Making Everything Easier!™

VMware Special Edition

Network Virtualization

FOR DUMMIES®

A Wiley Brand

Learn:

- Why you need to virtualize your network
- How network virtualization works
- Best practices and how to get started

Brought to you by

vmware®

Mora Gozani

About VMware, Inc.

VMware is a leader in cloud infrastructure and business mobility. Built on the company's industry-leading virtualization technology, VMware solutions deliver a brave new model of IT that is fluid, instant, and more secure. VMware technology is designed to help organizations innovate faster by rapidly developing, automatically delivering, and more safely consuming any application. With 2014 revenues of $6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world.

To learn more, visit: www.vmware.com.

Network Virtualization

FOR DUMMIES®

A Wiley Brand

VMware Special Edition

by Mora Gozani

FOR DUMMIES®

A Wiley Brand

Network Virtualization For Dummies®, VMware Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-12583-9 (pbk); ISBN 978-1-119-12585-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Becky Whitney
Project Editor: Elizabeth Kuball
Acquisitions Editor: Katie Mohr
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Dummies Marketing: Jennifer Webb
Production Editor: Siddique Shaik

Table of Contents

Introduction

Welcome to *Network Virtualization For Dummies,* your guide to a new and greatly improved approach to data center networking.

Before I start getting to the heart of the matter of network virtualization, I briefly describe some topics that I cover within these pages. All the following requirements build the case for moving out of the hardwired network past and into the flexible world of network virtualization, which I describe in depth in Chapter 1:

- The network needs to move as fast as the business.
- Network security needs to move faster than cybercriminals do.
- Applications need the flexibility to move across data centers.

So, how do you get there? The first step is to immerse yourself in the concepts of this new approach to data center networking. That's what this book is all about.

About This Book

Don't let the small footprint fool you. This book is loaded with information that can help you understand and capitalize on network virtualization. In plain and simple language, I explain what network virtualization is, why it's such a hot topic, how you can get started, and steps you can take to get the best bang for your IT buck.

Foolish Assumptions

In writing this book, I've made some assumptions about you. I assume that

- You work in an IT shop.
- You're familiar with network terminology.
- You understand the concept of virtualization.

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

Take careful note of these key "takeaway" points.

Read these optional passages if you crave a more technical explanation.

Follow the target for tips that can save you time and effort.

Where to Go from Here

The book is written as a reference guide, so you can read it from cover to cover or jump straight to the topics you're most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome: a better understanding of network virtualization and how it can help you increase business agility, data center security, and application mobility.

Chapter 1

The Next Evolution of Networking: The Rise of the Software-Defined Data Center

In This Chapter

- Introducing the software-defined data center
- Building the case for network virtualization
- Exploring today's networking challenges

Why should you care about network virtualization? That question has more than a single answer. In fact, in this chapter, I describe several themes that point to a single overarching need: It's time to move out of the hardwired past and into the era of the virtualized network. Here's why:

- To stay competitive, businesses need the agility of the software-defined data center (SDDC).
- Antiquated network architectures are blocking the road to the SDDC.
- Legacy network architectures limit business agility, leave security threats unchecked, and drive up costs.

The SDDC is rewriting the rules for the way IT services are delivered. The SDDC approach moves data centers from static, inflexible, and inefficient to dynamic, agile, and optimized.

In this new world, virtualization enables the intelligence of the data center infrastructure to move from hardware to software. All IT infrastructure elements — including compute, networking, and storage — are virtualized and grouped into pools of resources. These resources can then be automatically deployed, with little or no human involvement. Everything is flexible, automated, and controlled by software.

In a SDDC, you can forget about spending days or weeks provisioning the infrastructure to support a new application. You can now get an app up and running in minutes, for rapid time to value.

The software-defined approach is really a much-needed framework for greater IT agility and more responsive IT service delivery, all at a lower cost. It's the key to the data center of the future.

One recent study (in June 2014) by the Taneja Group, "Transforming the Datacenter with VMware's Software-Defined Data Center vCloud Suite," found that SDDCs deliver a 56 percent reduction in annual operational costs for provisioning and management. Even better, software-defined approaches can slash the time required to provision a production network for a new application from three or four weeks to a matter of minutes.

The Business Needs Speed

The chapter opener presents all the good news about software-based data centers. Here's the catch: Network architectures rooted in hardware can't match the speed and agility of SDDCs.

For large companies, the pace of business is pretty crazy, and the pace of change is only increasing. Everything needs to be done yesterday. And everything now revolves around IT's ability to support the business. This new reality has big implications for the network.

When a business wants to wow its customers with a new app, roll out a hotly competitive promotion, or take a new route to market, it needs the supporting IT services right away —

not in weeks or months. In today's world, you either go for it or you miss out. We're in the era of the incredible shrinking window of opportunity.

When the business turns to the IT organization for essential services, it wants to hear, "We'll get it done. We'll have it up and running right away," and not, "Well, we can't do that just yet because we would first need to do blah, blah, blah to the network, and that will take us at least a few weeks." That's not good enough. When business leaders hear that kind of talk, they're likely to walk away from in-house IT and walk right into the arms of a public cloud provider.

The velocity of business won't slow down. It's all one big racetrack out there, with people trying to change a full set of tires and fuel up the car in seven seconds. That means IT needs to move a lot faster. Networks now need to change at the turbocharged speed of a digitally driven business. And that requires big changes in the current hardwired approaches to the network.

Security Requirements Are Rising

Long ago, a young Bob Dylan advised the world, "You don't need a weatherman to know which way the wind blows." Today, you could say pretty much the same thing about network security. In today's enterprises, a roaring wind is blowing in the direction of increased network security.

Everyone knows that we need to do more to avoid costly breaches that put sensitive information into the hands of cybercriminals. And no company is immune to the threat. Just consider some of the headline-grabbing security breaches of the past few years — breaches that have brought corporate giants to their knees. From healthcare and investment banking to retail and entertainment, all companies are now caught up in the same costly battle to defend the network.

It's like one big war game. A company fortifies its data center with a tough new firewall and the cybercriminals slip in

through a previously unknown back door — like a simple vulnerability in a client system — and run wild in the data center. The traditional strategy of defending the perimeter needs to be updated to include much more protection inside the data center as well.

All the while, the costs keep rising — in terms of damage to brand reputation and actual out-of-pocket costs. According to a research report published in May 2015 titled "2015 Cost of Data Breach Study: Global Analysis," by the respected Ponemon Institute, the average total cost of a data breach hit $3.79 million in 2014, and the average cost paid for each single lost or stolen record containing sensitive and confidential information rose 6 percent to $154.

Clearly, something has to give. Enterprises need a better architecture to defend against the trolls *under* the digital bridge. And this need for a better architecture is a strong argument for transforming the network through virtualization.

Apps Need to Move Around

The rise of server virtualization has made a lot of great things possible. In a big step forward, applications are no longer tied to a single physical server in a single location. You can now replicate apps to a remote data center for disaster recovery, move them from one corporate data center to another, or slide them into a hybrid cloud environment.

But there's a catch: the network. It's like a hitch in your giddy-up, to borrow some words from the cowboys of old. The network configuration is tied to hardware, so even if apps can move with relative ease, the hardwired networking connections hold them back.

Networking services tend to be very different from one data center to another, and from an in-house data center to a cloud. That means you need a lot of customization to make your apps work in different network environments. That's a major barrier to app mobility — and another argument for using virtualization to transform the network.

Network Architectures Rooted in Hardware Can't Keep Up with the SDDC

The SDDC is the most agile and responsive architecture for the modern data center, achieved by moving intelligence into software for *all* infrastructure elements. So, let's take stock of where things are today:

- Most data centers now leverage server virtualization for the best compute efficiency. *Check!*
- Many data centers now optimize their storage environments through virtualization. *Check!*
- Few data centers have virtualized their network environments. *No check.*

Though businesses are capitalizing on server and storage virtualization, they're challenged by legacy network infrastructure that revolves around hardware-centric, manually provisioned approaches that have been around since the first generation of data centers.

In the next several sections, I walk you through some of the specific challenges of legacy architectures.

Network provisioning is slow

Although some network provisioning processes can be scripted — and software-defined networking promises to make this a reality — with hardware-based systems, there is no automatic linkage to compute or storage virtualization. As a result, there is no way to automatically provision networking when the associated compute and storage is created, moved, snapshotted, deleted, or cloned. So, network provisioning remains slow, despite the use of automated tools.

All the while, the thing that matters the most to the business — getting new apps ready for action — is subject to frequent delays caused by the slow, error-prone, manual processes used to provision network services.

This is all rather ironic when you take a step back and consider the bigger picture: The limitations of legacy networks tie today's dynamic virtual world back to inflexible, dedicated hardware. Server and storage infrastructure that should be rapidly repurposed must wait for the network to catch up. Provisioning then becomes one big hurry-up-and-wait game.

Workload placement and mobility are limited

In today's fast-moving business environments, apps need to have legs. They need to move freely from one place to another. This might mean replication to an offsite backup-and-recovery data center, movement from one part of the corporate data center to another, or migration into and out of a cloud environment.

Server and storage virtualization makes this kind of mobility possible. But you have to be aware of another problem: the network. When it comes to app mobility, today's hardwired network silos rob apps of their running shoes. Workloads, even those in virtual machines, are tethered to physical network hardware and topologies. To complicate matters, different data centers have different approaches to networking services, so it can take a lot of heavy lifting to configure an app running in data center A for optimal performance in data center B.

All of this limits workload placement and app mobility and makes change not just difficult but risky. It's always easiest — and safest — to simply leave things just the way they are.

The current hardware-centric approach to networking restricts workload mobility to individual physical subnets and availability zones. To reach available compute resources in the data center, your network operators may be forced to perform box-by-box configuration of switching, routing, firewall rules, and so on. This process is not only slow and complex but also one that will eventually hit a wall — including the technical limitation of 4,096 total VLANs in a single LAN.

Hardware limitations and lock-ins breed complexity and rigidity

The current closed black-box approach to networking — with custom operating systems, ASICs, CLIs, and management — complicates operations and limits agility. This old approach locks you into not only your current hardware but also all the complexities of your current network architecture, limiting your IT team's ability to adapt and innovate — which in turn puts the same limits on the business itself because the business can move no faster than IT.

One study, "Network Agility Research 2014," by Dynamic Markets, found that 90 percent of companies are disadvantaged by the complexities of their networks — impacting when, where, and what applications and services can be deployed. Here are some rather telling findings from the same study:

- IT makes, on average, ten changes to the corporate network in a 12-month period that require a maintenance window. The average wait for maintenance windows is 27 days each.
- Businesses spend a total of 270 days a year — or 9.6 months — waiting for IT to deliver a new or improved service.
- Larger enterprises require significantly more of these changes and wait even longer for maintenance windows.

