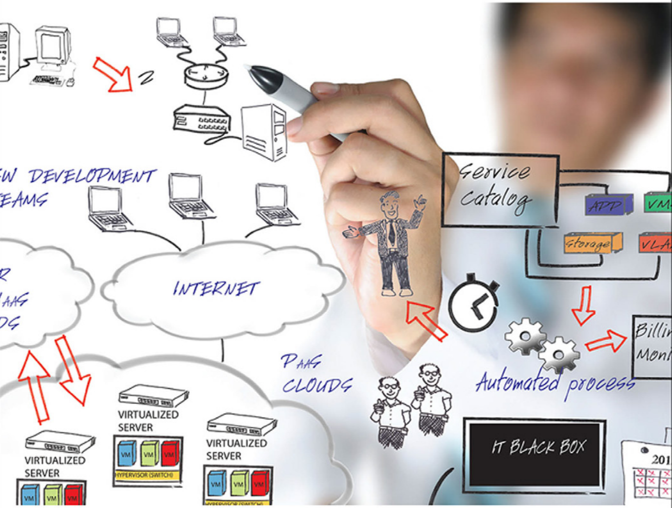
SDN and NFV Simplified

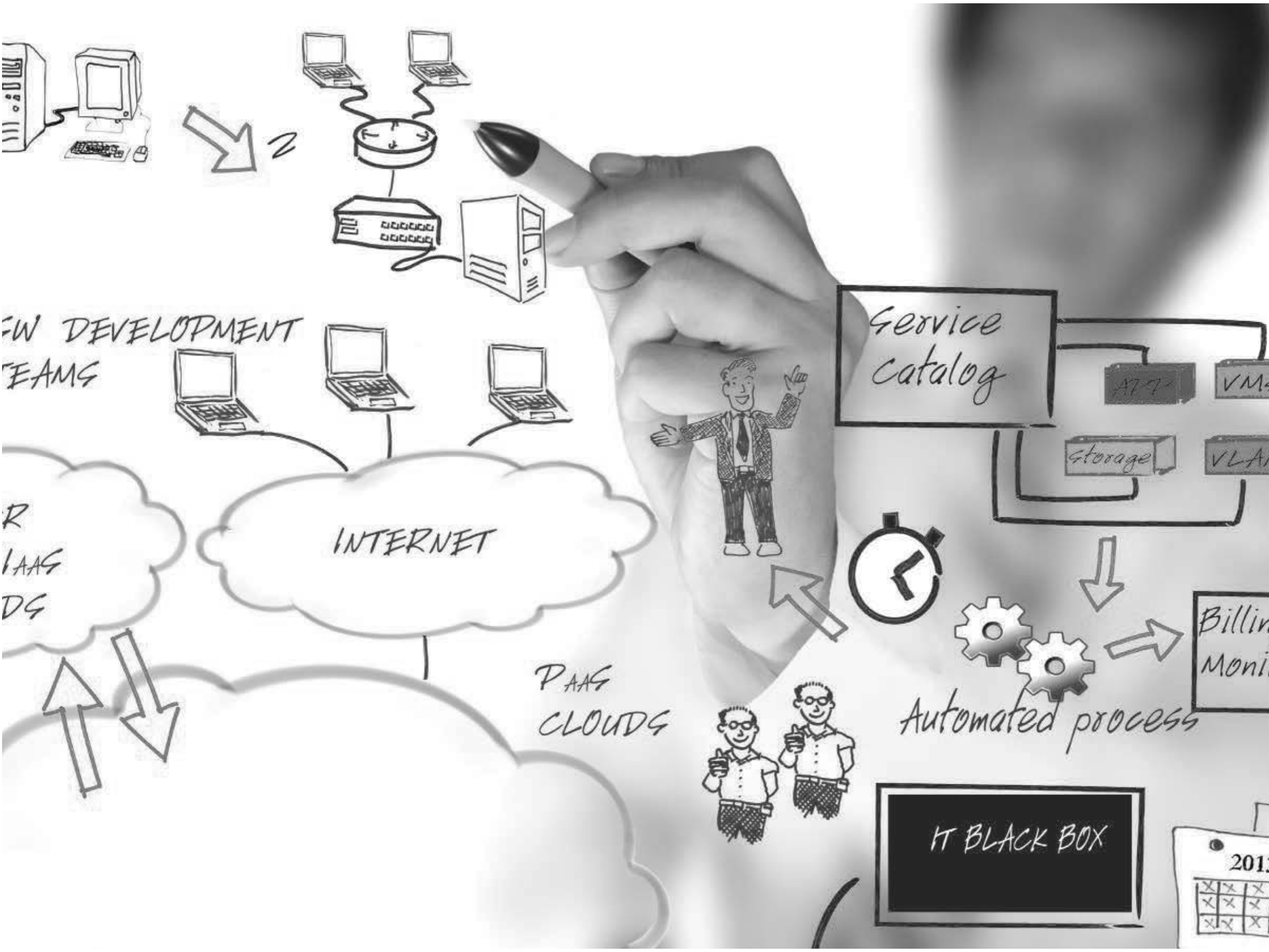
A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization



