routers, logical firewalls, logical load balancers, logical VPNs and more – to connected workloads. These network and security services are delivered in software and require only IP packet forwarding from the underlying physical network.

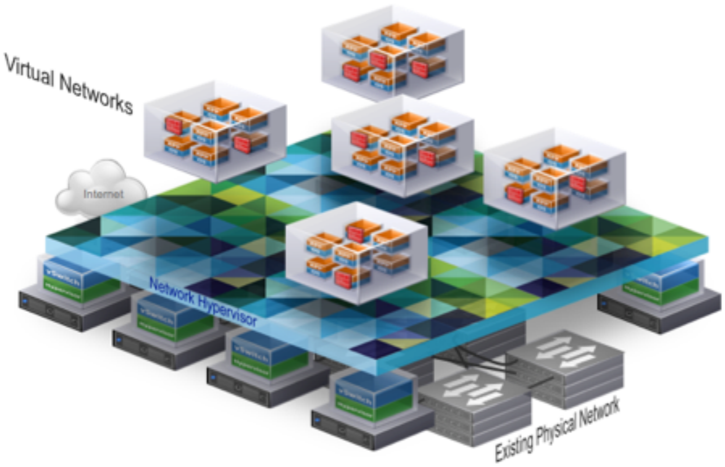


Figure 2: The “Network Hypervisor”

Figure 3: Virtual networks are provisioned by taking advantage of a cloud management platform (CMP) which uses the RESTful API exposed by the NSX Controller to request the virtual network and security services be instantiated for the corresponding workloads (step 1). The Controller then distributes the necessary services to the corresponding vSwitches and logically attaches them to the corresponding workloads (step 2).

This approach not only allows different virtual networks to be associated with different workloads on the same hypervisor, but also enables the creation of everything from basic virtual networks involving as few as two nodes, to very advanced constructs that match the complex, multi-segment network topologies used to deliver multi-tier applications.

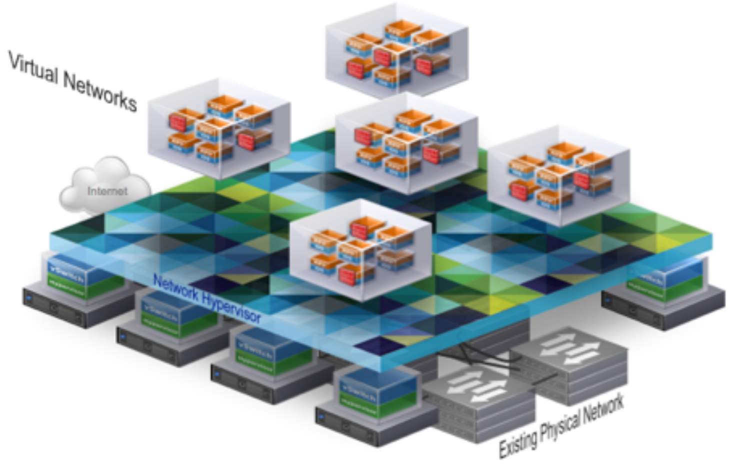


Figure 3: Virtual Network Provisioning

Figure 4: To connected workloads, a virtual network looks and operates like a traditional physical network. Workloads “see” the same Layer 2, Layer 3, and Layer 4-7 network services that they would in a traditional physical configuration. It’s just that these network services are now logical instances of distributed software modules running in the hypervisor on the local host and applied at the vSwitch virtual interface. applications.

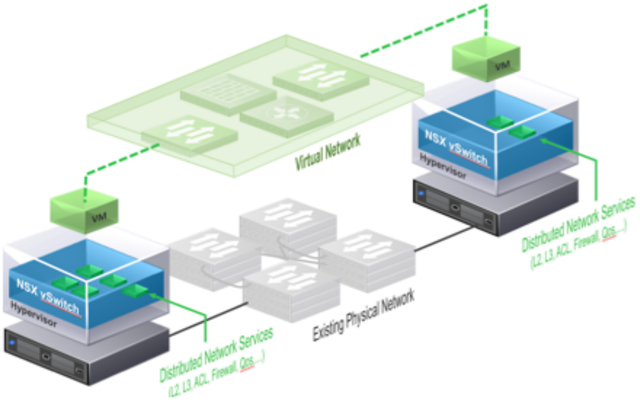

Virtual Network
VM
VM
NSX vSwitch
Hypervisor
NSX vSwitch
Hypervisor
Distributed Network Services
(L2, L3, ACL, Firewall, Qos...)
Distributed Network Services
(L2, L3, ACL, Firewall, Qos...)
Existing Physical Network

