# WHAT IS NETWORK VIRTUALIZATION AND WHY DO YOU NEED IT NOW?

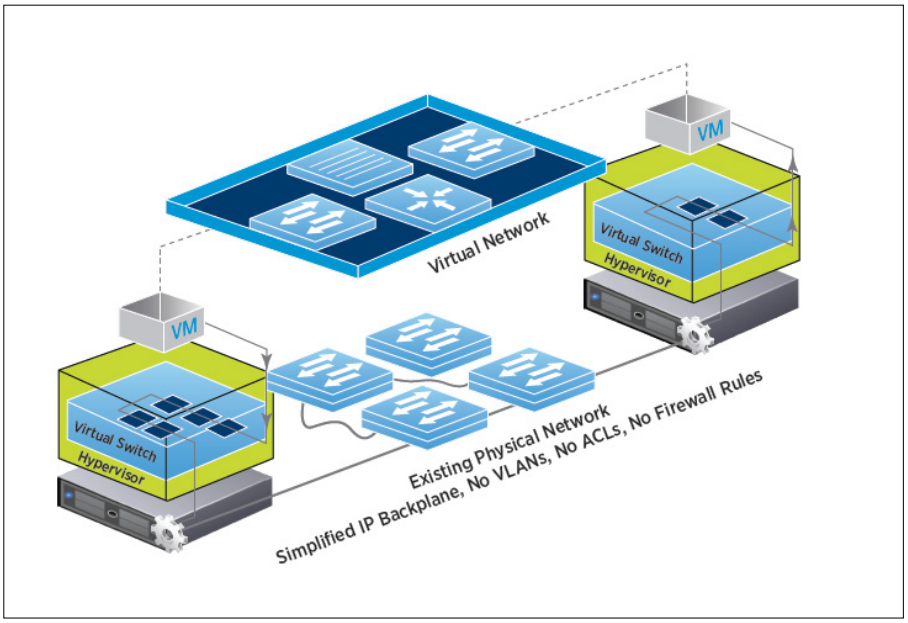
## Ensuring that Network Services and Security Keep Up with Business Demands

### THE CONSTRAINTS OF HARDWARE-CENTRIC NETWORKS

- Difficulty in supporting the mobility of applications and workloads that compute virtualization enables
- Long provisioning time (days or weeks) that can delay service delivery for LOBs and time to market for new products
- Manual configuration errors resulting in network downtime
- VLAN and firewall rule sprawl and overall operational complexity that increase OpEx
- Performance choke points
- Escalating hardware costs, especially for proprietary hardware
- Ongoing, costly data center security breaches

### What is Network Virtualization?

Network virtualization is conceptually very similar to server virtualization. As shown in Figure 1, the functional equivalent of a "network hypervisor" reproduces the complete set of Layer 2 to Layer 7 networking services in software.




Server virtualization allows administrators to programmatically create, snapshot, delete and restore software-based virtual machines (VMs) on demand. Similarly, with network virtualization you can programmatically create, provision, snapshot, delete and restore complex networks all in software.

The underlying physical network is greatly simplified, providing a pool of transport capacity that can be consumed and repurposed on demand.

### How Network Virtualization Works

#### How network hypervisors "containerize" network services for workloads

Network virtualization coordinates the virtual switches already present in server hypervisors across the data center. Network services are pushed to the virtual switches for connected VMs to effectively deliver a platform – or "network hypervisor" – for the creation of virtual networks.

In essence, a virtual network is a software container that presents logical network and security services–logical switches, routers, firewalls, load balancers, VPNs, and workload security–to connected workloads.

Provisioning and changing virtual networks takes minutes, compared to the time required (days or even weeks) for hardware-centric networks.

Build a fundamentally more agile, efficient and secure application environment with VMware NSX® network virtualization on powerful industry standard infrastructure featuring Intel® Xeon® processors and Intel® Ethernet 10GB/40GB Converged Network Adapters.

### How a single hypervisor can be associated with different workloads

One way to provision virtual networks is by using a cloud management platform (CMP) to request the virtual network and security services for the corresponding workloads. The controller then distributes the necessary services to the corresponding virtual switches, and logically attaches them to the right workloads.