Jim Doherty

SDN and NFV Simplified

A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization



Jim Doherty

SDN and NFV Simplified

Jim Doherty

ISBN-13: 978-0-13-430640-7
ISBN-10: 0-13-430640-6

Library of Congress Control Number: 2015956324

Text printed in the United States on recycled paper at RR Donnelley in Kendallville, Indiana.

First printing: March 2016

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Visit us on the Web: informit.com/aw

Editor-in-Chief
Dave Dusthimer

Executive Editor
Mary Beth Ray

Development Editor
Jeff Riley

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Keith Cline

Indexer
Tim Wright

Proofreader
Debbie Williams

Technical Reviewer
Brian Gracely

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Compositor
Studio Galou

To Katie, Samantha, and Conor

Contents

Acknowledgments

I would like to thank the following people.

First and foremost, I want to thank my researcher and writing assistant, Alasdair Gilchrist. This book simply could not have happened without his hard work and dedication.

This book has been in the works for quite a while, and over the course of a few years, it has morphed from what was originally called *Cloud Networking Simplified*. For a variety of reasons, there were stops and starts, do overs, and evolutions, and in a couple of cases, potential co-authors were brought in. Among them were Dave Asprey, who was a very knowledgeable tech guy before becoming the "Bullet Proof Coffee" guy, and Brian Gracely, who is still a very knowledgeable tech guy who ended up being the technical reviewer of this version of the book. While this book is its own thing, several of their original contributions influenced this version.

Brian Gracely also gets his own thank you for being the technical reviewer of this book. He kept me on my toes and spent a lot of time reading, reviewing, and verifying my work. This book is much better than it would have been without his efforts.

Finally, I want to thank the great team at Pearson. Always the consummate professionals, they make my job much easier, and they are all a pleasure to work with. Specifically, I'd like to thank Executive Editor Mary Beth Ray, who had the patience to keep this project alive through all the iterations. Development Editor Jeff Riley for being a great "man behind the curtain." Line Artist Laura Robbins for helping with the whiteboard layouts and line art. And last but not least, the editing team, including Project Editor Mandie Frank, Development Editors Drew Cupp and Jeff Riley, and Copy Editor Keith Cline, who I'm sure I drove crazy with my many spelling errors, typing errors, run-on sentences, and use of passive voice. This is my sixth book with Pearson, and every crew I've worked with has been outstanding. This one is no exception. Thank you all.

Jim Doherty

About the Author

Jim Doherty has more than 17 years of engineering and marketing experience across a broad range of networking, security, and technology companies. Focusing on technology strategy, product positioning, and marketing execution, Jim has held leadership positions for Cisco Systems, Certes Networks, Ixia, and Ericsson Mobile. Currently, he is the SVP of Sales and Marketing for Percona.