Configuration processes are manual, slow, and error prone

On a day-to-day basis, physical networks force your network team to perform a lot of repetitive, manual tasks. If a line of business or a department requests a new application or service, you need to create VLANs, map VLANs across switches and uplinks, create port groups, update service profiles, and on and on. On top of this, this configuration work is often done via clunky CLIs.

The rise of software-defined networking (SDN) — which I explain in Chapter 2 — is meant to help here by allowing programmatically controlled hardware, but this still leaves you with a lot of heavy lifting. For instance, you still need to build multiple identical networks to support your development, test, and production teams, and you still lack the ability to deploy your (hardware-based) network in lock step with your virtualized compute and storage.

And then there's the other issue: All this manual configuration work is error prone. In fact, manual errors are the main cause of outages. Studies consistently find that the largest percentage of network incidents — in the realm of 32 percent to 33.3 percent — is due to human-caused configuration errors. (The 33.3 percent estimate is from the Dimension Data report "2015 Network Barometer Report," and the 32 percent estimate is from the Ponemon Institute report "2013 Cost of Data Center Outages.")

OpEx and CapEx are too high

The limitations of legacy network architectures are driving up data center costs — in terms of both operational expenditures (OpEx) and capital expenditures (CapEx).

OpEx

The heavy use of manual processes drives up the cost of network operations. Just consider all the labor-intensive manual tasks required to configure, provision, and manage a physical network. Now multiply the effort of these tasks across all the environments you need to support: development, testing, staging, and production; differing departmental networks; differing application environments; primary and recovery sites; and so on. Tasks that may be completed in minutes with automated processes — or even instantaneously with *automatic* deployment of networks — take hours, days, or weeks in a manual world.

And then there are the hidden costs that come with manually introduced configuration errors. One mistake can cause a critical connectivity issue or outage that impacts business. The financial effect of an unplanned data center outage can be huge. The average reported incident length in the study "Network Agility Research 2014" by Dynamic Markets was 86 minutes at a cost of $7,900 per minute. The average cost per incident was $690,200.

CapEx

On the capital side, legacy network architectures require your organization to invest in stand-alone solutions for many of the networking and security functions that are fundamental to data center operations. These include routing, firewalling, and load balancing. Providing these functions everywhere they are needed comes with hefty price tags.

There is also the issue of the need to overprovision hardware to be sure you can meet peak demands, plus the need to deploy active-passive configurations. In effect, you need to buy twice the hardware for availability purposes.

And then there is the cost of forklift upgrades. To take advantage of the latest innovations in networking technology, network operators often have to rip and replace legacy gear, with most organizations on a three- to five-year refresh cycle. Legacy network architectures rooted in hardware also require overprovisioning to account for spikes in usage. The inability of hardware-based networks to scale automatically based on demands requires this inefficiency. And up goes the costs of networking.

Legacy network architectures can also result in other inefficiencies. Often, network designers must reserve parts of a network for a specific use to accommodate special security or compliance requirements. Coupled with the need for overprovisioning, the inefficiencies are magnified, leading to swaths of "dark servers" kept around "just in case" — without serving any useful purpose. The result looks like a badly fragmented hard drive.

You can't leverage hybrid cloud resources

Cloud service providers have proven that applications and services can be provisioned on demand. Enterprises everywhere would like to enjoy the same level of speed and agility. With that thought in mind, forward-looking executives envision using hybrid clouds for all kinds of use cases, from data storage and disaster recovery to software development and testing.

But, once again, there is a network-related catch. In their quest to move to the cloud, enterprises are hampered by vendor-specific network hardware and physical topology. These constraints that come with legacy data center architectures can make it difficult to implement hybrid clouds. Hybrid clouds depend on a seamless extension of the on-premises data center to a public cloud resource, and how do you achieve this when you can't control the public cloud network to mirror your hardware networking systems?

Networks have inadequate defenses

Many of the widely publicized cyber attacks of recent years share a common characteristic: Once inside the data center perimeter, malicious code moved from server to server, where sensitive data was collected and sent off to cybercriminals. These cases highlight a weakness of today's data centers: They have limited network security controls to stop attacks from spreading inside the data center.

Perimeter firewalls are pretty good at stopping many, but not all, attacks. As the recent attacks have shown, threats are still slipping into the data center through legitimate access points. Once inside, they spread like a deadly viral disease. This has been a tough problem to solve because of the realities of physical network architectures. Put simply, with legacy networking systems, it's too costly to provide firewalling for traffic between *all* workloads inside the data center. With today's networks, it's hard to stop an attack from laterally propagating from server to server using east–west traffic.

Let's recap. To this point, I've noted that:

- To stay competitive, businesses need the agility of the software-defined data center.
- Antiquated network architectures are blocking the road to the SDDC.
- Legacy network architectures limit business agility, leave security threats unchecked, and drive up costs.

These themes point to a single overarching need: It's time to move out of the hardwired past and into the era of the virtualized network.

Chapter 2

It's Time to Virtualize the Network

In This Chapter

- Explaining the basics of network virtualization
- Highlighting the benefits of this new approach
- Outlining key characteristics of a virtualized network

In this chapter, I dive into the concept of network virtualization — what it is, how it differs from other approaches to the network, and why the time is right for this new approach.

To put things in perspective, let's begin with a little background on network virtualization, the state of today's networks, and how we got to this point.

How Network Virtualization Works

Network virtualization makes it possible to programmatically create, provision, and manage networks all in software, using the underlying physical network as a simple packet-forwarding backplane. Network and security services in software are distributed to hypervisors and "attached" to individual virtual machines (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.

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 switching, logical routing, logical firewalling, logical load balancing, 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. The workloads themselves are connected via a software representation of a physical network "wire." This allows for the entire network to be created in software (see Figure 2-1).

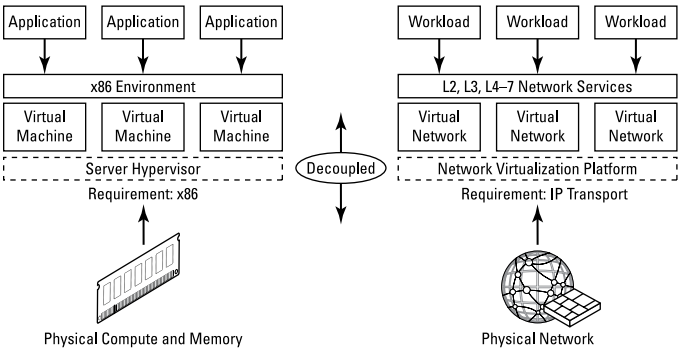


Figure 2-1: Compute and network virtualization.

Network virtualization coordinates the virtual switches in server hypervisors and the network services pushed to them for connected VMs, to effectively deliver a platform — or "network hypervisor" — for the creation of virtual networks (see Figure 2-2).

One way that virtual networks can be provisioned 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 corresponding workloads (see Figure 2-3).

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, multisegment network topologies used to deliver multitier applications.

To connected workloads, a virtual network looks and operates like a traditional physical network (see Figure 2-4). Workloads "see" the same layer 2, layer 3, and layer 4 through 7 network services that they would in a traditional physical

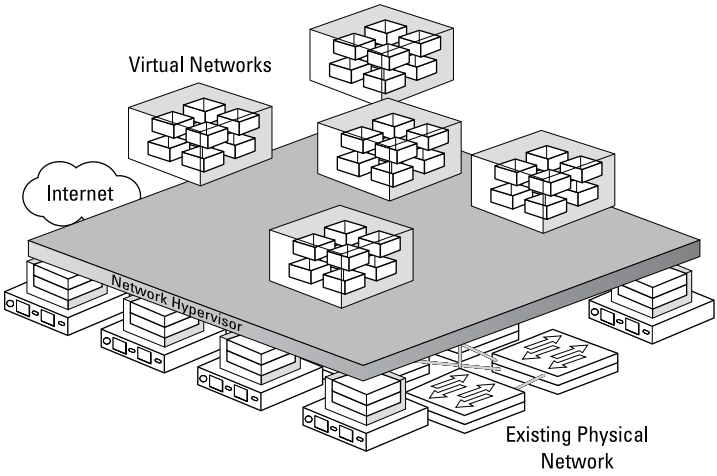


Figure 2-2: The "network hypervisor."

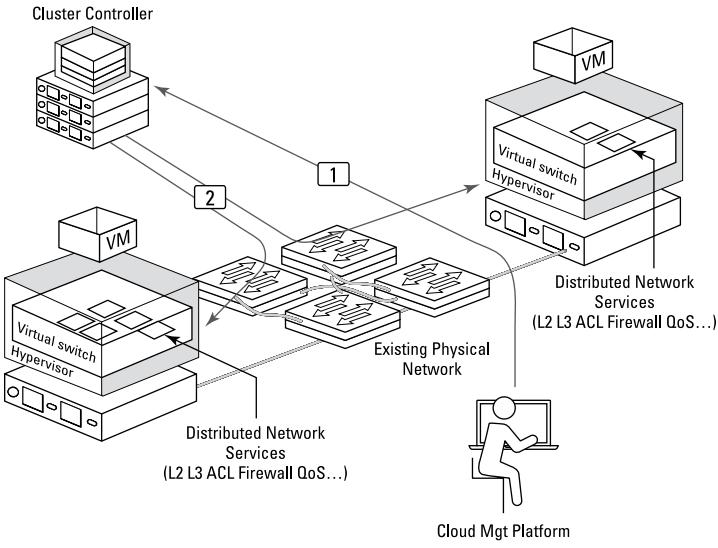


Figure 2-3: Virtual network provisioning.

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 virtual interface of the virtual switch.

To the physical network, a virtual network looks and operates like a traditional physical network (see Figure 2-5). The

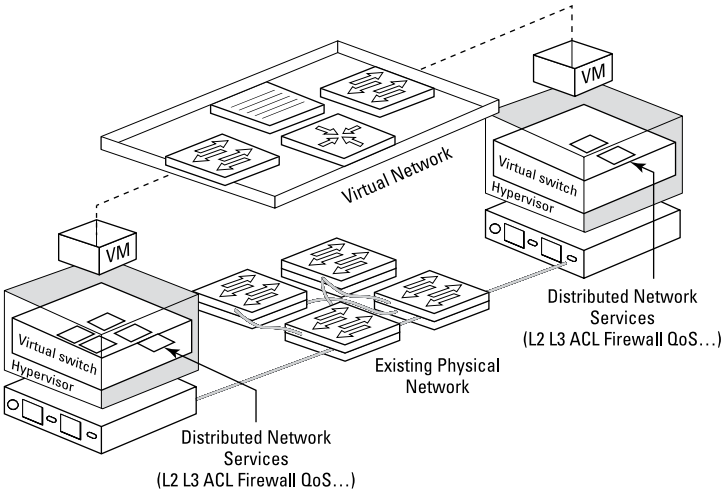


Figure 2-4: The virtual network, from the workload's perspective (logical).

