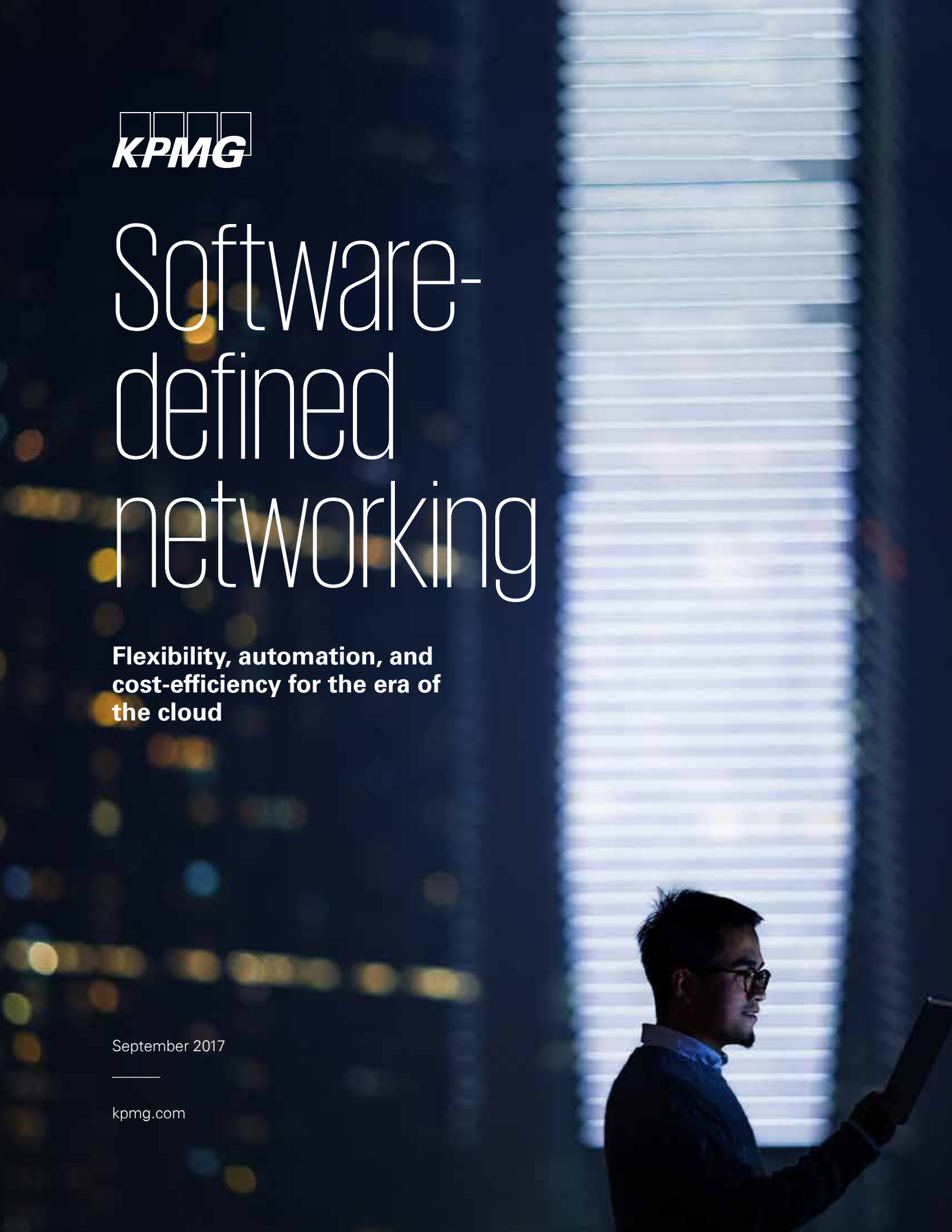


KPMG

Software-defined networking

Flexibility, automation, and cost-efficiency for the era of the cloud

September 2017

kpmg.com

Introduction

What software-defined networking (SDN) offers

Imagine if you had the ability to centrally manage and orchestrate all your organization's networking resources. You could quickly and automatically shift them as needed from one application to another. You could draw first on one piece of hardware, then another, then the cloud, then back to your hardware again, depending on what's most suitable and cost-efficient at a given moment.