Figure 4: The Virtual Network – From the Workload’s Perspective (i.e., Logical)

Figure 5: To connected workloads, a virtual network looks and operates like a traditional physical network. Workloads “see” the same Layer 2, Layer 3, and Layer 4-7 network services that they would in a traditional physical configuration. It’s just that these network services are now logical instances of distributed software modules running in the hypervisor on the local host and applied at the vSwitch virtual interface. applications.

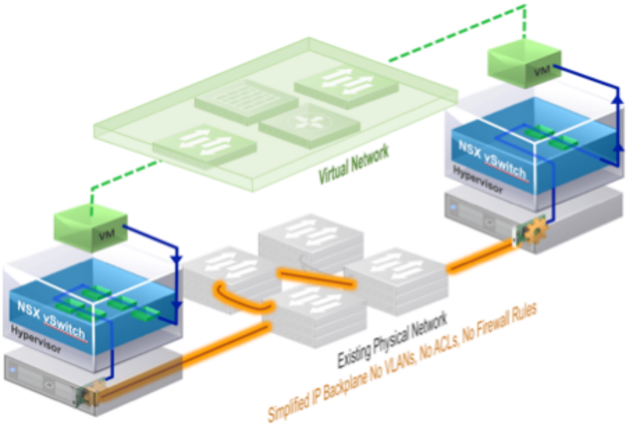

Virtual Network
VM
VM
NSX vSwitch
Hypervisor
NSX vSwitch
Hypervisor
Existing Physical Network
Simplified IP Backplane No VLANs, No ACLs, No Firewall Rules

Figure 5: The Virtual Network – From the Network’s Perspective (i.e., Physical)

Figures 6a and 6b: The ability to apply/enforce security services at the vSwitch virtual interface also eliminates "hair-pinning" – an unfortunate "feature" of traditional physical network architectures where East-West communications traffic – for example, between two VMs on the same hypervisor but in different subnets – is required to traverse the network to reach essential services, such as routing and firewalling. With NSX, inefficient traffic patterns such as these, which often lead to core link over-subscription, become a thing of the past.

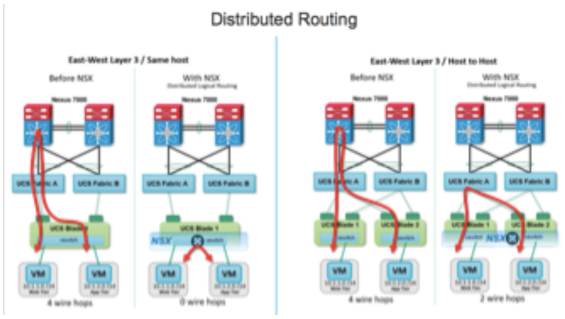


Figure 6a: Distributed Routing with NSX

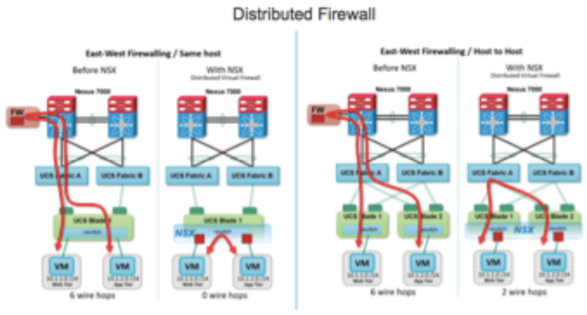


Figure 6b: Distributed Firewall with NSX

Compelling Technical Features and Characteristics

Several key features and characteristics are instrumental to the value NSX delivers, both to IT and the business at-large. These include the ability to work with your existing network infrastructure, support progressive adoption of network virtualization, and substantially reduce network complexity.