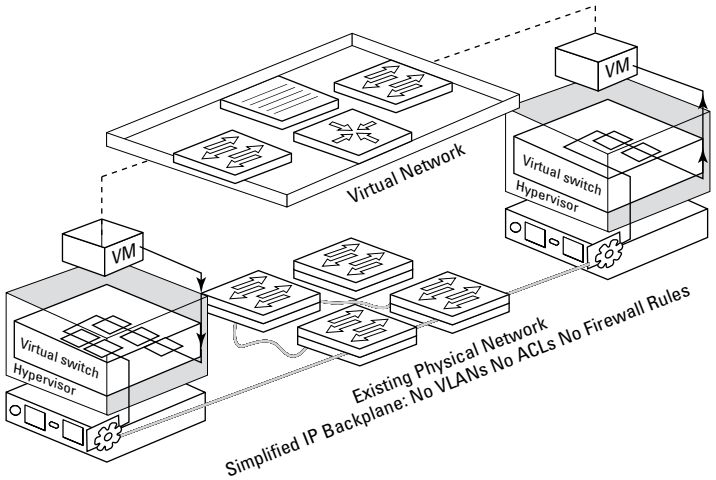


Figure 2-5: The virtual network, from the network's perspective (physical).

physical network "sees" the same layer 2 network frames that it would in a traditional physical network. The VM sends a standard layer 2 network frame that is encapsulated at the source hypervisor with additional IP, user datagram protocol (UDP), and virtual extensible LAN (VXLAN) headers. The physical network forwards the frame as a standard layer 2 network frame, and the destination hypervisor decapsulates the headers and delivers the original layer 2 frame to the destination VM.

The ability to apply and enforce security services at the virtual interface of the virtual switch also eliminates hairpinning (see Chapter 3) in situations where east–west traffic 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.

What's the difference between a virtual network and a VLAN?

If you work in networking, you know all about VLANs, or virtual local area networks. They've been around for a long time. So, why aren't VLANs sufficient? Let's look at the differences between VLANs and virtual networks.

The VLAN approach breaks up a physical local area network into multiple virtual networks. Groups of ports are isolated from each other as if they were on physically different networks. The VLAN approach is like slicing a big network pie into a lot of bite-size networks. Looking ahead, as your network grows you could eventually run into a dead end: the limitation of 4,096 total VLANs in a single LAN.

The problems with VLANs don't stop there. Another big limitation is that VLANs don't allow you to save, snapshot, delete, clone, or move networks. And then there is the inherent security issue with VLANs — they don't allow you to control traffic between two systems on the same VLAN. This means that an attack that hits one system can jump to another system.

Network virtualization is far more than VLANs, making possible the creation of entire networks in software — including switching, routing, firewalling, and load balancing. This provides far greater flexibility than has been possible in the past. With all networking and security services handled in software and attached to VMs, labor-intensive management and configuration processes can be streamlined and automated, and networks are created automatically to meet workload demands.

Network Virtualization versus Software-Defined Networking

Network virtualization may sound a lot like software-defined networking (SDN), but there are actually major differences between these terms. Let's look at these two concepts.

Though the term *software-defined networking* means different things to different people, this much is clear: SDN allows software to control the network and its physical devices. SDN is all about software talking to hardware — you can essentially call it a next-generation network management solution. Though it centralizes management and allows you to control network switches and routers through software, SDN doesn't virtualize all networking functions and components. In other words, SDN doesn't allow you to run the entire network in software. Hardware remains the driving force for the network.

In contrast to SDN, network virtualization completely decouples network resources from the underlying hardware. All networking components and functions are faithfully replicated in software. Virtualization principles are applied to physical network infrastructure to create a flexible pool of transport capacity that can be allocated, used, and repurposed on demand.

With your networking resources decoupled from the physical infrastructure, you basically don't have to touch the underlying hardware. Virtual machines can move from one logical domain to another without anyone having to reconfigure the network or wire up domain connections. You implement network virtualization in the hypervisor layer on x86 servers rather than on network switches. As I note earlier, the physical network serves as a packet-forwarding backplane controlled from a higher level.

Software-defined networking allows you to control network switches and routers through software. It doesn't virtualize all networking functions and components.

Network virtualization replicates all networking components and functions in software. It allows you to run the entire network in software.

Virtual Appliances versus Integration in the Hypervisor

What about virtual appliances? Networking functions, of course, can be delivered via *virtual appliances* (ready-to-go virtual machines that run on a hypervisor). Virtual appliances are usually designed to deliver the functionality of a single network function, such as a router, a WAN accelerator, or a network firewall.

Though they meet targeted needs, virtual appliances have some distinct drawbacks. For starters, virtual appliances run as guests on top of a hypervisor, which limits performance. And then there is the issue of virtual appliance sprawl. Because of the limited performance of the devices, you may end up having to deploy tens, hundreds, or even thousands of virtual appliances to reach the scale of the full data center. This presents a huge CapEx barrier and is also an operational nightmare.

The real value of network virtualization emerges in the integration of all networking functions *in* the hypervisor. This more sophisticated approach allows the network and the full range of its functions to follow virtual machines as they move from one server to another. There's no need to reconfigure any network connections, because those are all in software. Basically, the network can go anywhere in the data center that is virtualized.

There are many other advantages to the hypervisor-based approach to network virtualization. I cover these in Chapter 3. For now, let's just say that this new approach to the network makes your data center a lot more agile. It's kind of like going from hardwired to wireless connections on your home network. Things can move around, and all the networking stuff goes with them.

Why the Time Is Right for Network Virtualization

People have been talking about network virtualization for years. It's now time to let the rubber meet the road — to meet pressing needs in today's data centers.

Here are some of the reasons why the time is right for network virtualization.

Meeting the demands of a dynamic business

Simply put, software moves faster than hardware. It's far easier to deploy services, make changes, and roll back to previous versions when the network is all in software. Today's businesses have constantly changing requirements, which puts increasing demands on IT to be able to support these changes. When the network environment is run purely in software, it's much more flexible in adapting to changes, making it possible for IT organizations to meet business demands more effectively.

Increasing flexibility with hardware abstraction

Network virtualization moves intelligence from dedicated hardware to flexible software that increases IT and business agility. This concept is known as *abstraction.* To explain this concept, let's start in the well-established world of server virtualization.

With server virtualization, an abstraction layer, or hypervisor, reproduces the attributes of the physical server — CPU, RAM, disk, and so on — in software. Abstraction allows these attributes to be assembled on the fly to produce a unique virtual machine.

Network virtualization works the same way. With network virtualization, the functional equivalent of a "network hypervisor" reproduces networking services — such as switching, routing, access control, firewalling, QoS, and load balancing — in software. With everything in software, virtualized services can be assembled in any combination to produce a unique virtual network in a matter of seconds.

This level of agility is one of the big benefits of the software-defined data center, and one of the big arguments for network virtualization.

Increasing security with network micro-segmentation

Another argument for network virtualization revolves around the need for stronger security. Network virtualization increases security by serving 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 shrink-wrap security around each workload, preventing the spread of server-to-server threats. I explain more on this concept in Chapter 4.

With network virtualization, networks are isolated by default, which means that workloads on two unrelated networks have no possibility of communicating with each other. Isolation is foundational to network security, whether for compliance, containment, or simply keeping development, test, and production environments from interacting. 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.

Virtual networks are also isolated from the underlying physical network. This isolation not only decouples changes in one virtual network from affecting another, but it also protects the underlying physical infrastructure from attacks launched from workloads in any of your virtual networks. Once again, you don't need any VLANs, ACLs, or firewall rules to create this isolation. That's just the way it is with network virtualization.

Taking a closer look at micro-segmentation

For a deep dive into the concept of micro-segmentation, download a copy of *Micro-segmentation For Dummies* (Wiley) at `http://info.vmware.com/content/33851_Micro-Segmentation_Reg?CID=70134000000NzKR&src=test&touch=1`. This tightly written book, sponsored by VMware, provides a close-up look at the concepts, technologies, and benefits of micro-segmentation with VMware NSX.

Establishing a platform for the SDDC

As I note in Chapter 1, the software-defined data center is a much-needed framework for greater IT agility and more responsive IT service delivery, all at a lower cost. As the critical third pillar of the SDDC, building on the pillars of compute and storage virtualization, network virtualization is key to the SDDC.

Network virtualization is a transformative architecture that makes it possible to create and run entire networks in parallel on top of existing network hardware. This results in faster deployment of workloads, as well as greater agility and security in the face of increasingly dynamic data centers.

Rethinking the Network

Though it leverages your existing network hardware, network virtualization is a fundamentally new approach to the network. This means you need to think about your network in new ways. In the past, network functions revolved all around hardware. Now they have all the flexibility of software.

A virtualized network should allow you to take an entire network, complete with all its configurations and functions, and duplicate it in software.

You should be able to create and run your virtualized network in parallel on top of your existing network hardware. A virtual network can be created, saved, deleted, and restored, just as you would do with virtual machines, but in this case you're doing it with the entire network.

In more specific terms, a virtualized network should give you the ability to

- Decouple the network from underlying hardware and apply virtualization principles to network infrastructure.
- Create a flexible pool of transport capacity that can be allocated, utilized, and repurposed on demand.

- Deploy networks in software that are fully isolated from each other, as well as from other changes in the data center.
- Transfer, move, and replicate the network, just as you can do with virtualized compute and storage resources.
- Make consistent network functionality available anywhere in your enterprise.

So, how do you get there? I cover that part of the story in Chapter 3, where I explore the technologies behind network transformation.

Chapter 3

Transforming the Network

In This Chapter

- Explaining the key functionality of a virtualized network
- Introducing the technologies for network virtualization
- Outlining key features of a virtualized network
- Exploring functional and economic benefits

In this chapter, I dive down into the technologies you need in order to bring the benefits of virtualization to your network environment. I begin with an introduction of the concepts behind network virtualization, and conclude with details of VMware NSX, a multi-hypervisor, multicloud management network virtualization platform.

