LEARNING MADE EASY

VMware Special Edition

Evolution of Software-Defined Networking

for dummies®
A Wiley Brand

What SDN means for you now

Network upgrade with software speeds time to value

Improve Security, Cost, and Visibility

Jacob Rapp
Director, Technical Product Management, VMware

As businesses grow, whether organically or due to mergers and acquisitions, the traditional data center networks that support them become increasingly complex. This growing complexity creates operational inefficiencies and introduces security risks. Thus, it is no longer acceptable for businesses to build or upgrade networks after their applications are deployed. The data center network is a core part of application architecture and the status quo for network upgrades has already changed, driven by the needs of the applications rather than speeds and feeds. Strategic business projects like cloud automation, data center consolidation, new disaster recovery scenarios, and enhanced security initiatives require a modern data center network. Software-defined networking (SDN) allows infrastructure to become fundamentally more efficient with security built-in, creating a new model for managing complexity. In this guide, you'll learn how!

A (Brief) History Networking and the Rise of SDN

Fundamentally SDN evolved from the need for networks to become more agile and flexible. In the early 2000s data center networking began to evolve past simple spanning-tree topologies that created large failure domains, to proprietary and software managed fabrics of purpose-built data center hardware of today. During this same time virtualization technologies grew to become a major part of the data center leading to increased pressure on networks due to the volume of changes. The competing pressures of stability versus agility came to a head, leading to the need to make the network more like software. Since the first uses of the term, SDN has evolved to solve many different needs including: network virtualizaiton (abstracting the networks of the workloads (VMs, containers, cloud) from the underlying hardware); fabric management (making the physical fabric easier to operate), and automation (private and public cloud automation of networks, security, compute and storage like a cloud). With all the SDN options available now, it is time to think software-first.

How Network Virtualization Fits

Network virtualization makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane. Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and "attached" to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application. When a workload is moved to another host, its networking and security services move with it. And when new workloads are created to scale an application, the necessary policies are dynamically applied to those as well.

TIP

In 2011, the *Wall Street Journal* published Marc Andreesen's "Why Software Is Eating the World." In his essay, Andreesen explained that the future of business — from retailers, entertainment companies, and automobile manufacturers to financial services, healthcare, and education — is in software.

Just seven years later, a survey conducted by Dell Technologies and the Institute for the Future found the mantra that "every business is now a software business" has become a reality, with 82 percent of respondents planning to be a software-defined business within five years. It is now the network's turn to go software-first.

Software May Be Eating the World, but Hardware Is Still Serving It Up

Though many businesses are enjoying the benefits of server and storage virtualization in their data centers, they're still held back. Physical networking infrastructure will always be needed to move packets from point A to point B, but more application-level networking operations — such as defining policies that automatically follow dynamic ephemeral workloads — are performed more efficiently in software and the cloud, which has no hardware boundaries and extends transparently through private data centers and to end users. Specific challenges of hardware-centric data center architectures include the following:

- **Physical networks are limited by the nature of the hardware — it doesn't know the applications.** Although some network provisioning and configuration can be scripted — and certain SDN models promise to make this a reality — with hardware-based systems, there is no direct knowledge of the application. As a result, network provisioning remains a task that is done after applications are built and at best at the time of provisioning. Additionally, as the shift from workload (ports and protocols) automation shifts to application (processes and frame-works) automation, this problem will only get worse.
- Workload placement and mobility are limited. In today's fast-moving business environments, apps need 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 data center to another, or migration into and out of a multi-cloud environment. Additionally you can forget about implementing a hybrid cloud environment with hardware-based network infrastructure.
- **Hardware limitations and lock-ins breed complexity and rigidity.** The closed black-box approach to networking doesn't address the dynamic nature of today's applications, and it locks you in — and not just with the vendor. It locks you into the complexities of your legacy network architecture, limiting your IT team's ability to adapt and innovate, which in turn limits the business itself, making IT a bottleneck.

- **Traditional (bolted on) data center network security is inadequate.** Modern cyberattacks share a common modus operandi: Once inside he data center perimeter, cybercriminals move freely across the network from server to server (east–west traffic) installing malware and stealing sensitive data. Perimeter-based firewalls and zone-based security simply aren't enough. But in a physical network architecture with legacy networking systems, it's impractical to create dynamic segments with defined security controls and services for every workload (known as micro-segmentation), and put a fire-wall on every segment inside the data center to stop lateral attack movement and data exfiltration.

Taking a Software-First Approach to the Network

The first step in modernizing your data center network with a software-first approach is network virtualization. Starting with network virtualization establishes a base platform that is hard-ware-agnostic, enables data center migrations, and flows seamlessly from the network edge or branch, to the data center, and into the cloud. In much the same way that server virtualization emulates a physical server within soft-ware, network virtualization emulates the components of network and security services in software. In this way, the virtualized network is provisioned and managed independent of your hardware, and physical networking devices simply become vehicles to forward packets.

Some key benefits of network virtualization include the following:

- Realizing networking agility, while **managing complexity:** Network admin-istrators can provision and change virtual networks — logical switches, routers, firewalls, load balancers, virtual private networks (VPNs), and workload security — in software, reducing the risks and failure domains associated with rapid change of the physical network. It does this by bridging virtualization and networking operational tools and processes.