NSX fits right in. Simply put, NSX works with:

- Any application. Workloads/applications need not be modified in anyway as the virtual network appears no different to them than the physical network.
- Any hypervisor. Out-of-the box support is available for many hypervisors (e.g., Xen, KVM, and VMware ESXi), while coverage can be extended to others (e.g., Microsoft Hyper-V) by re-configuring them to incorporate standard vSwitch capabilities.
- Any network infrastructure. Hardware independence is achieved based on the fact that NSX virtual networks require nothing more than connectivity and packet-forwarding from the underlying IP infrastructure.
- Any cloud management platform. Out-of-the-box support is available for many cloud management platforms (including CloudStack, OpenStack, VMware vCloud Automation Center,), and integration with other management platforms is provided through the NSX API.

NSX network virtualization is not an all-or-nothing proposition. Because NSX virtual networks require no configuration changes to the underlying physical network (outside of allowing NSX encapsulated packets through existing firewalls) they transparently co-exist with existing application deployments on the physical network today. IT departments have the flexibility to virtualize portions of the network by simply adding hypervisor nodes to the NSX platform. In addition, Gateways – available as software from VMware or top-of-rack switch hardware from several NSX partners – deliver the ability to seamlessly inter-connect virtual and physical networks. These can be used, for example, to support Internet access by workloads connected to virtual networks, or to directly connect legacy VLANs and bare metal workloads to virtual networks.

NSX simplifies networking. NSX abstracts virtual networks from the underlying physical network enabling increased automation. Operators are not required to interact with the physical network and are therefore spared the inconsistencies across platforms. Operators no longer need to deal with VLANs, ACLs, spanning trees, complex sets of firewall rules, and convoluted hair-pinning traffic patterns – because these are no longer necessary when the network is virtualized. NSX network virtualization is not an all or nothing proposition. As organizations incementally employ NSX virtual networks, they can increasingly streamline their physical network configuration and design. Vendor lock-in becomes a thing of the past, since the physical network only needs to deliver reliable high-speed packet-forwarding, it's then possible to mix and match hardware from different product lines and vendors.

NSX provides essential isolation, security, and network segmentation. Because each virtual network operates in its own address space, it is inherently isolated from all other virtual networks, and the underlying physical network, by default. This approach effectively delivers the principle of least privilege, without the need for physical subnets, VLANs, ACLs, or firewall rules. It also makes it possible to have separate development, test and production virtual networks – each with different application versions but using the same IP addresses – all operating at the same time and on the same underlying physical infrastructure. In addition, NSX virtual networks can easily support multi-tier network environments. For example, multiple Layer 2 segments, Layer 3 segmentation, and/or micro-segmentation on a single Layer 2 segment (using distributed firewall rules) can all be implemented in whatever combination is needed to effectively segment traffic between the different components of an n-tier web application.

NSX delivers proven performance and scale.

- The processing required for execution of distributed network services is only incremental to what the vSwitch is already doing for connected workloads – typically between 25% and 50% of one core on each host
- The vSwitch, along with all of the NSX network services run as a kernel-integrated module
- Virtual network capacity scales linearly (alongside VM capacity) with the introduction of each new hypervisor/host adding 40 Gbps of switching and routing capacity and 30 Gbps of firewalling capacity
- Key components, such as the NSX Controller, feature a scale-out architecture that enables seamless scaling of additional capacity, while also delivering service provider class high-availability

The outcome is real-world, production NSX deployments where a single controller cluster is being used to deliver over 10,000 virtual networks in support of over 100,000 virtual machines.

NSX enables unparalleled visibility: With the traditional approach to networking, configuration and forwarding state is spread across a multitude of disparate network devices. This situation often impairs visibility and can impede related troubleshooting efforts. In comparison, NSX provides all configuration and state information for all network connections and services in one place. Connectivity status and logs for all NSX components and virtual network elements (logical switches, routers, etc.) are readily accessible, as is the mapping between virtual network topologies and the underlying physical network. Furthermore, network administrators can continue to take advantage of all the familiar monitoring, management, and analysis tools they've been using right along.