With such a system, you could react quickly to applications' changing needs, to new business opportunities, or to security breaches. You could find efficiencies and automate many functions. And your network services would no longer be dependent on a particular piece of hardware—or a particular hardware vendor.

This system could cut your organization's networking costs, improve the user experience, allow you to use old hardware resources for new challenges, and align your networks with the speed and flexibility that cloud computing, digital labor, and mobile computing demand.

Such is the promise of software-defined networking (SDN). SDN is a new paradigm, and has begun to redefine both data centers and wide area networks.

This paper will outline the basics of how SDN works and offer guidance for organizations interested in reaping its benefits.

KPMG

Networking is facing new and growing demands

Enterprise network architectures that were built over the last two decades are relatively static. Most of this architecture is centered on campus and data center networks built with high performance, feature-rich Ethernet switches. This network architecture uses routers to connect with remote branches and external networks. Additional components such as application delivery controller, firewalls, WAN optimizers, and intrusion detection and protection systems enhance functionality and safety.

In these legacy network architectures, the control plane (the brain of the network) is integrated inside hardware with the data (or forwarding) plane that actually moves packets across the network.

This old setup has two major disadvantages:

— Systems in silos make it hard for an organization's networks to work together

— Dependence on hardware makes it time-consuming and costly to make changes.

As long as the demands made upon networks were relatively static and independent of each other, these limitations were acceptable. But, applications today are increasingly virtualized, dynamic, and hosted as a service in the cloud to support a highly mobile user community. Legacy networks aren't keeping pace with the emerging business and operational requirements.

The SDN solution: Flexible and centralized

SDN, by moving controls to specialized software, remedies these limitations with two important steps:

— Decoupling the local control plane from the data plane within individual network systems

— Positioning centralized control systems to configure and manage the individual networks.

The underlying network systems are still responsible for transferring data packets, but the SDN controller actively configures network capacity and characteristics to support data flows based on applications' changing needs. Application programmable interfaces (APIs) are the core of SDN, replacing the clunky command line interface (CLI) and the rigid simple management network protocol (SMNP) to manage and configure the routes by which packets pass with a universal GUI (graphical user interface) – driven management platform.

One can think of a traditional network as a hard-set system of highways, each with its predefined traffic flows, speed limits and local transportation authorities. With SDN, the data highway can quickly and automatically change the number of lanes in each route, the traffic that flows through them, and their speed limits and safety regulations. And SDN makes these changes to align with a central authority's vision of applications' needs.

In other words, with SDN, the network architecture itself is dynamic.