- **Achieving greater operational efficiency with automation:** Auto-mation in modern networks is not a goal; it's a necessity. Physical network infrastructure continues to evolve and networking hardware forms a web of highly reliable connections which, by itself, is a challenge to refine to a highly efficient operational model. Manual, error-prone network provisioning and management processes lead to costly business delays and potential security risks. Automation decoupled from hard-ware and moved closest to the appli-cation speeds deployment, reduces errors, and enables massive scalability.

- **Increasing agility, flexibility, and security with workload independence.** The ability to place and move workloads (and their associated services and controls) independent of physical topology enables greater business agility, deployment and operational flexibility, and improved network security within the data center. Security that is intrinsic to data center workloads grows automatically and evolves naturally, while being domain-agnostic — it is broad, deep, and highly extensible.


TIP

Many organizations are realizing the power of network virtualization to transform from hardware-based infrastructures to agile, software-based architectures. Using a software-first approach, they can deliver services faster, enhance security, keep applications up and running, and reduce CapEx and OpEx.

Key Considerations and Design Criteria in a Software-First, Modern Data Center Network

Whether you're deciding on the next generation of switches or which fabric management technology to use in your data center, thinking software-first fundamentally enables an enterprise cloud strategy. Modernizing your data center network is a perfect opportunity to envision a solution that starts with software and simplifies your upgrade path. Consider the following when designing your software-first, modern data center network:

- **Do the hardware and software services blend to form one cohesive management, control, and data plane layer?** If so, hardware device capacity and serviceability, together with its management software, will refresh in a codependent fashion. This codependency can lead to upgrades of some components being held hostage by other components, thereby negating the agility and flexibility benefits of a software-first approach. If, on the other hand, hardware and software services are disaggregated, then hardware and software life cycles are independent of each other and software capabilities and features can be continually updated with minimal impact on its hardware underlay.

TIP

Start with the desired end-state and identify how many control points of critical components (VMs, virtual switches, etc.) exist to map how future trouble-shooting would work.

- **Where does the division of labor lie between managing a hardware switch fabric and managing a virtualized stack for the application and its related service dependencies?** Defining this point will help provide the highest level of productivity. This is the ideal point at which management, application agility, and operational availability, can be attained. This point isn't always important for identifying where the virtual platform should be deployed, but it enables a view of operational efficiencies gained across the stacks.

- **Are intersections between hardware and software well-defined?** Designing intersections is nothing new for software. Interactions through application programming interfaces (APIs) are well defined and used. Applications themselves disaggregate and interact through APIs. Now, this same level of disaggregation is happening for software running the data center infrastructure, but in a slightly nuanced way. Platforms don't just expose APIs; they also develop interfaces or plugins. Take, for example, the network interface for containers. This interface maps a complete flow along with a set of APIs to support a level of integration and service. If well defined, these interfaces create the building blocks of the software-defined data center (SDDC).

- **What is the changing mind-set necessary to accomplish the goals of a software-first, modern data center network?** Networking and security must attain the agility, speed, manageability, and portability characteristics of the cloud. Network teams must break the traditional hardware-centric solution treadmill to promote change. This doesn't mean adopting a virtualization-only solution, but instead adopting a solution that best addresses the business problems that exist today while creating a platform for future growth. This approach enables a new model for managing complexity, not only for future innovations, but for current networking operations. The networking and security mind-set must evolve.

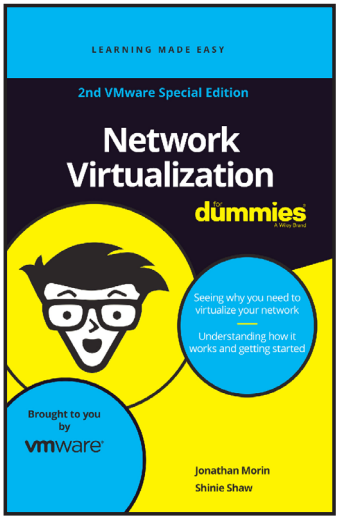
REMEMBER

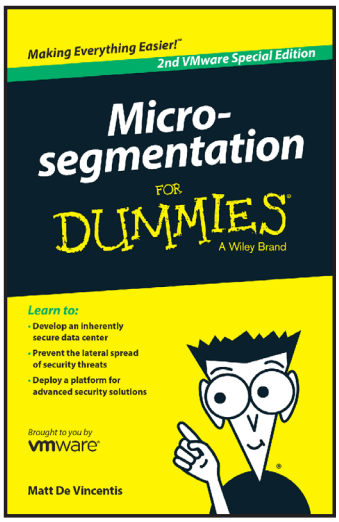
"Software-first" doesn't mean "software-only." All data center networks require a hardware fabric to move packets. Software services run the fabric and drive the deployment, management, and various operations of the applications.

TIP

Download the following guides from VMware learn more about SDN, network virtualization and micro-segmentation:

- Learn more about Software-Defined Networking
- Network Virtualization For Dummies e-book
- Micro-segmentation For Dummies e-book
- VMware NSX Data Center product page
- VMware NSX YouTube channel





For Dummies is a trademark of John Wiley & Sons, Inc. ISBN: 978-1-119-53542-3