The Key Functionalities of a Virtualized Network

Let's dive a little deeper into some of the key functionalities of a virtualized network, including overlays and packet flow.

Overlays

Network virtualization makes use of overlay technologies, which sit above the physical network hardware and work with the server hypervisor layer. Logical switching is achieved via the use of overlays, as shown in Figure 3-1.

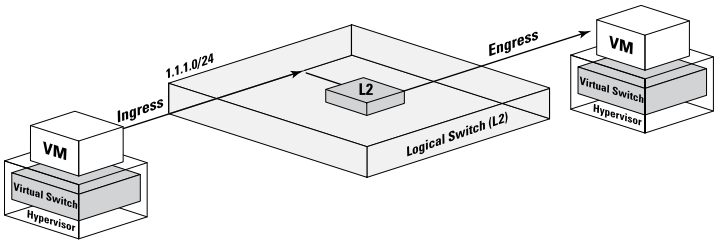


Figure 3-1: Logical switching via the use of overlays.

Network overlays make it possible to run networks entirely in software, abstracted from the supporting physical network infrastructure. They basically create tunnels within the data center network.

Packet flow from sender to receiver

As I note elsewhere, virtual networks use the underlying physical network as a simple packet-forwarding backplane. When VMs communicate with each other, the packet is encapsulated with the IP address information of the destination hypervisor. The physical network delivers the frame to the destination hypervisor, which can remove the outer header, and then the local vSwitch instance delivers the frame to the virtual machine.

In this way, the communication uses the underlying physical network as a simple IP backplane — one that requires no STP, no VLANs, no ACLs, and no firewall rules. This approach dramatically simplifies configuration management and eliminates physical network changes from the network provisioning process.

Overlay technologies

There are various overlay technologies. One industry-standard technology is called Virtual Extensible Local Area Network, or VXLAN. VXLAN provides a framework for overlaying virtualized layer 2 networks over layer 3 networks.

You may have also heard of NVGRE, another type of overlay. NVGRE stands for *network virtualization using generic routing encapsulation.* NVGRE is similar to VXLAN in its goals, but it uses different approaches to create the overlay. NVGRE has

had limited adoption in comparison to the momentum of VXLAN.

In a VMware environment, network virtualization is based on VXLAN. This widely adopted standard was developed jointly by VMware and major networking vendors.

A VXLAN primer

With its broad industry support, VXLAN has become the de facto standard overlay (or encapsulation) protocol. VXLAN is key to building logical networks that provide layer 2 adjacency between workloads, without the issue and scalability concerns found with traditional layer 2 technologies.

VXLAN is an overlay technology encapsulating the original Ethernet frames generated by workloads (virtual or physical) connected to the same logical layer 2 segment, usually named a logical switch (LS).

VXLAN is a layer 2 over layer 3 (L2oL3) encapsulation technology. The original Ethernet frame generated by a workload is encapsulated with external VXLAN, UDP, IP, and Ethernet headers to ensure that it can be transported across the network infrastructure interconnecting the VXLAN endpoints (virtual machines).

Scaling beyond the 4,096 VLAN limitation on traditional switches has been solved by leveraging a 24-bit identifier, named VXLAN Network Identifier (VNI), which is associated with each layer 2 segment created in the logical space. This value is carried inside the VXLAN header and is normally associated with an IP subnet, similar to what traditionally happens with VLANs. Intra-IP subnet communication happens between devices connected to the same virtual network (logical switch).

Hashing of the layer 2, layer 3, and layer 4 headers present in the original Ethernet frame is performed to derive the source port value for the external UDP header. This is important to ensure load balancing of VXLAN traffic across equal cost paths potentially available inside the transport network infrastructure.

The source and destination IP addresses used in the external IP header uniquely identify the hosts originating and terminating the VXLAN encapsulation of frames. This hypervisor-based logical functionality is usually referred to as a VXLAN Tunnel EndPoint (VTEP).

Encapsulating the original Ethernet frame into a UDP packet increases the size of the IP packet. We recommend increasing the overall maximum transmission unit (MTU) size to a minimum of 1,600 bytes for all the interfaces in the physical infrastructure that will carry the frame. The MTU for the virtual switch uplinks of the VTEPs performing VXLAN encapsulation is automatically increased when preparing the VTEP for VXLAN.

Figure 3-2 describes (at a high level) the steps required to establish layer 2 communications between VMs leveraging VXLAN overlay functionality:

- VM1 originates a frame destined to the VM2 part of the same layer 2 logical segment (IP subnet).
- The source VTEP identifies the destination VTEP where VM2 is connected and encapsulates the frame before sending it to the transport network.
- The transport network is required only to enable IP communication between the source and destination VTEPs.
- The destination VTEP receives the VLXLAN frame, de-encapsulates it, and identifies the layer 2 segment to which it belongs.
- The frame is delivered to VM2.

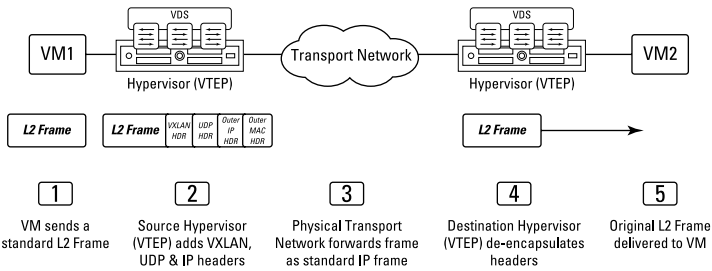


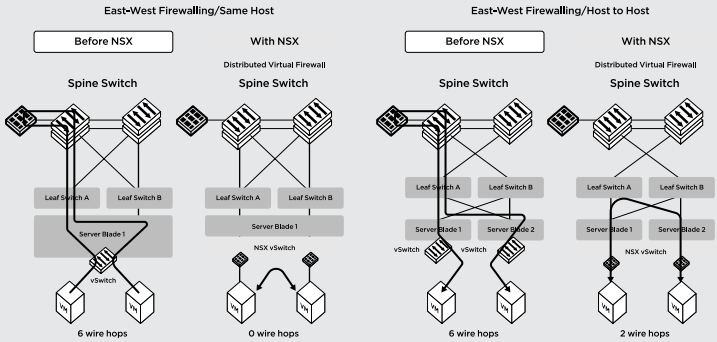
Figure 3-2: Establishing layer 2 communication between VMs with VXLAN.

Network virtualization in action: An example

Here's one of many potential examples of how network virtualization makes life better for your security and network administrators.

Communication on a conventional network can be inefficient when services, such as firewalling, are applied. Traffic must be routed out of the virtual environment, passed through the physical security infrastructure (centralized firewall), and then redirected back to the virtual environment. This process is called *hairpinning.* It adds complexity, increases instability, and decreases the ability to move workloads.

By contrast, when network services are integrated into the hypervisor, there's no need for this hairpinning process. These concepts are illustrated in the following figure.



The Big Payoff

Network virtualization helps enterprises achieve major advances in speed, agility, and security, by automating and simplifying many of the processes that go into running a data center network.

Here's a quick checklist of some of the key benefits that come with this new approach to the network. Network virtualization helps you

- Reduce network provisioning time from weeks to minutes.
- Achieve greater operational efficiency by automating manual processes.

- Place and move workloads independently of physical topology.
- Improve network security within the data center.

Meet VMware NSX: Networking for the SDDC

First, a simple definition: VMware NSX is the network virtualization and security platform for the software-defined data center. NSX reproduces the entire network model in software. This end-to-end model enables any network topology — from simple to complex multitier networks — to be created and provisioned in seconds. It delivers all the goodness of network virtualization that I cover in Chapter 2.

While increasing agility and streamlining your approach to the network, NSX enhances security inside the data center. These security gains are delivered via automated fine-grained policies that wrap security controls around individual virtual machines or small groups of virtualized resources. This approach can be a huge help in blocking attacks that move laterally within the data center, jumping from workload to workload with little or no controls to block their propagation. With NSX, workloads can be isolated from each other, as though each were on its own network.

How It Works

Let's pop the latch and take a look under the hood of VMware NSX.

The NSX architecture

The NSX approach to network virtualization allows you to treat your physical network as a pool of transport capacity that can be consumed and repurposed on demand. Virtual networks are created, provisioned, and managed in software, using your physical network as a simple packet-forwarding backplane.

Virtualized network services are distributed to each virtual machine independently of the underlying network hardware or topology. This means workloads can be added or moved on the fly and all the network and security services attached to the virtual machine move with it, anywhere in the data center. Your existing applications operate unmodified. They see no difference between a virtual network and a physical network connection.

Integration with existing network infrastructure

NSX works with your existing compute and networking infrastructure, applications, and security products. You can deploy NSX nondisruptively on top of your current infrastructure.

Better still, NSX is not an all-or-nothing approach. You don't have to virtualize your entire network. You have the flexibility to virtualize portions of your network by simply adding hypervisor nodes to the NSX platform.

Gateways, available as software from VMware or top-of-rack switch hardware from VMware partners, give you the ability to seamlessly interconnect virtual and physical networks. These can be used, for example, to support network access by workloads connected to virtual networks or to directly connect legacy VLANs and bare-metal workloads to virtual networks.

Simplified networking

After NSX is deployed, little interaction with the physical network is required. You no longer need to deal with the physical network configuration of VLANs, ACLs, spanning trees, complex sets of firewall rules, and convoluted hairpinning traffic patterns — because these are no longer necessary when the network is virtualized.

As you deploy NSX virtual networks, you can increasingly streamline your physical network configuration and design. Vendor lock-in becomes a thing of the past because the physical network only needs to deliver reliable high-speed

packet-forwarding. This means you can mix and match hardware from different product lines and vendors.

Extreme flexibility and extensibility

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. It's all defined by the application policies you set for each workload.

This high degree of flexibility applies not only to native NSX services but also to a wide variety of compatible third-party solutions — including virtual and physical instances of next-generation firewalls, application delivery controllers, and intrusion prevention systems.

Let's take a step back and consider the bigger picture here. The availability of many NSX-compatible products from VMware partners is a sign of industry support for the new operational model delivered by the NSX platform. This gives you greater confidence as you move into the realm of the virtualized network. You have a broad ecosystem on your side.

What It Does: The Key Capabilities of NSX

Let's look at some of the key technical capabilities of VMware NSX. At the outset, keep this point in mind: NSV virtualizes all network functions. That means things that used to be done in hardware are now done in software. In this sense, NSX is like a magic carpet that floats over all the networking gear described in the following sections.

