# Is Your Business Ready for the Next Big Thing?

The technology industry tends to operate on micro and mega innovation cycles. Micro cycles happen every hour, day, week, and year. But mega cycles are far less frequent—about every 20 years. During these upheavals, there is a massive and fundamental disruption that changes not just the technology industry, but every other business and industry thanks to the far-reaching ripple effect. The upshot: Life on planet Earth gets impacted profoundly in terms of how we work, live, and play.

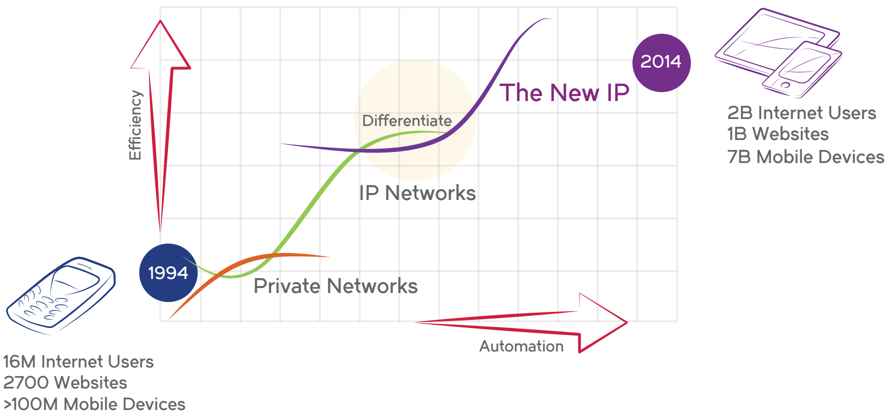
## We are now entering the next mega cycle.

To provide context for the coming technology shakeup, a brief tour of history is in order. From the mid-1970s to the mid-1990s, the mainframe terminal and host model provided the platform for business innovation. IDC refers to this as the "First Platform" for innovation. The defining network for this era was "Systems Network Architecture" (SNA), and it was based on circuit-switched private lines with a limited requirement for the deployment of cybersecurity.

Twenty years later, in the mid-1990s, the next mega-cycle began. The platform for innovation during this era was the client-server model, and the network was LAN/WAN, where we addressed point security challenges with individual security appliances as a reaction to emerging trends in data and user privacy. IDC refers to this as the "Second Platform." During this period, the shift to IP networks began in earnest, and the largest and most famous of these shifts was, and still is, the Internet.

## The New IP

**Enabling the next generation of business**



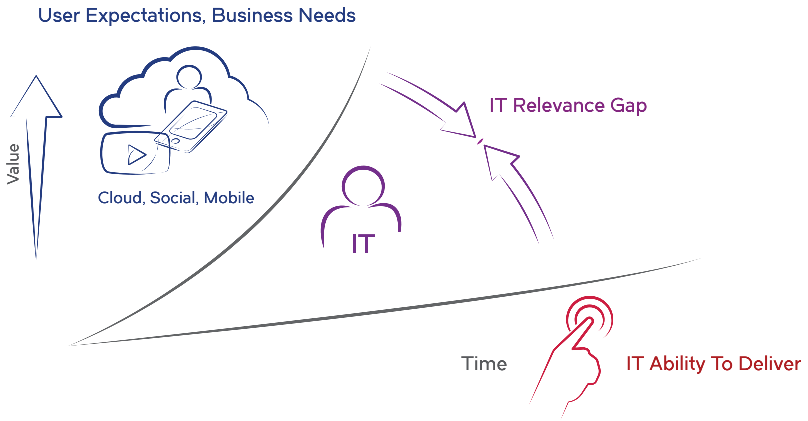
16M Internet Users
2700 Websites
>100M Mobile Devices

2B Internet Users
1B Websites
7B Mobile Devices

At the start of 1995, when IP networking technology was being deployed, there were 16 million users on the Internet, 2700 Web sites, and the concept of e-commerce had yet to emerge. Mobility, likewise, was nascent with fewer than 100 million mobile subscribers globally. Back then, you couldn't connect your mobile device to the Internet—smart phones weren't even around yet—and most Internet connections were via dial-up from a desktop computer.

# Close the IT Relevance Gap

**Transform your IT department into a trusted provider of services**



Over the next 20 years, the Internet would become so popular that it would give life to a brand new culture—the online culture. It would also change, and to some degree transform, almost every industry it touched. In fact, by 2014, mobile devices had increased 70 times to 7 billion. Today, there are 2 billion Internet users and 1 billion Web sites. And every year the volume of data grows by more than 50 percent with security fast becoming, if not already, a top concern for CIOs.