Doherty is also the creator and co-author of the *Networking Simplified* series of books, which includes *Cisco Networking Simplified*, *Home Networking Simplified*, and several other titles. He has also written books on mobile security and other networking topics.

Jim is a former U.S. Marine Corps Sergeant and holds a Bachelor of Science degree in electrical engineering from North Carolina State University and an MBA from Duke University. Jim lives in Raleigh, North Carolina, with his wife and two children.

Introduction

Dear Reader,

Thank you for buying (or considering) this book. By way of background, this book is the latest in a series of *Networking Simplified* books that have covered topics such as basic networking with *Cisco Networking Simplified*, and other titles that have taken a "simplified" approach to Voice over IP (VoIP), security, and home networking.

If you are not familiar with the approach of the *Networking Simplified* books, the idea is to explain networking concepts and technologies to people who are not intending to become technical experts, but want to know what underlying networking technologies are and how they work at a high level. This includes business and marketing folks, salespeople, investors, people who work in technical companies but in nontechnical roles, and even technical people from different vocations who want a cursory introduction to networking.

In others words, I wanted to write a book that explains how all this stuff works, and why it matters, without assuming people needed to configure a router or set up a wireless network, and without assuming the readers were dummies. The aim is to not go too deep but not be too light either.

To that end, I've now written (with the help of many people listed in the acknowledgments) a book on the next big wave in networking: software-defined networking (SDN) and network functions virtualization (NFV). My approach to this book is similar to the previous books in that I start with some foundational topics, which in this case is virtualization. In fact, the first several sections of the book focus on this because 1) it's really important and 2) I did not think that there was a good resource out there that took the same simplified approach. The book then moves into SDN and NFV, and through it all are parts about cloud networks, virtualized data centers, and network virtualization.

Whiteboards

Also throughout this book, typically at the end of chapters, are "whiteboard" diagrams. These hand-drawn (and then digitized) whiteboards are meant to capture key aspects of the chapter topics and present those ideas as if they were drawn on a whiteboard.

In keeping with the at-a-glance feature of the previous *Networking Simplified* books, the whiteboards are meant as enhancements to the text, and it is hoped that they will help aid in your understanding of the topics they cover.

Who Is This Book For, and What Will You Get Out of It?

This book is mostly meant for nontechnical people who want to know what SDN, NFV, virtualization, and cloud networking are about: what they are, how they all work, and why they are important. You won't walk away from this book knowing how to configure an SDN controller, but you will know what one is and what it does. If you are a technical person with no exposure to these topics, this book can serve as a high-level introduction.

How This Book is Organized

I've broken the book into ten sections, each covering a central theme. This allows you to bounce around and pick one topic at time. If this is all brand new to you, tackling the topics in order is recommended, because they tend to build on each other.

Part 1: Virtualization 101: The Basics of Virtualization

As the name implies, Part I provides a primer on virtualization and virtual machines (VMs): what they are, how they work, and why they were adopted so quickly.

Part 2: Virtualization 201: Virtualizing the Data Center (a.k.a. Clouds)

Once you understand what VMs are, you need to know how they work together and what happens when you have an entire data center of them. This part focuses on the particulars of how clouds work and how they are managed.

Part 3: Network Functions Virtualized: Why Stop With Servers?

Servers aren't the only thing you can virtualize. In fact, many of the traditional applications such as firewalls can be virtualized, too. NFV is a key aspect of modern networking. This part explores not only the technology, but also the impact on how the networks work as a result.

Part 4: Modern Networking Approaches to Virtualization

Understanding how virtualization works is a great start, but unless you can connect to them over a network, a VM is not very useful. It turns out, however, that connecting to VMs requires some changes to networking before you can leverage their full power. This part explores some of the ways modern networks are managed.

Part 5: Software Defined Networks: Virtualizing the Network

SDN represent a pivot point in how networks are built and who manages them. The technology is analogous to the virtualization of data centers, and in fact, the shift to SDN is in large part an attempt to leverage the most value out of virtualized data centers and clouds. This part covers the basics of SDN technology and the economic impact of its adoption.