Everything in software

Here are the key features of VMware NSX:

- **Logical switching:** NSX allows you to reproduce the complete layer 2 and layer 3 switching functionality in a virtual environment, decoupled from the underlying hardware.
- **NSX gateway:** This layer 2 gateway enables seamless connection to physical workloads and legacy VLANs.
- **Logical routing:** Routing between logical switches provides dynamic routing within different virtual networks.
- **Logical, distributed firewalling:** NSX allows you to create a distributed firewall, integrated into the hypervisor and wrapping security around each workload.
- **Logical load balancer:** NSX provides a full-featured load balancer with SSL termination.
- **Logical VPN:** NSX supports site-to-site and remote access VPNs in software.
- **NSX API:** This RESTful API enables integration into any cloud management platform.

Essential isolation, segmentation, and advanced security services

Every year, businesses spend billions of dollars to secure the perimeter of their data centers. And guess what? Breaches continue to mount. Though it is an essential part of a security strategy, perimeter protection doesn't do everything you need. We need a new model for data center security. Micro-segmentation, a concept I introduce in Chapter 2, provides this model.

NSX brings security inside the data center with automated fine-grained policies tied to the virtual machines. Network security policies are enforced by firewalling controls integrated into the hypervisors that are already distributed throughout the data center. These security policies move when VMs move and adapt dynamically to changes in your data center.

Virtual networks can operate in their own address spaces or have overlapping or duplicate address spaces — all without interfering with each other. Virtual networks are inherently isolated from all other virtual networks, and the underlying physical network, by default. Each virtual network is like an island in a data center sea. This approach allows you to securely isolate networks from each other. You end up with an inherently better security model for the data center. Malicious software that slips through your firewall is no longer free to jump from server to server.

Of course, none of this means you have to give up your favorite network security solutions. NSX is a platform for bringing the industry's leading networking and security solutions into the software-defined data center. Thanks to tight integration with the NSX platform, third-party products and solutions can be deployed as needed and can adapt dynamically to changing conditions in your data center.

NSX network virtualization capabilities enable the three key functions of micro-segmentation:

- **Isolation:** No communication across unrelated networks
- **Segmentation:** Controlled communication within a network
- **Security with advanced services:** Made possible by tight integration with third-party security solutions

Performance and scale

NSX delivers proven performance and scale. Because networking functions are embedded in the hypervisor, NSX features a scale-out architecture that enables seamless scaling of additional capacity while also delivering solid availability and reliability.

Here's an example of the extreme scalability of NSX: In a real-world NSX deployment, a single cluster of controllers is being used to deliver more than 10,000 virtual networks, which in turn support more than 100,000 virtual machines.

In the NSX environment:

- The processing required for the execution of distributed network services is only incremental to what the vSwitch is already doing for connected workloads.
- The vSwitch is a module that is integrated with the hypervisor kernel, along with all the NSX network and security services.
- Virtual network transport capacity scales linearly (alongside VM capacity) with the introduction of each new hypervisor/host, adding 20 Gbps of switching and routing capacity and 19.6 Gbps of firewalling capacity.

Unparalleled network visibility

NSX takes visibility into the network to an all-new level. With conventional approaches to networking, configuration and forwarding state are spread across lots of disparate network devices. This fragmentation can cloud your view and complicate troubleshooting.

By contrast, 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, and the like) are readily accessible, as is the mapping between virtual network topologies and the underlying physical network. This enables full visibility of traffic between VMs — even when the communicating VMs are on the same host and network traffic never reaches the physical network.

Better yet, with NSX, you have access to advanced troubleshooting tools like TraceFlow. This function injects a synthetic packet into a virtual switch port, providing the opportunity to observe the network path as it traverses physical and logical network systems. This allows administrators to identify the full path a packet takes and troubleshoot any points where the packet is dropped (for instance, because of firewall policies) along the way.

This level of visibility isn't possible if you're running traditional physical networking hardware, and it definitely wouldn't be possible with physical networking in situations where two VMs are communicating on the same host.

The Key Benefits of VMware NSX

Now we're getting to the really good stuff. Let's look at some of the ways your organization can cash in on the capabilities of network virtualization with VMware NSX. You can break the story into two camps: functional benefits and economic benefits.

Functional benefits

The functional benefits of NSX revolve around four pillars of the software-defined data center: speed, agility, security, and reliability. Let's look at how these benefits are delivered.

Creating entire networks in software in seconds

NSX arms you with a library of logical networking elements and services, such as logical switches, routers, firewalls, load balancers, VPN, and workload security. You can mix and match these components to create isolated virtual network topologies in seconds.

Minimizing the risk and impact of data breaches

You can use NSX to isolate workloads, each with its own security policies. This capability helps you contain threats and block the movement of malicious software within your data center. Better internal security can help you avoid or reduce the costs of data breaches.

Speeding IT service delivery and time to market

With network virtualization, you can reduce the time required to provision multitier networking and security services from weeks to minutes. Some enterprises use NSX to give application teams full self-service provisioning capabilities. Even better, the automation and orchestration capabilities in NSX help you avoid the risk of manual configuration errors.

Simplifying network traffic flows

You can use NSX to lessen the load of server-to-server traffic (east–west traffic) on the oversubscribed core. With a virtual

network, VMs communicate with one another through the vSwitch or aggregation fabric. This cuts down on east–west traffic hops and helps you avoid the pitfalls of convoluted traffic patterns. The idea is to make better use of your current assets and avoid the costs of building up core capacity with more hardware.

Increasing service availability

Cloud-scale data centers have few outages because they have flatter fabrics with equal-cost multipath routing between any points on the network. Simplified leaf-spine fabrics make individual links or devices inconsequential. The network can withstand multiple simultaneous device failures with no outage. With the network virtualization capabilities of NSX, you can achieve the same high availability in your data center.

Economic benefits

The economic benefits of network virtualization with NSX emerge in the form of savings on both capital and operational expenditures.

Reducing the risk of costly breaches

Historically, deploying firewalls to control an increasing volume of east–west traffic inside the data center has been cost prohibitive for many enterprises. What's more, the sheer number of devices needed and the effort required to set up and manage a complex matrix of firewall rules have made this approach operationally infeasible. The micro-segmentation capabilities that come with network virtualization make this all not just doable but affordable. You can now reduce the risk of cross–data center security breaches while avoiding high-dollar capital expenditures for additional hardware and software.

Reducing time and effort

Network virtualization can greatly reduce the effort and time it takes to complete network tasks. Generally, NSX reduces the effort from hours to minutes, and the cycle times from days to minutes. If you consider all the manual tasks required to provision and manage a physical network — across development, testing, staging, and production environments — and

the fact that NSX automates these, you begin to see lots of opportunities to reduce operational costs.

Improving server asset utilization

In traditional topologies, each network cluster has its own compute capacity. IT admins often overprovision compute to avoid the lengthy, error-prone network reconfiguration required to reach available capacity in another cluster. NSX gives you a better way to get things done. You can use NSX to bridge two or more network clusters and deploy workloads to the unused capacity. By making better use of existing server capacity, you can avoid the need to buy new physical servers.

Improving price/performance savings

Many enterprises are using the capabilities of NSX and network virtualization to replace expensive proprietary hardware with lower-cost infrastructure that can be bought from various vendors — whoever has the best price/performance.

Extending the hardware life cycle

You can use NSX to pull more value from your existing network infrastructure. Here's how: NSX offloads an increasing volume of east–west traffic from the network core. This allows you to extend the hardware lifespan without having to add expensive capacity. With NSX, the underlying network hardware becomes a simple IP-forwarding backplane. Rather than refresh your networking gear at the end of the accounting depreciation cycle, you can use it for longer periods. With this approach, you touch the hardware only to add more capacity or to replace individual devices when they fail.

Chapter 4

Network Virtualization Use Cases

In This Chapter

- Enhancing data center security
- Automating IT processes
- Improving application continuity

In this chapter, I walk through a series of examples of the way people are putting network virtualization into action. As I note in Chapter 3, virtualization with NSX is not an all-or-nothing approach. You don't have to virtualize your entire network. You can virtualize portions of your network for targeted use cases and then expand your use of virtualization over time.

And here's a cool fact: Enterprises can often justify the cost of NSX through a single use case — while they establish a strategic platform that automates IT and drives additional use cases and projects over time.

In the following sections, I drill down into some of the more common use cases, to show how you can use network virtualization to speed up processes, strengthen security, and keep your applications up and running.

Securing the Data Center

As I note elsewhere, security is a huge and ever-growing concern for enterprises. Here are some of the ways that

network virtualization can help you mitigate the risks of data breaches.

Limiting lateral movement within the data center

Modern attacks exploit inherent weaknesses in traditional perimeter-centric network security strategies to infiltrate enterprise data centers. After successfully evading the data center's perimeter defenses, an attack can move laterally within the data center from workload to workload with little or no controls to block its propagation.

Micro-segmentation of the data center network restricts unauthorized lateral movement but, until now, hasn't been operationally feasible in data center networks.

Traditional packet-filtering and advanced next-generation firewalls implement controls as physical or virtual choke points on the network. As application workload traffic passes through these control points, network packets are either blocked or allowed to traverse the firewall based on the firewall rules that are configured at that control point.

There are two key operational barriers to micro-segmentation using traditional firewalls: throughput capacity and security management.

Limitations on transport capacity can be overcome, but at a significant cost. It's possible to buy enough physical or virtual firewalls to deliver the capacity required to achieve micro-segmentation, but in most (if not all) organizations, purchasing the number of firewalls necessary for effective micro-segmentation isn't financially feasible. I'm effectively talking about a separate firewall per virtual machine. How many virtual machines does your data center have? Hundreds? Thousands? This would mean potentially thousands of firewalls for a typical data center.

The burden of security management also increases exponentially with the number of workloads and the increasingly dynamic nature of today's data centers. If firewall rules need to be manually added, deleted, and/or modified every time

a new VM is added, moved, or decommissioned, the rate of change quickly overwhelms IT operations. It's this barrier that has been the demise of most security teams' best-laid plans to realize a comprehensive micro-segmentation or least-privilege, unit-level trust strategy in the data center.

The software-defined data center (SDDC) leverages a network virtualization platform to offer several significant advantages over traditional network security approaches — automated provisioning, automated move/add/change for workloads, distributed enforcement at every virtual interface and in-kernel, scale-out firewalling performance, distributed to every hypervisor and baked into the platform.

The growth of east–west traffic within the data center

Over the past decade, applications have increasingly been deployed on multitier server infrastructures, and east–west server-to-server communications now account for significantly more data center traffic than north–south client-to-server and Internet communications. In fact, traffic inside the data center now accounts for as much as 80 percent of all network traffic. These multitier application infrastructures are typically designed with little or no security controls to restrict communications between systems.