KPMG

Nuts and bolts: SDN standards

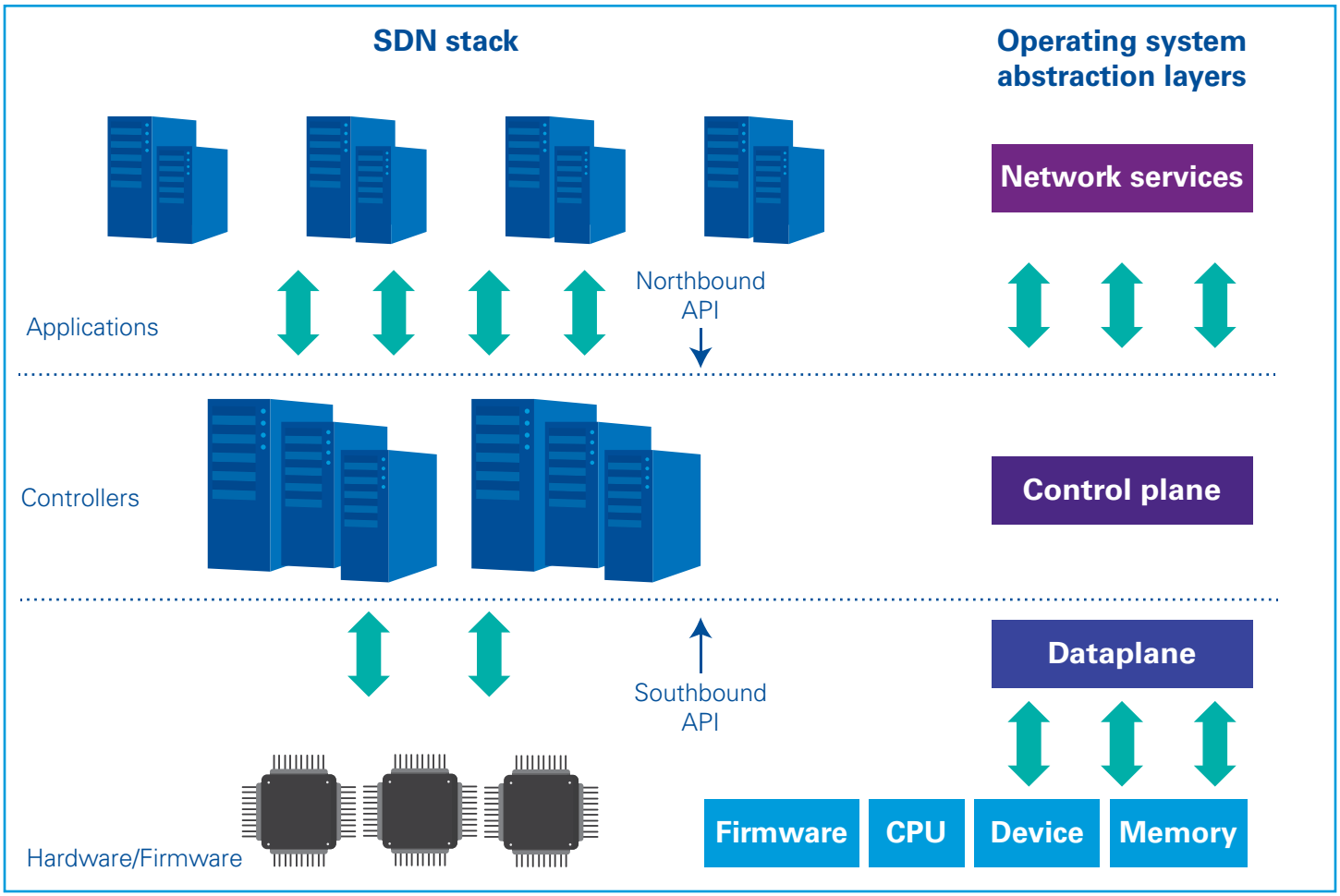
The leading body right now for SDN standards is the Open Networking Foundation (ONF), which promotes the OpenFlow protocol as a vendor-neutral standard for the south bound interface (SBI), which allows the controller to communicate with the network systems (hardware/firmware) below or south of it.

There's currently no dominant leader in the competition to establish a standard for the north bound interface (NBI) which permits the SDN controller to communicate with the applications above or north of it, though OpenDaylight is a strong contender.

Most network vendors, including Cisco, Juniper, Extreme Networks, Arista, and Hewlett-Packard, support OpenFlow. But many vendors have also deployed products with proprietary SDN protocols to add functionality and better integrate with existing operating systems, so different vendors may be more or less suited to a given organization's needs .

It's a positive sign for SDN's likely growth that so many network hardware vendors are moving to decouple the control plane from the data plane.