Part 6: SDN Controllers

Furthering the SDN discussion, this part goes into depth about SDN controllers. There's a lot of competition among many companies to be among the leaders in this technology, and given the economic benefits of being among the leaders, the stakes are high. In addition to looking at specific controllers, this part also looks at the economics of the technology.

Part 7: Virtualized Networks: Connecting It All Together

With an understanding of the pieces, this part puts virtualization, SDN, and NFV together. More than just how it works, the chapters here explore building and managing virtualized networks.

Part 8: Security: The Security Thing

Security is an ever-present part of networking these days, and in virtualized networks, where you don't always know where your data assets are, security is always an interesting topic. The chapters in this part deal with the unique security aspects of virtualization and virtualized networks.

Part 9: Visibility

You can only manage and control what you see, and this is no different in virtualized networks. The problem is that the very nature of virtualization creates blind spots in the network because data and information can move in a way that traditional network monitoring cannot detect. This part looks at how virtual networks are monitored.

Part 10: The Big Picture

In the last part of the book, all the topics previously mentioned come together for a view of how it all works together. Here we also look at how this technology will affect the way people work and communicate, and we take a peek into what might be coming next.

In the end, I'm hopeful that you will find this book to be useful, informative, and interesting. I sincerely appreciate having the opportunity to share this information with you.

—Jim Doherty

This page intentionally left blank

This page intentionally left blank

How Do You Virtualize a Network?

This chapter attempts to answer an important question: How do you virtualize a network? Before attempting an answer, though, it's a good time to take a step back and answer a couple of "big" questions, such as:

- What exactly is network virtualization, and how does it relate to the virtualization covered so far in this book?
- How does network virtualization fit into the grand scheme of network functions virtualization (NFV) and software-defined networking (SDN)?

Once we answer these questions, it's much easier to answer the question that the chapter title poses. More importantly, these answers provide the framework of *why* we would want to virtualize the network.

Network Virtualization

As mentioned throughout the first two sections of this book, virtualization (which typically means server virtualization when used as a standalone phrase) refers to the abstraction of the application and operating system from the hardware.

In a similar way, network virtualization is the abstraction of the network endpoints from the physical arrangement of the network. In other words, network virtualization allows you to group or arrange endpoints on a network independent from the their physical location.

It's worth noting that network virtualization is nothing new. In fact, it's been around a long time. The most common forms of network virtualization are virtual LANs (VLANs), virtual private networks (VPNs), and Multiprotocol Label Switching (MPLS). All of these technologies essentially enable the administrators to group physically separate endpoints into logical groups, which makes them behave (and appear) as if they are all on the same local (physical) segment. The ability to do this allows for much greater efficiencies in traffic control, security, and management of the network.

In many cases, this type of virtualization is performed via some form of encapsulation whereby messages or traffic between endpoints in the same logical group are "packaged" into another message that is better suited for transport over a physical segment of the network. Once the message has reached the endpoint, the original message is unpacked, and the intended endpoint receives the message in the same format as it would have if the two endpoints were on the same physical segment of the network.

Figure 10-1 illustrates one way that VLANs would be used. In this case, workers in different departments work on multiple floors of a building. A single switch can service each floor of the building, such that all workers on a given floor would be part of the same network segment. VLANs allow you to logically group endpoints so that they all look as if they are on the same segment. Further, this can be done across many buildings or even across large networks where endpoints are scattered all over the globe—although care should be taken when extending VLANs over long distances because they can create fragile networks.