This allows different virtual networks to be associated with different workloads on the same hypervisor. It also enables the creation of everything from basic virtual networks (involving as few as two nodes), to advanced constructs that match the complex, multi-segment network topologies used to deliver multitier applications.

### How connected workloads see the virtualized network

To connected workloads, a virtualized 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.

## Why Do You Need Network Virtualization Now?

The response time of network teams to new business requirements is too slow. Virtualized server and storage solutions can be quickly provisioned, but they have to wait for the network services to support them. This can cause friction between network teams and lines of business (LOBs).

### Move faster to meet constantly changing business needs

Simply put, software moves faster than hardware. When network services are provided in software, you can respond to change with greater speed. It's far easier to deploy services, make changes, and roll back to previous versions when the network is all in software. You can develop, test and deploy new applications faster than ever before. This makes it possible for your network team to keep up with—and even get ahead of—the dynamic demands of your business.

### Increase flexibility with hardware abstraction

Network virtualization moves intelligence from dedicated hardware to flexible software, which increases IT and business agility. This concept is known as abstraction. With everything in software, virtualized services can be assembled in any combination to produce a unique virtual network in a matter of seconds. Each virtual network is customizable for the workloads it supports.

### Increase security with micro-segmentation

Network virtualization serves as the foundational building block for micro-segmentation (the use of fine-grained policies and network control to enable security inside the data center). Micro-segmentation allows you to wrap security around each workload, preventing the spread of server-to-server threats.

**Inherent isolation:** When virtual networks are created, they remain isolated from each other unless you decide to connect them. No physical subnets, no VLANs, no access control lists (ACLs), and no firewall rules are required in order to enable this isolation.

**Dynamic network security:** Security policies are automatically attached to workloads when a VM is created. These policies and the capabilities to enforce them automatically migrate with their respective VMs and are deleted when their respective VMs are decommissioned.

**Distributed network security:** Security policies are enforced at each workload's hypervisor-based virtual switch. This approach is far more effective than relying on perimeter firewalls, which cannot see the majority of server-to-server (or east-west) traffic. Distributed network security also eliminates bandwidth-consuming hairpinning (where inter-VM server traffic must be routed through a perimeter firewall).

### Speed service delivery with IT automation and orchestration

In large data centers, manual processes strain OpEx budgets. They are also a major cause of service disruption due to human error. Network virtualization automates the manual tasks associated with network configuration, provisioning, management and more. Orchestration capabilities distribute network services in parallel with VMs. Network virtualization allows you to standardize and maintain predefined templates that consist of network topologies and services. Using templates, environments can be provisioned in seconds with consistent configuration and security.

### Improve disaster recovery with replication of entire network and services

IT organizations are measured by their ability to maintain application continuity in the face of unplanned outages. With the capacity to enable faster recovery and reduce downtime, network virtualization can serve to complement an existing disaster recovery. Network virtualization enables IT organizations to replicate entire network and security services for any app with a push of a button. Such replicated network and security services—untied to physical networks, locations, and topologies—come at a fraction of the cost of traditional DR solutions, and can subsequently be available in standby mode at the push of a button. Such cloud-scale service availability reduces the risk and impact of outages, and consequently saves on related costs—known to range from hundreds of thousands of dollars to tens of millions of dollars per incident.

### Establish a platform for SDDC

Network virtualization is the critical third pillar of Software-Defined Data Center (SDDC). By matching the capabilities and benefits derived from familiar server and storage virtualization solutions, network virtualization enables you to achieve the agility, economics, and choice that are the hallmarks of the SDDC.

## Conclusion

There is an expanding gap between network capabilities and transformations in other parts of the data center through virtualization. Not surprisingly, a survey by SDxCentral found that 88 percent of respondents insist that it's "important" or "mission critical" to adopt a network virtualization solution in the next two to five years.

Network virtualization enables networking teams to maintain the control they require over critical service and security resources. At the same time, your teams can deliver those services faster, easier, more economically, and with greater flexibility and scalability.

For an introduction to network virtualization, download the Network Virtualization For Dummies Guide.

To learn more about the VMware NSX network virtualization platform, visit: vmware.com/products/nsx

---

[1] SDxCentral, "2015 Special Report: Network Virtualization in the Data Center," December 2015.

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