Clearly, we are entering the era of the "Third Platform," which also has distinct hallmarks in term of innovation: Cloud, mobile, social, and Big Data are all a part of it. Gartner calls these elements the "Nexus of Forces" and advocates the need to become a digital business in order to survive this next wave of disruption.

On the plus side, the Third Platform is expanding the options and flexibility for businesses by a wide margin. On the downside, IT has never been more challenged, as it now falls to these organizations to figure out how to manage this nonstop deluge of global data while addressing breaches of security in real time, if not before they happen. Adding to the challenge, many organizations still use IP networks that were built for a Second Platform world—which was a reality 20 years ago, but is woefully out of step for the IT needs of today.

These pressures will only continue to mount, along with a groundswell of opportunities that the Third Platform is expected to create over the next 20 years. Over this period, Gartner predicts that every business, regardless of industry, will become a digital business (Source: "Digital Business: Implications for CPOs and Supply Management Leaders").

The implications of this shift to the underlying network infrastructure, and the teams that provide and support them, are profound.

## The Relevance Gap and the Old IP

In the last three years, cloud spending has increased to $65 billion worldwide. We've gone from connecting places and people to connecting things: Billions and, eventually trillions, of things. And all these things love to generate and consume data. The challenge is that all of the data takes a lot of work to manage and secure.

After all, you have to store it, move it, and analyze it—without compromising the security of the data and network—before it becomes truly valuable information. The speed of innovation of cloud service providers such as Amazon and Google, in combination with the low cost of delivery, is creating a relevancy gap for IT departments and traditional service providers. Every day, users go around these entities to buy IT services and applications directly from the cloud. User expectations for self-service, immediate delivery, and a faster pace of innovation are rising by the day because this is the experience they already have with consumer applications. But, for many companies, the IT department struggles to keep pace. The network architecture is outdated, because it was never designed to meet these needs, and 70 percent of the IT budget is used just to maintain the old infrastructure.

IT used to be the drivers of corporate innovation and value, and every IT department wants to meet the changing and growing needs of users. They want to deliver a platform for fast innovation on which to build a competitive digital business, just as the cloud providers do today. The same aspiration holds true for traditional service providers. Unfortunately, the reliance on legacy network architectures makes this difficult. Many even say that the old architecture is what is holding them back.

These legacy IP networks, referred to as "old IP," have served incredibly well for the last 20 years. The resiliency of these networks is a testimony to IP's elegance. And nobody is suggesting that we toss them out. But staying the course is not an option. A dramatic change is needed.

The good news is that an advanced but evolutionary networking architecture is here—the New IP.

## The New IP

What is the New IP? It's the old IP networks reimagined for a modern world and designed to meet the needs of cloud, mobile, social, and Big Data.

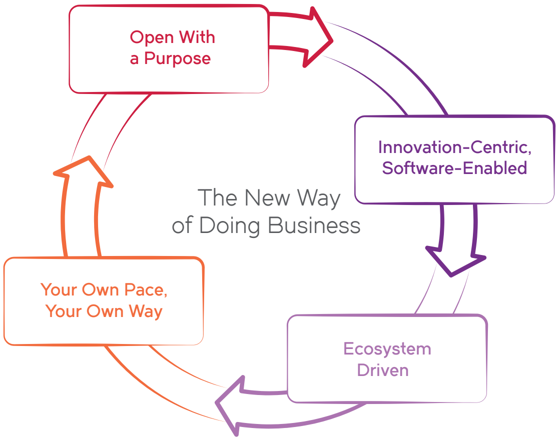
The New IP is a new way to architect networks that accelerate business changes and growth while maintaining or increasing high levels of security. The New IP emphasizes open, automated, software-defined elements to increase agility and reduce costs while meeting the challenges of the Third Platform.

It's good to compare where we are today to the promise of the New IP, and then describe the advantages and implications of this transformation.

The old IP is based on closed systems in which innovation cycles are constrained by custom hardware, while the provisioning of network resources is a complex and labor-intensive task. Interoperation is limited. Vendors are at the center of the ecosystem, costs are high, and innovation is slow.

In contrast, the New IP is based on open source and open standards that extend beyond proprietary adherence to industry standards. The New IP gives IT the choice of using Commodity Off-The-Shelf (COTS)-based or workload-specific hardware. Provisioning network resources is automated and can be done in a self-service model. Open APIs are the key to interoperability. The customer is at the center of the ecosystem, CapEx and OpEx costs are reduced, and innovation happens at the speed of business.