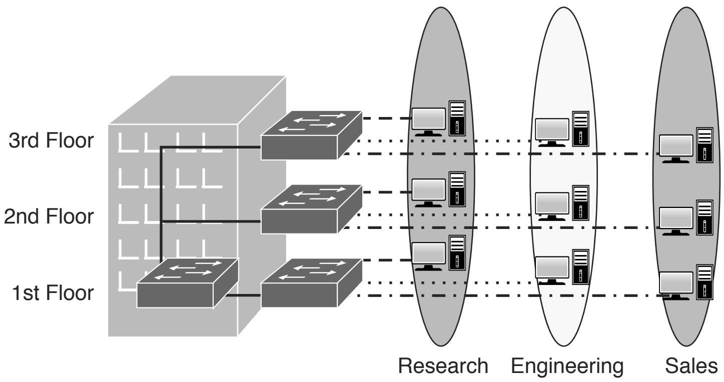


Figure 10-1 *Virtual LANs, or VLANs, were an early form of network virtualization that allowed physically separate endpoints to behave as if they were all connected to the same local switch.*

It turns out that this good old technique that has been around for many years makes server virtualization, or more accurately connecting VMs, much easier and much more efficient. It's easy to see why when you imagine the VMs being spun up here, there, and everywhere in a virtualized data center or cloud, and then being paused, moved, started again, or even being moved while still being active.

With all that spontaneous creation and movement that is done without any regard for the specific physical location in the data center (or even with regard to a specific data center), having the ability to create and manage logical groupings becomes critical.

How Does This Fit with NFV and SDN?

With a basic grasp of what server virtualization is from previous chapters and with the newly gained understanding of network virtualization, it's worth spending a few words on how they are related to network functions virtualization (NFV) and software-defined networking (SDN). To keep it in context, all four topics are summarized here.

Server Virtualization

Server virtualization is the abstraction of applications and operating systems from physical servers. This allows for the creation of VMs (app and OS pairs) that offer much greater usage efficiency on physical servers and afford enormous flexibility with regard to provisioning of applications.

Network Virtualization

Network Virtualization refers to the creation of logical groupings of endpoints on a network. In this case, the endpoints are abstracted from their physical locations so that VMs (and other assets) can look, behave, and be managed as if they are all on the same physical segment of the network. This is an older technology, but one that is critical in virtual environments where assets are created and moved around without much regard for the physical location. What is new here is the automation and management tools that have been purposely built for the scale and elasticity of virtualized data centers and clouds.

Network Functions Virtualization

NFV refers to the virtualization of Layer 4 through 7 services such as load balancing and firewalling. Basically, this is converting certain types of network appliances into VMs, which can then be quickly and easily deployed where they are needed. NFV came about because of the inefficiencies that were created by virtualization. This is a new concept; so far, only the benefits of virtualization have been covered, but virtualization causes a lot of problems, too. One of them was the routing of traffic to and from network appliances that typically were located at the edge of the data center network. With VMs springing up and being moved all over, the traffic flows became highly varied, which caused problems for fixed appliances that had to serve the traffic. NFV allows us to create a virtual instance of a function such as a firewall, which can be easily "spun up" and placed where it is needed, just as they would a VM. Much of this section focused on how this is done.

Software-Defined Networking

SDN refers to the ability to program the network. SDN is a newer technology, one that was born as a result of virtualization and the shift of where the "chokepoint" is in data communications. In short, the ability to set up or make changes to a network cannot keep up with the ability to provision applications with a click of a button. SDN makes the network programmable (which means network admins can quickly make adjustments to the network based on changing requirements). SDN is made possible by separating the control plane (the brains of the network) from the data plane (the muscle of the network). SDN is covered in depth in Part 5, "Software Defined Networks: Virtualizing the Network," and Part 6, "SDN Controllers," of this book.

All four of these technologies are designed to improve the mobility, agility, and flexibility of networks and data communication. However, virtualization, network virtualization, and network functions virtualization can all work on existing networks because they reside on servers and interact with "groomed" traffic sent to them. SDN, however, requires a new network topology and SDN-aware devices where the data and control planes are separate and programmable.

Virtualizing the Network

One of the reasons it's a good idea to make the change to network virtualization is that it allows network admins and users to fully realize many of the awesome features of server virtualization, such as vMotion, snapshot backups, and push button disaster recovery (to name just a few). Indeed, the most common reason for virtualizing the network is precisely to get VM mobility and vMotion to work.