Figure 1 – fundamental SDN architecture



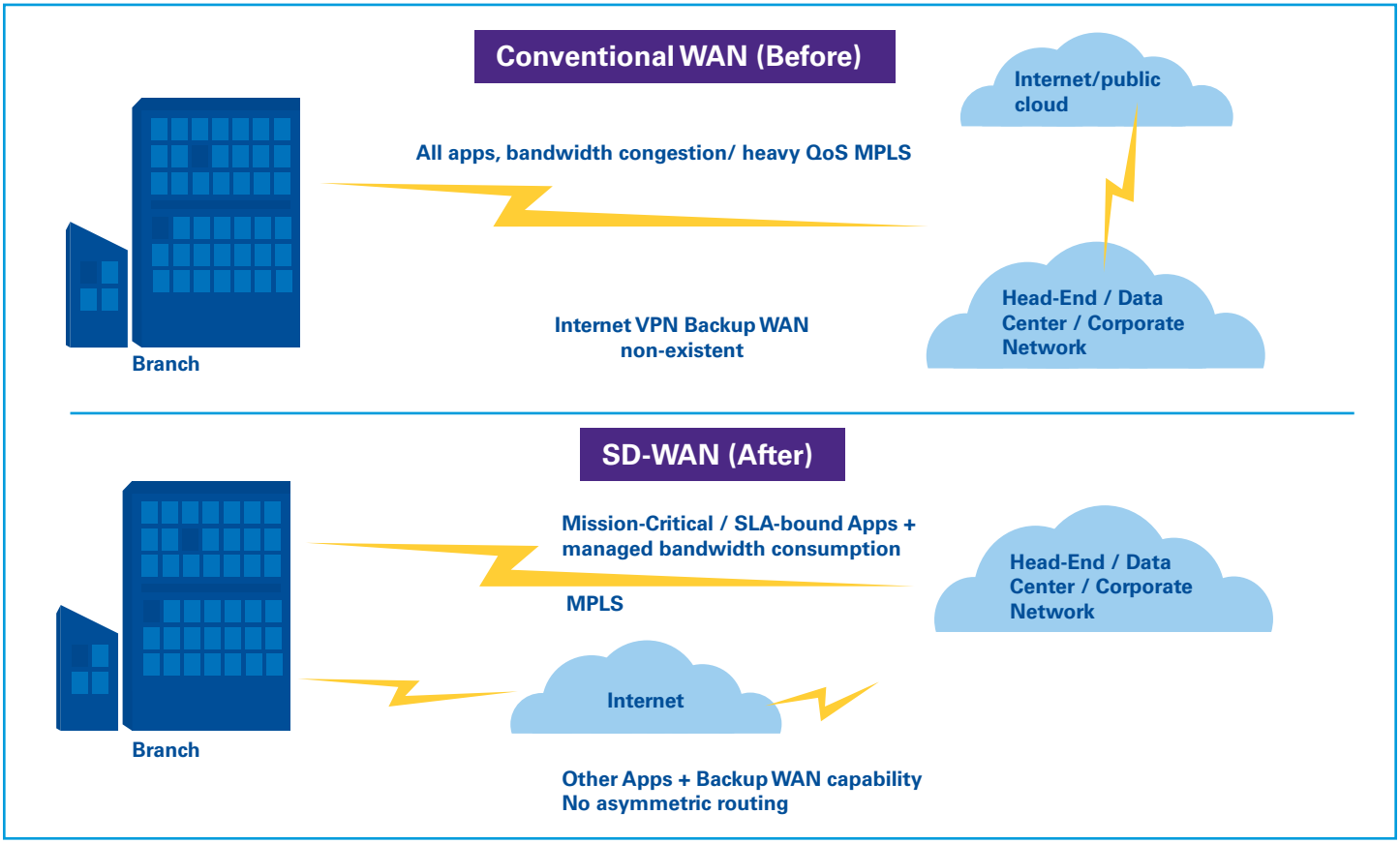
Software-defined wide area network (SD-WAN)

Traditional, router-based WAN solutions are complex, labor intensive, and difficult to customize. A SD-WAN applies the SDN concept to WANs, using a central controller to set policies and direct application traffic flows to meet changing requirements for performance, quality, or cost. A SD-WAN is application and WAN fabric aware and WAN transport agnostic. In other words, it considers the status and characteristics of all available WAN circuits/paths when directing traffic flows (see figure 2).

Through the controller, the administrator dynamically directs flows across the WAN fabric to meet applications' needs. Performance data feeding data analytics within the controller enable the administrator to rapidly address service issues (such as outages) and manage capacity and demand to prevent congestion.

In a SD-WAN, forwarders—which are largely virtual and can send data along multiple routes—replace routers. Programmed by the controller through APIs, SD-WAN forwarders identify individual flows and forward traffic onto different routes in line with the controllers' policies. They also manage quality of service, policy routing and redundancy, and WAN security including firewalls and encryption. They can run on commodity x86 hardware, and for added security, traffic between them is encrypted by default.