NSX is extremely flexible, highly extensible, and widely supported. A powerful traffic steering capability allows any combination of network and security services to be chained together in any order as defined by application policies, for every application workload. This high degree of flexibility applies not only for native NSX services, but also for a wide variety of compatible third-party solutions – including virtual and physical instances of next generation firewalls, application delivery controllers, and intrusion prevention systems. By enabling network and security teams to leverage familiar products and technologies within the virtual network environment, NSX increases operational efficiency and ensures consistent service delivery while allowing organizations to extract maximum value from their existing investments in hardware-based networking and security solutions. The availability of an extensive array of NSX-compatible partner products is also indicative of the broad industry acceptance and backing for the new operational model delivered by NSX network virtualization.

A Proven Solution with Many Powerful Use Cases. NSX has been deployed in full production, at scale, by several of the largest cloud service providers, global financials and enterprise data centers in the world. AT&T, NTT, Rackspace, eBay, and PayPal are just a handful of the companies that have virtualized their networks with NSX and are now benefiting from the speed and operational efficiency this game changing solution delivers. Typical use cases include:

Data Center Automation

- rapid application deployment with automated network provisioning in lock-step with compute and storage provisioning
- quick and easy insertion for both virtual and physical services

Data Center Simplification

- freedom from VLAN sprawl, firewall rule sprawl, and convoluted traffic patterns
- isolated development, test, and production environments all operating on the same physical infrastructure

Data Center Enhancement

- fully distributed security and network services, with centralized administration
- push-button, no-compromise disaster recovery / business continuity

Multi-tenant Clouds

- automated network provisioning for tenants while enabling complete customization and isolation
- maximized hardware sharing across tenants (and physical sites)

Compelling Capabilities and Business Value

The technical foundation put in place by the NSX network virtualization platform paves the way for several compelling IT/networking capabilities and a number of key value propositions.

NSX accelerates network provisioning and streamlines operations. NSX reduces both the effort and time to provision network and security services - from weeks to minutes With NSX:

- Network engineers no longer need to scrutinize each network configuration change to ensure it will notadversely impact delivery of other applications . With NSX each virtual network is not only customizable for the workloads it supports but also isolated from all other virtual networks
- Network administrators no longer need to bounce between multiple fragmented management consoles. All requisite network services can be configured and monitored from a single interface
- Network administrators can leverage a new operational approach to networking that allows them to programmatically create, provision, snapshot, delete and restore complex networks all in software

Most importantly, by aligningnetwork and security provisioning with compute/storage provisioning, NSX enables organizations to develop, test and deploy new applications faster than ever before. For many NSX customers a faster time-to-market has resulted in a tangible competitive advantage and increased top line revenue by.

NSX provides flexible, highly adaptable networking. Traditional networks are rigid, and their functionality is slow to evolve. In comparison, NSX virtual networks can be re-configured on the fly, and new services – whether they are virtual or physical – can be inserted as needed, and as they become available. In addition, networking features and capabilities now evolve at software release cycle speeds (months) instead of hardware release cycle and refresh/upgrade speeds (years). Other aspects of the solution also deliver tremendous flexibility. For example, the ability of NSX virtual networks to accommodate overlapping IP addresses and provide Layer 2 adjacency between geographically dispersed data centers makes it considerably easier for organizations to take advantage of hybrid cloud configurations (e.g., for cloud offload/bursting). A software defined data center architecture, leveraging NSX network virtualization also allows data centers, either internal or external, to have different physical network hardware. This supports easy integration for data center mergers and acquisitions and the broadest choice of external services providers. In comparison, an HDDC architecture would require that all data centers, whether internal or external, have the same version of physical hardware to deliver consistent services.