Attackers have modified their attack strategy to take advantage of this paradigm shift in data center traffic, as well as the fact that prevailing perimeter-centric defense strategies offer little or no controls for network communications within the data center. Security teams must likewise extend their defense strategy inside the data center — where the vast majority of network traffic actually exists and is unprotected — instead of focusing almost exclusively on perimeter defenses.

Visibility and context

The growth of east–west traffic within the data center and the rise of server virtualization are two trends that have contributed to an alarming lack of visibility and context in the data center.

For the most part, east–west server communications in the data center do not pass through a firewall and are, therefore, not inspected. For all intents and purposes, this traffic is invisible to network security teams. When east–west traffic *is* forced through a firewall — using techniques such as hairpinning to backhaul the traffic through a firewall choke point — the result is a complex and inefficient communication path that negatively affects network performance throughout the data center.

Innovation in server virtualization has far outpaced the underlying network and security constructs in traditional data and context in the data center. Deploying multiple virtual workloads on a single physical host configured with multiple network interface cards (NICs) is common in virtual server environments. Without virtual switches, the traffic going to and from individual VMs cannot be easily identified. This can cause significant issues for network teams attempting to identify and troubleshoot problems, and is fertile ground for an attacker.

The network hypervisor in a virtualized network is uniquely positioned to see all traffic in the data center, down to the level of individual VM workloads. This level of visibility and context enables micro-segmentation based on attributes that are unique to each workload, such as the operating system, patch level, running services, and many other properties. This capability, in turn, enables more intelligent network and security policy decisions that can be defined with an understanding of the specific purpose of each individual workload in the data center. For example, unique policies can be specifically defined for the web tier of an order-taking application, or for an enterprise human resources management system, based on the needs of the individual workload rather than be constrained by the underlying network topology.

Isolation

Isolation is an important principle in network security, whether for compliance, containment, or simply keeping development, test, and production environments separated. Manually configured and maintained routing, access control lists (ACLs), and/or firewall rules on physical devices have

traditionally been used to establish and enforce isolation in data center networks.

Forrester Research outlines its Zero Trust model of information security and isolation, in which perimeter security controls are extended throughout the entire data center. It requires organizations to protect external and internal data resources and enforce strict access controls. Zero Trust incorporates the principle of *least privilege,* a cornerstone of information security that limits access and permissions to the minimum required to perform an authorized function. Finally, the Trust, But Verify concept is so 1980s (with respect to, and apologies to, President Ronald Reagan). Never Trust, Always Verify is the new paradigm for a safe and secure world.

Virtual networks are inherently isolated from other virtual networks and from the underlying physical network by design. This concept is distinctly different from the legacy approach of assuming some default level of trust within the data center. Isolation is inherent to network virtualization — no physical subnets, VLANs, ACLs, or firewall rules are required in order to enable this isolation. Virtual networks are created in isolation and remain isolated unless deliberately and explicitly connected.

Any isolated virtual network can be made up of workloads distributed anywhere in the data center, and workloads in the same virtual network can reside on the same or separate hypervisors. Additionally, workloads in several isolated virtual networks can reside on the same hypervisor. Isolation between virtual networks also allows for overlapping IP addresses. So, it's possible, for example, to have isolated development, test, and production virtual networks, each with a different application version, but with the same IP addresses, all operating at the same time on the same underlying physical infrastructure.

Finally, virtual networks are also isolated from the underlying physical infrastructure. Because traffic between hypervisors is encapsulated, physical network devices operate in a completely different address space than the workloads connected to the virtual networks. For example, a virtual network could support IPv6 application workloads on top of an IPv4 physical network. This isolation protects the underlying physical infrastructure from any possible attack initiated by workloads

in any virtual network. Again, all this is independent from any VLANs, ACLs, or firewall rules that would traditionally be required in order to create this isolation.

Segmentation

Related to isolation, but applied within a multitier virtual network, is segmentation. Traditionally, network segmentation is achieved with a physical firewall or router that allows or denies traffic between network segments or tiers — for example, segmenting traffic between a web tier, application tier, and database tier. Segmentation is an important principle in security design because it allows organizations to define different trust levels for different network segments and reduces the attack surface should an attacker breach the perimeter defenses. Unfortunately, data center network segments are often far too large to be effective, and traditional processes for defining and configuring segmentation are time consuming and prone to human error, often resulting in security breaches.

Network segmentation, like isolation, is a core capability of a network virtualization platform. A virtual network can support a multitier network environment — multiple layer 2 segments with layer 3 segmentation (or micro-segmentation) on a single layer 2 segment, using distributed firewalling defined by workload security policies. These could represent a web tier, an application tier, and a database tier, for example.

In a virtual network, network and security services — such as layer 2, layer 3, ACLs, firewall, quality of service (QoS), and others — that are provisioned with a workload are programmatically created and distributed to the hypervisor virtual switch and enforced at the virtual interface. Communication within a virtual network never leaves the virtual environment, removing the requirement for network segmentation to be configured and maintained in the physical network or firewall.

Automation

Automated provisioning enables the correct firewalling policies to be provisioned when a workload is programmatically

created, and those policies follow the workload as it's moved anywhere in the data center or between data centers.

Equally important, if the application is deleted, its security policies are automatically removed from the system. This capability eliminates another significant pain point — firewall rule sprawl — which potentially leaves thousands of stale and outdated firewall rules in place, often resulting in performance degradation and security issues.

Enterprises can also apply a combination of different partner capabilities by chaining advanced security services together and enforcing different services based on different security situations. This enables organizations to integrate their existing security technologies to build a more comprehensive and correlated security capability inside the data center. Existing security technologies actually function better with micro-segmentation than otherwise possible, because they have greater visibility and context of individual workload VM traffic inside the data center, and security actions can be customized for individual VM workloads as part of a complete security solution.

For example, a workload may be provisioned with standard firewalling policies, which allow or restrict its access to other types of workloads. The same policy may also define that if a vulnerability is detected on the workload during the course of normal vulnerability scanning, a more restrictive firewalling policy would apply, restricting the workload to be accessed by only those tools used to remediate the vulnerabilities.

Security vendors can take advantage of the network virtualization platform to trigger advanced security service responses from a completely different security vendor's technology solution — an innovation that's accelerated with network virtualization.

Secure user environments: Micro-segmentation for VDI

Many enterprises have deployed virtual desktop infrastructure (VDI) to leverage virtualization technologies beyond the data center. Micro-segmentation enables these organizations

to extend many of the security advantages of the SDDC to the desktop — and even to mobile environments — including the following:

- Integrating key network and security capabilities into VDI management
- Eliminating complex policy sets and topologies for different VDI users
- Setting firewall and traffic filtering and assigning policies for logical groupings
- Decoupling security policies from the network topology to simplify administration

Through its ability to implement micro-segmentation, VMware NSX effectively enables each virtual desktop to have its own firewall. This allows a much more granular level of security — that extends all the way down to the virtual network interface. Based on policies, all traffic to and from that VM can be secured, preventing unauthorized communication between VMs or other workloads. If an end-user's virtual desktop becomes compromised, the exposure can easily be contained to only that user.

Automating IT Processes

In large data centers, manual processes are the bane of the IT admin's existence and a drain on the manager's budget. Network virtualization helps you address these challenges by automating labor-intensive, error-prone tasks associated with network configuration, provisioning, management, and more.

IT automation

With NSX, powerful orchestration capabilities distribute network services in parallel with virtual machines. You can use NSX to standardize and maintain predefined templates that consist of network topologies and services. With the template approach, environments can be provisioned in seconds with consistent configuration and security.

When you step up to bat with NSX IT automation capabilities, you're poised for a triple play: Reduce operational expense, accelerate time to market, and speed IT service delivery.

Developer cloud

NSX is ideally suited for use as a platform for self-service developer clouds, as well as other Infrastructure-as-a-Service (IaaS) initiatives. You can use automated network and service provisioning to give your development and test teams fast access to the infrastructure they need — so that they can get software apps and upgrades into the hands of users in less time.

NSX can provision thousands of isolated networks for development, testing, and staging environments — all on the same physical infrastructure. In this new way of doing business, NSX removes the manual tasks and cycle time associated with procuring, installing, and configuring network infrastructure. Networks are deployed in lock step with their workloads — as fully audited self-service transactions. Applications quickly move through development, testing, staging, and production without changes to their IP addresses.

Thanks to virtualization, provisioning network infrastructure for development/testing teams is no longer a bottleneck that slows down the business and delays time to market.

Multitenant infrastructure

In multitenant cloud environments, you can use the micro-segmentation and isolation capabilities of NSX to maintain isolation between tenants. NSX enables you to create virtual networks and have them completely isolated from any other virtual network and from the underlying physical network. You can have two different tenants running on the same IP addresses on the same physical infrastructure without having any conflict between these IP addresses because the virtual networks don't even know that each other exists, nor do they know that the physical network exists.

For a broader solution, you can add advanced services based on virtual network, network segment, or security group. For example, you might add deep packet inspection via firewalls such as those from Palo Alto Networks. With this service, you can granularly define traffic flows that will be redirected to the Palo Alto Networks VM-Series firewall for inspection and enforcement. Traffic allowed by the VM-Series Firewall is then returned to the NSX virtual switch for delivery to the final destination (guest VM or physical device).

Enabling Application Continuity

Keeping applications up and running is one of the top mandates of the IT organization. Network virtualization can help you maintain the availability of apps through its ability to enable disaster recovery, metro pooling, and hybrid cloud use cases.

Disaster recovery

You can use NSX as a complement to your existing disaster recovery solutions — to enable faster recovery and reduce downtime. In this use case, NSX replicates the entire network and its security environment. You can then periodically snapshot the network construct, along with its applications and services, and maintain your copy at a recovery site.

To make things easier, you don't need to change IP addresses, because the virtual network is decoupled from the underlying hardware and topology. The disaster recovery site is identical to the primary site, with no trade-offs in functionality or performance. The copy sits at the recovery site in standby mode for push-button activation in the event of a disaster. Any changes made to the source network are automatically replicated to the copy at the recovery site.

Metro pooling

Network virtualization enables the pooling of compute resources that are in different physical locations but in close proximity (local area or metro area). Disparate resources can then be treated as a unified set of compute resources.

Applications can be deployed in any location yet seamlessly connect to the resources located across the sites. This has been a prevalent use case for NSX in multisite deployments.