In Chapter 9, "Multitenancy and the Problems of Communal Living," you were introduced to VXLAN, which is VLAN technology with some extensions that allow it to tunnel Layer 2 frames through the IP transport network, as well as extend the number of VLANs beyond 4096. The "tunnel" that this creates allows it to bridge virtual extensible VXLAN tunnel endpoint (VTEP) devices across a network, making data transfers easy and simple regardless of where the endpoints reside (or if they move).

As noted earlier, the VMs supporting applications or services require network connectivity via physical switching and routing to be able to connect to other VMs switching the data center or cloud and with clients of the data center over a WAN link or the Internet. In addition, in a data center environment, the network also requires security and load balancing. The first switch encountered by traffic leaving the VM is the virtual switch (hypervisor), and from there a physical switch that is either top of rack (TOR) or end of row (EOR). In other words, once traffic leaves the hypervisor, it is on the physical network, and unfortunately that network cannot easily keep up with the rapidly shifting state of the VMs that are connected to it.

The way around this issue is to create a logical network of VMs that spans the physical networks the traffic travels across. VXLAN (see Figure 10-2) does this just as most network virtualization does—through the use of encapsulation. Unlike simple VLANs, though, which are limited to 4096 of these logical networks on any given physical network, VXLAN can create about 16 million. That scale is important when it comes to large data centers and clouds.

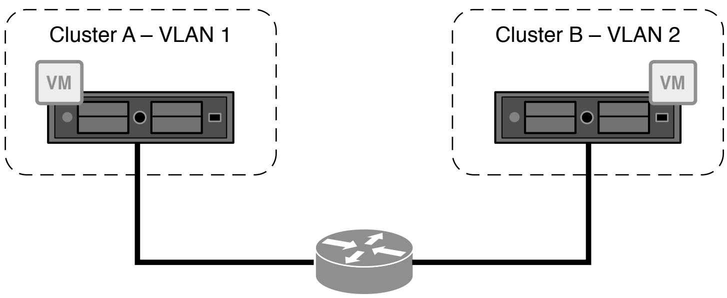


Figure 10-2 *VXLAN allows for millions of logical partitions across a physical network.*

Imagine that you have two VM clusters on a network, and imagine that a router separates those clusters because they are in different data centers. Both clusters in this case are on different VLANs. For these two VMs to talk to each other, the traffic between them must be routed. Now suppose you want these clusters to be on the same VLAN.

As shown in Figure 10-3, by using VXLAN, you can set up a VTEP that encapsulates or wraps the VM traffic on one end for transport over the routed network and then decapsulates (strips off the wrapper) on the other end. This effectively creates a logical network between the two clusters, which now appear to be on the same switched segment of a local network.

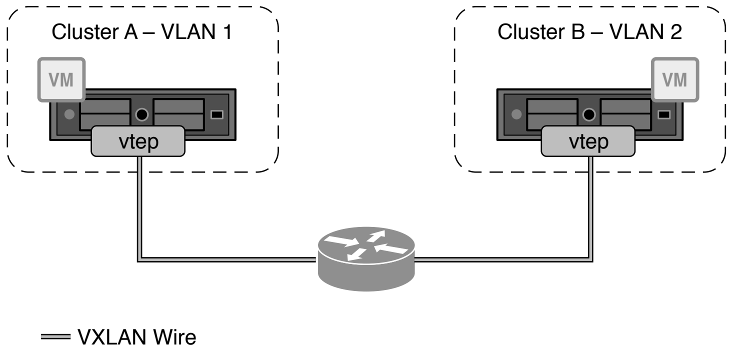


Figure 10-3 *VTEPs create a logical network between the two clusters, which then appear to be on the same switched segment of a local network.*

So, what's the big deal?