NSX enables unrestricted workload mobility and placement. With NSX, workloads can freely move (or "vMotion") across subnets and availability zones, and their placement is not dependent on the physical topology and availability of physical network services in a given location. Everything a VM needs from a networking perspective is provided to it by NSX, wherever it physically resides. An important benefit of this capability is that it's no longer necessary to over-provision server capacity within each application/network pod. Instead, organizations can take advantage of available resources wherever they're located, thereby allowing substantially greater optimization of resource utilization and consolidation.

NSX dramatically enhances network security. NSX improves network security in several distinct ways. To begin with, policies can be applied more granularly. Instead of being tied primarily (or even solely) to IP addresses, rules can be enabled based on virtual containers, applications, and Active Directory identities – and they can be richer too, for example, by taking advantage of VM introspection capabilities. Two other gains in this area are the result of policy enforcement becoming both more dynamic and more distributed.

- Dynamic network security – With NSX virtual networks, security policies are automatically attached to workloads at the time of VM creation based on a flexible, hierarchical policy model. Moreover, not only do these policies *and the capabilities to enforce them* migrate along with their respective VMs, but centrally made changes to the policies are immediately distributed to each virtual network that is impacted.
- Distributed network security – With NSX virtual networks, security policies – including those associated with inserted physical security services – are enforced at the very edges of the network (i.e., at the ingress/egress ports of each workload's hypervisor-based vSwitch). This approach is far more effective than that used with traditional physical networks, where organizations typically rely on a handful of centrally located security devices (which are blind to the majority of east-west traffic), and/or resort to an excessive amount of hair-pinning to ensure that inter-VM traffic gets properly controlled and inspected.

NSX enables push-button, zero-compromise disaster recovery. With the traditional approach to networking, utilizing a back-up site for disaster recovery requires striking a balance between cost and capabilities. Rather than faithfully reproducing their network topology and services in a second location, most organizations opt for a "good enough" solution where tradeoffs made to reduce costs translate into diminished capabilities relative to their primary data center. NSX eliminates the need to compromise. With NSX network virtualization running alongside the organization's compute and storage virtualization solutions, IT can snapshot a complete "application architecture" and then ship a copy off to a disaster recovery site where it's on standby for push-button recovery – on any hardware and without any fall-off in functionality.

NSX reduces network TCO. NSX delivers numerous opportunities for reducing both operational and capital expenditures related to networking. For example, NSX:

- Automates network provisioning and configuration, while also eliminating manually introduced errors and downtime

- Streamlines ongoing administration, monitoring, and troubleshooting by enhancing network visibility and eliminating the need to navigate and maintain VLANs, ACLs, and complex firewall rule sets
- Obviates the need to invest in separate, standalone solutions for many of the networking and security functions that are fundamental to data center networking, including distributed routing, firewalling and load balancing
- Requires fewer switch ports and less switching capacity overall – as a result of reducing the need for standalone networking and security appliances and eliminating the need for traffic hair-pinning, respectively
- Allows selection of least-cost networking equipment – as all that's needed when building/extending physical networks are basic forwarding and resiliency capabilities
- Enables "data center de-fragmentation" – as server utilization can be optimized across application/networking pods and even greater degrees of data center consolidation can be achieved
- Eliminates the need to purchase new networking equipment and/or conduct forklift upgrades in order to take advantage of new innovations in networking technology
- Supports development, testing, and production "environments" all on the same physical infrastructure

The result is the ability for both enterprises and service providers to save thousands – if not millions – of dollars in periodic and recurring costs associated with their networks.

Unleashing the Software defined Data Center

The platform for network virtualization, VMware NSX decouples network services from the data center network hardware, reproducing and making them available in software so they can be programmatically configured in lockstep with the workloads they serve, in any combination and location needed. By matching the capabilities and benefits derived from familiar server and storage virtualization solutions, this transformative approach to networking unleashes the full potential of the software defined data center – enabling data center managers to achieve orders of magnitude better agility, economics, and choice. Furthermore, NSX accomplishes all of this in a way that allows organizations to fully leverage their existing physical network infrastructure and investments. With NSX, organizations already have the network needed for the next-generation data center today.

For more information, please visit www.vmware.com/products/nsx/

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com