Hybrid cloud networking

NSX is a good networking choice for hybrid cloud environments that extend the on-premises network to a public cloud. NSX enables secure, on-demand access to IT resources with the flexibility to move workloads onsite or offsite to meet specific needs.

Better still, NSX is designed to work with any cloud management platform. Out-of-the-box support is available for many platforms, and integration with other management platforms is provided through the NSX API. This makes it easy to gain the security you need in your private cloud with the scalability and reach of a public cloud.

Chapter 5

Operationalizing Network Virtualization

In This Chapter

- Introducing the concept of operationalizing
- Exploring operations investment areas
- Addressing issues related to staffing and jobs

Operationalizing NSX involves optimizing people, processes, and technology to use network virtualization and the security capabilities it enables.

Your enterprise must be successful at operationalizing NSX to achieve the promise of network virtualization — and the overarching benefits of speed, agility, and security. How well you operationalize NSX will determine how fast you realize the IT and business benefits.

Operationalizing network virtualization should be viewed as a gradual cultural and technical journey, where your organization achieves ever-growing maturity and sophistication as you move from a hardware-defined data center to a software-defined data center. It's a journey that will make heroes and careers, just as compute virtualization did a decade ago.

The purpose of this chapter is not to provide all the answers to what it takes to operationalize NSX, which would take a book in itself, but rather to introduce the topic and highlight some of the key areas you should consider on your journey to network virtualization.

As you embark on your NSX journey, clearly define your long-term vision for your fully optimized SDDC. Consider how you need to evolve your people, processes, and technology to get you there.

Operations Investment Areas

You should consider six key operations investment areas on your journey toward network virtualization. These investments help you gain maximum business value for your organization and maximum career value for your IT staff.

I recommend that you take a holistic approach, one that encompasses these concepts:

- Organizational structure
- Roles and responsibilities
- Processes
- Tooling
- Architecture
- Infrastructure

Organization and people

SDDC operations impact most of the IT organization. These operations span compute, networking, storage, security, and personnel — including operators, administrators, engineers, and architects. When you operationalize NSX, include all necessary players in the process, and be transparent.

Here are some other best practices regarding your IT organization and its people:

- **Your existing network and security teams take on NSX.** There's no need to change your teams or create new ones. Functional roles also remain the same (for example, architects, engineers, operators, admins). Existing roles and responsibilities evolve to include network virtualization.

- **Consider how you can create a more blended cloud team** with cross-domain and cross-disciplinary skills, common goals and operating principles, intra-team training and development, and alignment around service delivery for the business.
- **Consider these networking and security roles for your cloud network:** architecture, security, orchestration and automation, development and integration, administration, operations, and support and escalation.
- **Garner your team's support.** Make sure all players on your team understand the value proposition and what it will mean to them personally and professionally as new opportunities to work on more interesting and strategic projects become available.
- **Reassure your networking staff about their job security.** Make it clear to your networking staff that they will not be automated out of a job and that their jobs will not be moved to the virtualization team. Your existing networking staff takes on network virtualization. Only they have the required networking expertise.
- **Involve your cloud operations staff early in the evaluation process.** Then they can learn how NSX will make their jobs easier, and so they become advocates for the project. Don't surprise them just before you want to deploy.
- **Include security early in the evaluation.** The security team needs to learn how isolated virtual networks are as secure as physical networks. They need to learn that micro-segmentation does not replace existing perimeter firewalls for north–south traffic, but rather allows your organization to control east–west traffic inside the data center.

Take advantage of VMware's operations-focused resources (technical guides, workshops, training, and certifications) to gain the necessary expertise, skills, and knowledge required for network virtualization and the SDDC.

Processes and tooling

One primary benefit of network virtualization is that formerly manual processes can be automated. This does, however, require some upfront investment in the appropriate tools.

Some automation of tasks can be achieved directly within the NSX Manager, whereas other automation functions will be provided by other tools, such as a cloud management platform.

NSX provides a central point of control — the NSX Manager — for the creation, management, and monitoring of virtual networks. Operation of an NSX environment will naturally focus on the NSX Manager, either through its UI or via API calls made to the NSX Manager by other tools (such as VMware vRealize Automation, VMware vRealize Operations, OpenStack, and other third-party tools).

In addition, it will be necessary to manage the underlying infrastructure, which includes both NSX components (controllers, edge nodes, hypervisors) and network infrastructure (the underlay). NSX provides its own ability to manage these elements, and third-party tools may also play a central role in managing the infrastructure.

When you operationalize NSX, take a step back and consider the full range of implications for your processes and tooling. In particular, keep these best practices in mind:

- **Analyze your existing network and security processes, and understand them in detail.** Determine how to simplify and streamline your processes via orchestration and automation.
- **Consider the impact that network virtualization has on activities such as monitoring, troubleshooting, change management, release management, and capacity management.** Understand how these key activities work today and how they can be simplified.
- **Determine your priorities for automating networking processes and standardizing environments (for example, configurations and policies) to reduce operational effort and expenses.** Automation and policy-based provisioning of networks and services eliminate common configuration errors and improve tracking of changes for audit and compliance.
- **Determine whether you should use your existing management and operations tools or whether you should evaluate modern alternatives.** These modern

alternatives provide an end-to-end view of application health across compute, storage, and networking. Gain visibility into the object relationships between virtual and physical components.

- **Identify VMware and third-party tools for management of virtual and physical components.** Assess how you can leverage NSX native capabilities and APIs for deep integration with existing tools, such as cloud management platforms and orchestration and automation tools.
- **Use your existing tools to operate virtual networks.** Virtual networks provide all the operational information that is expected from physical networks (for example, packet and byte counters, NetFlow export). Many existing tools can leverage the information provided by NSX for operational tasks.
- **Use your existing favorite tools to monitor and troubleshoot.** A single-vendor approach does not always give you the best visibility. You may find that using multiple tools (for example, vRealize Operations, Splunk, Wireshark, NetFlow collectors) will allow you to best monitor and troubleshoot your network infrastructure.

Architecture and infrastructure

NSX network virtualization decouples network services from the underlying physical infrastructure. This makes it possible to design the underlying physical infrastructure with a focus on operational efficiency rather than support of particular features or services. The physical network can be engineered for stability, and changes to the configuration of the physical network become rare.

From an operational point of view, this means that deployment of networking capabilities (for example, firewalling) can be decoupled from the deployment of physical infrastructure. This sets the stage for incremental deployment of new capabilities on a per-application basis. It also means that hardware upgrades (for example, deployment of new network switches) can be decoupled from the deployment of NSX.

With NSX, a unified virtualization platform injects simplicity and consistency across your operations. It provides a centralized point of control for networking, security functions, and

the distributed implementation of policies. Automation minimizes manual changes to the physical network, whereas security policies are applied more efficiently and more accurately.

In another important benefit, operationalizing NSX frees your workloads from the shackles of VLANs and IP addressing. This has a direct impact on operations. It enables faster provisioning and application access, more efficient resource utilization, lower operations costs, and happier application teams.

Here are a few of the key steps forward in operationalizing NSX:

- **Incrementally deploy network virtualization and security.** You can start small with a single use case and set of applications. Identify workloads with the best risk/reward profile to leverage new capabilities.
- **Minimize costly rip and replacement of physical networks.** NSX does not require a re-architecture of the physical network, but it does make a change in network architecture more feasible. NSX frees network designers to use leaf-spine architectures, because it abstracts the virtual network topology (as seen by VMs) from the physical topology.
- **Create a single application-level view for monitoring and troubleshooting across the physical and virtual infrastructure.** Because the NSX switch sees every packet as it enters and leaves a VM, NSX provides the highest level of visibility into the behavior of network traffic.
- **Establish a regular cadence for developing and releasing new cloud networking and security features.** This practice promotes active participation and feedback from the cloud infrastructure and application teams.
- **Create a centralized point of control for the management and monitoring of virtual networks and security.** The combination of centralized control with distributed implementation of services means that fine-grained policies can be operationalized. For example, VMs in the same tier of a three-tier app can talk to other tiers, but not to each other.
- **Set security policies based on high-level constructs (for example, OS name, user, group) rather than**

low level (for example, IP address). Security policy can be more efficiently applied and with higher precision and correctness.

- **Deploy NSX on hypervisors connected to any existing physical network infrastructure, and support next-generation fabrics and topologies from any vendor.**

Focus on the Big Picture

Like any major IT initiative, network virtualization changes a lot of things in your data center. But one thing it doesn't change is your job security. Networking pros are essential to the success of a virtualized network environment. You can't get there without them.

When you're part of a network virtualization initiative, you have the opportunity to participate in and contribute to the transformation of networking and security at your company. The outcome will be beneficial for you, just as it was for those who championed and built their careers on compute virtualization. Embrace this important leadership opportunity.

As you virtualize and automate your infrastructure, it will free you up to work on more interesting and strategic initiatives. For example, rather than the mundane work of configuring a router or updating firewall rules, you can work on designing a spine-leaf network, automating networking and security workflows, or perhaps building a developer cloud.

Today is the Golden Era of Networking. Participating in a network virtualization initiative will enrich you professionally, prepare you for the future, and make you more valuable in the job market — just as server virtualization did for server admins a decade ago.

Network virtualization advances your career, allowing you to spend more time on network architecture, design, and traffic engineering.

- **When you implement network virtualization, you won't be automated out of a job.** Instead, your job will be transformed to allow you to work on more interesting and strategic projects.

- **Your job won't go to the virtualization team.** NSX relies on the same networking concepts and technologies as physical networks; therefore, it requires networking and security expertise.
- **Virtualization won't make your job more difficult.** The virtual overlay, combined with automation and a simplified physical underlay, streamlines network provisioning and management.

Chapter 6

Ten (Or So) Ways to Get Started with Network Virtualization

In This Chapter

- Highlighting resources packed with valuable insights
- Test-driving with the number-one Hands-on Labs
- Exploring how to deploy NSX in your environment

In this chapter, I tell you ten things (more or less) that you've always wanted to know about getting started with network virtualization but were afraid to ask. I walk you through a library of resources on network virtualization, highlight opportunities to deploy the VMware NSX platform with Cisco infrastructure, and explain how NSX is designed for integration with your existing infrastructure and third-party solutions for network services, such as load-balancing devices and next-generation firewalls.

Don't Miss the Essential Resources

I begin with a look at some of the resources that are available to help you enrich your understanding of network virtualization, the components of a virtualized network, and the tools that are available to help you get started.