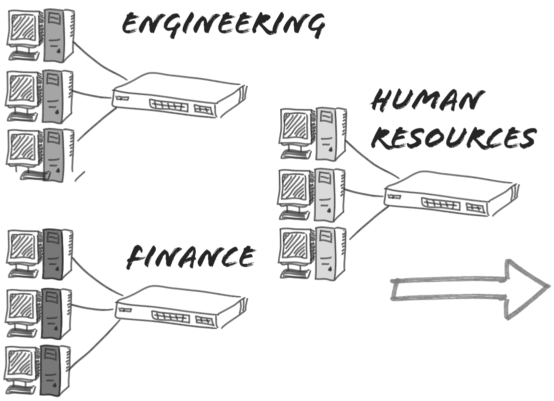
If you are new to networking, this might not seem like such a big breakthrough. If you are familiar with networking, though, you might be thinking, "This is just another way to create VLANs." There is more to it than that, though, because network virtualization in general, and VXLAN in particular, has some key benefits that become important at data center/cloud scale:

- First, this ability enables migration to a software-defined data center model. Using a vSphere administrator to provision VMs that can communicate with each other over different networks without having to involve the network team to configure the physical switches and routers eliminates one of the biggest chokepoints in the flexibility that data center virtualization affords us.
- This technology smashes through the previous limitation of 4096 VLANs
- VXLAN runs over standard switching hardware, and requires no need for software upgrades or special code versions on the switches. Therefore, you can virtualize your network using the stuff you already have.

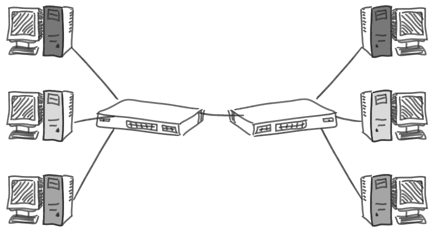
In summary, network virtualization, although an older technology, plays a key role in the creation of virtualized data centers and clouds. It is also one of the key drivers that allows and enhances both NFV and SDN, as you will see in later chapters.

How VLANs Work

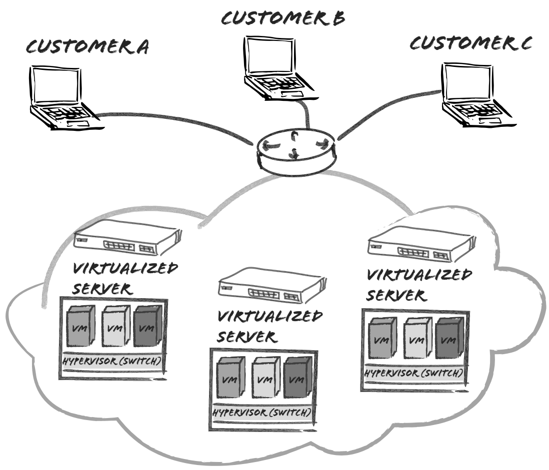
And Why They Matter in Cloud Networks



When networks were first rolled out, admins tried to keep like-users on the same switch. This local area network (LAN) model was desired, because the machines on any given LAN all received the same network instructions. It also nicely partitioned user traffic by providing physical segmentation.



As networks got bigger, it became impossible to keep like-users on a common switch. This led to the creation of the virtual LAN or VLAN. A VLAN is a means of logically grouping devices so that they appear to be connected to the same switch. VLANs provide logical partitioning and segmentation when it's not practical to physically segment.



In cloud environments, VLANs are essential because a user's VMs can span multiple servers. VLANs allow easy grouping of users resources into a single logical partition. Going further, the network admins can associate a VLAN with its IP subnet. A subnet is a way to partition a layer 3 (routing) domain. This makes it easy to connect to a cloud (and all your resources) over the Internet without needing to manually configure all of your connections.

Note that VLAN segmentation is often positioned as a form of security—VLANs do segment user data, but this is a very weak form of security that does not actually protect data.

INDEX

A

B

C

D

E

F

G

H

I-J

K

L

M

N

O

P

Q-R

S

T

U

V

W

X-Y-Z