Diagram 2 – SD-WAN Fundamentals

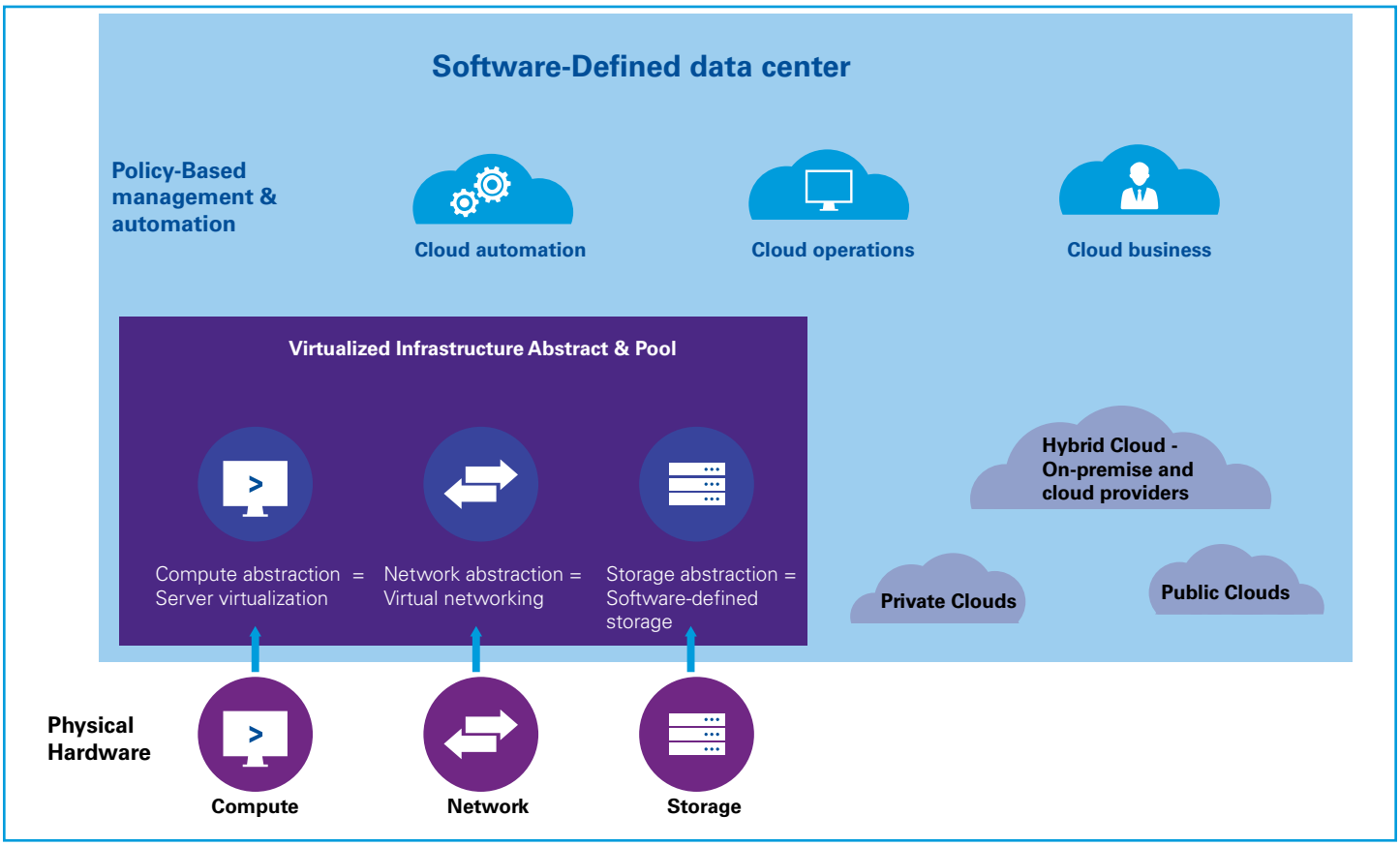


Software-defined data centers (SDDC)

A software-defined data center (SDDC) applies SDN concepts to all data center resources, including servers, storage, network functions, and security, with APIs on all resources, which have to be virtualized (see figure 3). Virtualized server and storage solutions have been on the market for many years, but only recently have network vendors started to offer virtualized versions of their products, called Network Function Virtualization (NFV) solutions.