Boning up on the basics

VMware offers a wide range of resources to help you get grounded in the basics of network virtualization:

- **The VMware NSX product page (`www.vmware.com/go/nsx`):** The NSX product page summarizes the basic features, functions, and benefits of the NSX platform. It also serves as a portal that provides links to a wide range of deep-dive assets, including technical information and business-focused content.
- **VMware NSX introduction video (`www.youtube.com/watch?v=PciyGPCykLI`):** This fast-moving video, which runs about four minutes, explains how VMware NSX serves as the foundation for a network virtualization platform that delivers the operational model of a virtual machine to the network. Meet Raj, the video narrator, a guy who works at a company where innovation can't come fast enough.
- **#VirtualizeYourNetwork (`http://virtualizeyournetwork.com`):** #VirtualizeYourNetwork is an online resource for the people, teams, and organizations that are adopting network virtualization to transform data center operations and economics. Via this site, you can explore how networking and the data centers are changing, engage with thought leaders and peers, and gain information that could help you evolve your IT career.

Taking a deeper dive

Available white papers cover business-oriented discussions, technical overviews, and the views of industry analysts. You can also dive into a detailed guide focused on using micro-segmentation to build a more secure data center. This list describes a couple of resources that are just a click or two away:

- **VMware NSX Network Virtualization Platform white paper (`www.vmware.com/files/pdf/products/nsx/VMware-NSX-Network-Virtualization-Platform-WP.pdf`):** This 12-page technical white paper explores the features, characteristics, capabilities, and benefits of the VMware NSX platform. You'll come away with a better

understanding of why growing numbers of technically savvy organizations are selecting NSX as their platform for network virtualization.

- ***Micro-segmentation For Dummies*** **(`http://info.vmware.com/content/33851_Micro-Segmentation_Reg?CID=70134000000NzKR&src=test&touch=1`):** This lively book, which is available online, provides a close-up look at micro-segmentation, including the basics on how it works, the enabling technologies, and the wide-ranging security benefits. Learn how to develop an inherently secure data center that helps prevents the lateral spread of attacks within your data center.

Chatting with bloggers

In these wide-ranging blogs, VMware network virtualization specialists share their insights and first-person experiences. Get the inside story directly from the people who live and breathe network virtualization:

- **The Network Virtualization blog (`http://blogs.vmware.com/networkvirtualization`):** Check out this blog for the latest news and technical insights about network virtualization. It serves as a key industry source for accurate news and factual information about network virtualization.
- **Scott Lowe's weblog (`http://blog.scottlowe.org`):** Via his weblog — as well as his books, video training series, and presentations — IT pro Scott Lowe shares his insights into virtualization, networking, open-source solutions, and cloud computing. This is a great place to gain information, insights, and technical knowledge on the technologies related to network virtualization.

Taking an NSX test drive with Hands-on Labs

To enrich your understanding of a platform like VMware NSX, it always helps to hop into the driver's seat for a test drive. That's the idea behind the VMware number-one Hands-on Labs (`www.vmware.com/go/try-nsx-en`).

VMware Hands-on Labs deliver a fully operational live desktop environment for you to experience VMware products with no setup required. With click-by-click guidance and all products preinstalled, you can focus on the product features you value most. This is a great way to get closely acquainted with the capabilities of VMware NSX without installing any software on your system.

Learning how to deploy NSX in your environment

When you're ready to explore your deployment options, you can get started by learning about network virtualization and NSX via on-demand resources. VMware offers a variety of ways to experience the benefits of network virtualization and NSX, from online courses to live webinars to self-paced on-demand courses.

Taking a VMware education course

Start your journey by learning about the fundamentals of network virtualization and the business challenges NSX can help you solve. After that, you can take a self-paced, on-demand course that provides a sneak peek into how to install, configure, and manage NSX. Just go to `http://mylearn.vmware.com/portals/www/search/results.cfm?ui=www_edu&pID=www&menu=search-results&searchtype=simple&orderBy=relevance&category=catalog&keyword=NSX&Search=Search&deliveryType=2&filters=deliveryType`.

Touring the Platform via NSX Product Walkthrough

If you're the more adventurous network virtualization type, you can continue your journey through the NSX Product Walkthrough (`https://featurewalkthrough.vmware.com`), a series of technically oriented introductory videos on the capabilities of NSX.

The NSX Product Walkthrough ranges from a look at the basic features of the NSX platform to integrations with

VMware and partner products. Here's a list of available presentations:

- **Introduction to VMware NSX:** Review key features and capabilities of NSX, including NSX Manager, gateway services, firewalls, monitoring and troubleshooting, and CMP integration.
- **VMware NSX for vSphere:** Learn how to use the features of VMware NSX, including VXLAN, network virtualization, and VXLAN-to-VLAN bridging services.
- **Security and Compliance:** Explore the security challenges of adopting a software-defined data center, how to add a distributed firewall using VMware NSX network virtualization, and the benefits of the NSX Service Composer.
- **NSX Partner Integration:** Take a look at the extensibility of VMware NSX and its integration with third-party gateways and security features.
- **Integration with VMware Components:** Learn about the benefits delivered by the integration of NSX with other VMware components.

Diving Down into the Technical Details

Oh, you say you want the technical view? To start your technical exploration, check out the NSX design guide and the NSX guide to getting started, both described in this section:

- **VMware NSX for vSphere Network Virtualization Design Guide (`https://communities.vmware.com/docs/DOC-27683`):** For the truly deep-dive technical stuff, download the design guide. This document is targeted toward virtualization and network architects interested in deploying the VMware NSX network virtualization solution in a vSphere environment. This guide includes detailed information on
    - NSX-v functional components
    - Functional services
    - Design considerations

- **NSX for vSphere Getting Started Guide (`https://communities.vmware.com/docs/DOC-27705`):** This resource provides step-by-step examples that demonstrate how to set up network services in NSX for vSphere, including the following:
  - Logical switches
  - Logical distributed routers
  - Distributed firewalls
  - Logical centralized routers (edge) with dynamic routing and with many-to-one network address translation (NAT)
  - Logical load balancers (edge)

Deploying NSX with Cisco UCS and Nexus 9000 Infrastructure

As NSX gains broader adoption, VMware has heard from many IT shops that want to run NSX on top of the latest Cisco infrastructure — specifically, Cisco UCS blade servers and Cisco Nexus 9000 Series switches. With this combination, the underlying hardware provides reliable, resilient capacity while the configuration, state, and advanced features move to faster, more flexible software.

As with any IP fabric, NSX works great with Nexus 9000 as the underlay. The combination of NSX and Nexus 9000 Series switches in stand-alone mode enables the benefits of the SDDC.

To help IT shops make this leap into the future, VMware offers a ready-to-go reference architecture, along with the VMware NSX for vSphere Network Virtualization Design Guide. The reference architecture covers the fundamental building blocks of NSX with VMware ESXi, recommended configurations with Cisco UCS, and connectivity of UCS to Nexus 9000 switches.

For a close-up look at this reference architecture, see the document *Reference Design: Deploying NSX with Cisco UCS and Nexus 9000 Infrastructure,* at `www.vmware.com/files/pdf/products/nsx/Design-Guide-for-NSX-with-Cisco-Nexus-9000-and-UCS.pdf`.

Integrating NSX with Your Existing Network Infrastructure

NSX is designed to integrate with your existing network infrastructure to bridge the physical and virtual worlds using the L2 gateway functionality. These integrations recognize that in the hyperdynamic environment of the modern data center, the underlay transport network and the overlay network virtualization solutions are codependent actors in the delivery of optimal performance, reliability, and scale.

To enable these integrations, VMware works actively with its L2 switching partners to create reference architectures and design guides for using NSX as an agile overlay that leverages the capabilities of the underlay infrastructure.

Here's a sampling of the technical resources that are available to guide the integration of NSX with your existing network infrastructure:

- **Arista:** VMware and Arista Network Virtualization Reference Design Guide for VMware vSphere Environments (`www.vmware.com/files/pdf/products/nsx/White_Paper_Design_VMware_Arista_3-15-2014.pdf`)
- **Brocade:** VMware and Brocade Network Virtualization Reference Whitepaper (`https://communities.vmware.com/docs/DOC-28347`)
- **Cisco:** Reference Design: Deploying NSX with Cisco UCS and Nexus 9000 Infrastructure (`https://communities.vmware.com/docs/DOC-29373`)
- **Dell:** Network Virtualization with Dell Infrastructure and VMware NSX Reference Architecture (`https://communities.vmware.com/docs/DOC-27684`)
- **Juniper:** Connecting Physical and Virtual Networks with VMware NSX and Juniper Platforms (`https://communities.vmware.com/docs/DOC-27610`)

Integrating with Your Networking Services Ecosystem Partners

In addition to integrating with your existing network infrastructure, NSX is designed to integrate with solutions for various network services, such as load-balancing devices and next-generation firewalls and services.

This list spells out the growing family of NSX partners:

- **Physical-to-virtual:** Arista, Brocade, Cumulus, Dell, HP, Juniper
- **Network security:** Check Point, Fortinet, Intel Security, Palo Alto Networks, Rapid 7, Symantec, Trend Micro
- **Visibility and monitoring:** Arkin Net, EMC Smarts, NetScout, Gigamon, Tufin, Riverbed (SteelCentral)
- **Application delivery controller:** F5 Networks

Make network virtualization work for your enterprise!

Today's data centers make heavy use of server and storage virtualization. This puts them on the path to the benefits of the software-defined data center. But there's a catch: the network. In many ways, networking is stuck in a hardwired past. With conventional approaches to the network, services still require manual provisioning and are anchored to vendor-specific hardware and topologies. This old way of doing things slows application deployment time and blocks the road to the software-defined data center.

Network virtualization changes this equation. Virtualized networks are created, provisioned, and managed entirely in software — to bring new levels of agility, efficiency, and security to data center operations. In simple, straightforward language, this quick-to-read book explains the core concepts and key components of network virtualization.

- ***See the big picture* — learn what network virtualization is, how it differs from conventional network architectures, and how it can help you operate more efficiently**
- ***Understand the architecture* — explore the ins and outs of this new approach to the network**
- ***Learn how to get started* — gain tips and tricks for your implementation and insights into best practices and common pitfalls**

Open the book and find:

- **Why the time is right for a new approach to the network**
- **Key use cases for network virtualization**
- **Why network virtualization is a key building block of the software-defined data center**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Mora Gozani is the Senior Product Line Marketing Manager for VMware's Network and Security (NSX) business unit. Mora received her BA from the University of California Santa Barbara and her MS from the Thunderbird School of Global Management. Mora currently resides in Los Altos, California.

FOR DUMMIES® A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-12583-9
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.