A SDDC permits most components of IT to be offered as a service (ITaaS), where the resources can reside on-premise or in the cloud. That greatly increases the options for flexibility and cost efficiency while making time to market faster.

Diagram 3 – An SDDC Overview



Why organizations should consider SDN

SDN is transforming network architecture and operations. One recent forecast estimates a $70 billion annual market for SDN by 2024. Another is even more optimistic: $133 billion a year by 2022. Whatever the exact number is, SDN is simply too powerful not to grow quickly.

Here are just some of the benefits that SDN's combination of centralized control and flexibility offers:

- Automated responses to application needs (e.g., low latency, high bandwidth)
- Automated path selection based upon path attributes such as bandwidth, quality of service, or cost
- Automated service provisioning based on application requirements
- Application-aware performance monitoring of the network
- Integrated and fast application provisioning—minutes instead of days or weeks
- No more bottlenecks from local data centers, as the centralized controller can seamlessly tap the whole organization's resources or the cloud
- Rapid innovation from an open ecosystem of competing software vendors
- Less vendor lock-in as software has lower barriers to market entry than hardware and since virtual systems rarely depend on a single vendor
- Commoditization of high-cost hardware as control-plane functionality becomes largely independent of data switches
- Less complexity as a centralized control plane eliminates the need for distributed configuration, management, and monitoring
- Greater reliability due to increased automation and redundancy
- Stronger security through micro network segmentation and automated response capabilities
- DevOps and other new development methodologies facilitated by greater automation and orchestration.

The overall result is network architecture that can quickly adopt to changing business demands, enhance performance and make it more predictable, increase network visibility, and lower costs. In particular, application deployment and provisioning that takes place in minutes rather than weeks or months can be a game changer for many organizations. Migrating from a manual configuration of servers, storage and networks to an orchestrated, automated system of computing, storage, networks, and network services really can accomplish that dramatic increase in speed.

Major network vendors are betting on SDN with acquisitions. To give just a few examples, Cradlepoint acquired Pertino at the end of 2015, Riverbed acquired Ocedo in 2016, and Cisco acquired Tetration in 2016 and Viptela in 2017. Expect acquisitions should continue, since SDN is still early in the product life cycle and consolidation is just beginning.

---

[1] https://globenewswire.com/news-release/2016/10/06/877486/0/en/SDN-Market-Size-Projected-To-Reach-70-41-Billion-By-2024-Grand-View-Research-Inc.html

[2] http://www.prnewswire.com/news-releases/software-defined-networking-sdn-market-is-expected-to-reach-1329-billion-by-2022-584680731.html

KPMG

Getting started

The advantages of SDN are such that most organizations will likely adopt it sooner or later. But how to make the transition at a reasonable cost, in an acceptable timeframe, and without disrupting on going operations? The following steps are a good start:

— Prepare for a new IT culture. SDN requires IT staff in currently distinct units (servers, virtualization, storage, security, and networking) to work together as a team and to integrate SDN into the greater IT environment, especially with the rise of hyper-converged environments.

— Include all IT teams from the start. To help create this new culture and get buy-in, your initial SDN team that will work to define requirements, evaluate products, create trainings, and design a pilot program should include at least one representative from every IT unit.

— Teach (or hire) new skills. Network engineers' focus will no longer be manually configured switches, routers, firewalls, and other network equipment. They'll need new skills including:

  – Programming the controllers and integrating them with tools to manage and orchestrate the network, likely with programming languages such as Python, JSON, and Ruby;

  – Making templates for applications that define all attributes, including hardware requirements, in order to orchestrate the provision of applications

  – Understanding applications flows and the layers of security that each application requires in order to align with SDN's application-centric focus.

— Make new operational plans. Your different teams will have to develop plans to change ongoing operations to support the new, integrated environment's new operational requirements.

— Change your equipment life cycle program. Acquire only SDN-capable equipment. Even if you have to change your hardware vendor to facilitate SDN implementation, SDN overlay technologies will still reduce costs over time.

— Invest in the right test lab. You'll need the right equipment and skills to test SDN, SD-WAN, and SDDC capabilities and features before producing and implementing each new element.

Conclusion

The future of networking

Networking's job is to be fast, flexible, reliable, and secure—while keeping costs down. As opportunities for both enterprise efficiency and market growth intensify in cloud technology, big data, and mobile computing, networking has to do more with less and do it more quickly.

Hardware-centric networks are usually too rigid and resource-inefficient to meet these new challenges. Software-defined networks, with their ability to rapidly and automatically reallocate resources depending on your organization's changing needs and opportunities, are a better solution.

IT departments, with security, applications, virtualization, storage, and networking teams operating in silos, may resist the transition to SDN, which requires new skills and a new culture. But if the transformation is done right—starting with the action steps above, leading to a few use cases to create early successes and momentum—then the gains in costs, speed, and efficiency can help make your whole organization more competitive.

The future of networking is here. The only question is, is your IT department part of that future or being left behind?

KPMG

Case study

Improved performance and $25 million in savings

The challenge
A healthcare organization had grown rapidly through acquisitions. Using routers and a "daisy chain"—each location plugged into the next until the last link in the chain reached the data center—the wide-area network (WAN) was overloaded and vulnerable. Outages in small clinics created cascades of problems that paralyzed hospital networks, halting access to patient and medication data. The IT department was on nonstop "firefighting mode," rushing teams to bring networks back online.

The old way
The organization was considering buying enough new hardware to establish direct connections (through multiprotocol label switching, or MPLS) between each unit and data center. Since the organization had over 800 branches, many in remote locations, this solution would cost over $30 million a year.

The SDN solution
KPMG's CIO Advisory practice presented a cost analysis for moving to software-defined WAN (SD-WAN), a migration plan, and a selection of vendors to implement it. The plan's steps included:

— Enabling data centers and cloud platforms

— Identifying and prioritizing critical assets

— Low-risk pilots to build organizational expertise and comfort

— Maximizing the use of existing hardware

— Internet connections to reduce costs where feasible

— Overlays of new and old networks to ensure reliability during testing.

The results
The organization today rarely suffers outages, as a mix of Internet connections for routine data and direct connections for critical data ensures reliability and redundancy. When a local outage occurs, SDN automatically deploys alternate networks and the end user's experience is seamless. SDN also adjusts which data flows through which networks to meet overall organizational needs.

The cost for this upgrade? $5 million a year, instead of the $30 million that a traditional WAN would have cost.

Need help with software-defined networking?

KPMG's CIO Advisory team consists of network specialists with deep knowledge of wired and wireless solutions, network service providers, and network security. We have experience across the globe in assessing whether or not SDN is the right solution and in designing and implementing software-defined WANs and data centers. As independent advisors, we offer vendor- and technology-neutral advice.

Learn more

KPMG recognizes that today's CIOs face increasingly complex demands and challenges in becoming the strategic technology partner their businesses require.

KPMG's CIO Advisory practice helps CIOs, technology leaders and business executives harness technology disruption, more effectively manage technology resources to drive agile and improved business performance, enhance strategic position, and improve the strategic value of their technology investments.

If your IT organization is seeking ways to leverage technology as a source of innovation and competitive growth, KPMG member firms can help. For more information on CIO Advisory's service and capabilities, please visit www.kpmg.com/us/CIOagenda and www.kpmg.com/us/IT.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

Contact us

Fredrik Lindstrom
Manager, Advisory
CIO Advisory
T: 214-840-4447
E: fredriklindstrom@kpmg.com

Timothy Lake
Lead Specialist, Advisory
CIO Advisory
T: 908-347-3299
E: tmlake@kpmg.com

Timothy Williams
Managing Director, Advisory
CIO Advisory
T: 720-573-7071
E: timothywilliams@kpmg.com