## The New IP is Transforming IT


Open With a Purpose
Innovation-Centric, Software-Enabled
Ecosystem Driven
Your Own Pace, Your Own Way
The New Way of Doing Business

There are four essential attributes to the New IP.

### Open with a purpose

- The New IP is more than just open—it's open with a purpose.
- Openness accelerates the rate of innovation, reduces vendor lock-in, and reduces both cost and complexity.
- Because no one can predict where this innovation cycle will go, the New IP allows components and services to be assembled from a broad community of innovators in order to solve challenges in new ways.
- Open solutions address security issues faster because there's information exchange and collaboration between security elements (physical or virtual), providing a more holistic view and key learnings from all sources.
- The New IP lets you combine vendors using open APIs and adjust your strategy and rate of innovation by giving you the freedom to choose and the flexibility to change quickly.

### Innovation-centric and software-enabled

- The New IP is innovation-centric and software-enabled to improve time-to-value and the overall customer experience.
- Today's industries demand innovation to power their growth. The New IP provides a platform for fast innovation.
- Software allows programmatic control over complex tasks, freeing IT to focus on strategic challenges to enable business growth and fast pivots as strategies and offerings shift with market forces.
- With the New IP, security is designed in, not bolted on, allowing you to abstract security from the underlying network infrastructure. As a result, the network can be pervasively vigilant, ensuring security of both data-at-rest and data-in-flight.

### Ecosystem-driven (with users at the center)

- The New IP is ecosystem-driven, enabling a pool of resources that accelerate innovation.
- The New IP goes beyond single-vendor limitations to allow businesses to keep pace with innovation by tapping into and building upon a vast pool of resources.
- With the New IP, innovations and solutions can come from anywhere. Every element has a vested interest in contributing to the community and being part of solving the security challenges. The ecosystem-centric approach of the New IP makes this possible in a way the vendor-centric model of the last 20 years does not.

### On your terms

- Taking evolutionary steps with the New IP, you can start transforming your infrastructure, your IT organization, and your business to achieve revolutionary results.
- On the security front, you can have better control over your security posture because you're not relying on primarily identity- and static-based solutions. New IP networks can take into consideration behavior rather than just identity when applying security policies. The security system is also continually learning and self-optimizing so that it can proactively mitigate threats rather than just respond to attacks.
- With the New IP, enterprise organizations can start deploying applications as much as 90 percent faster and cut operational expenses as much as 50 percent by evolving a data center network to an SDN-ready Ethernet fabric. CapEx can be reduced and agility improved by replacing hardware-based appliances with virtualized network functions that run on commodity servers, or that are provided directly from the cloud as an edge service.
- You don't have to take a rip-and-replace approach with the New IP. You can think big and start small, while you move rapidly toward a more agile network architecture.

New IP networks have some surprising implications:

### The data center is everywhere… and anywhere.

- The New IP allows you to host and manage your workloads from any source (private cloud, public cloud, or hybrid cloud) based on business goals and corporate policies. This approach improves efficiency, scalability, and agility—and it makes the IT and network organization a better provider of services to its internal customers, vendors, and partners.

### You're able to move faster and be more efficient than your competition.

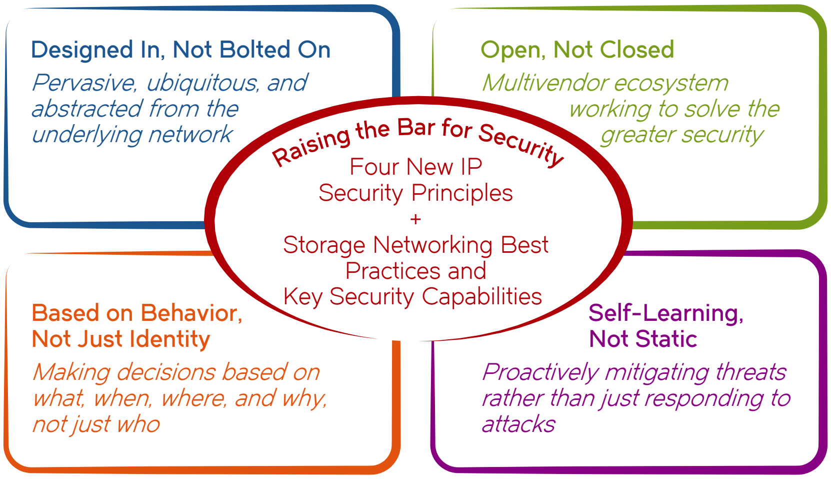
- Your business needs to move and innovate faster and run leaner than ever before. The New IP helps accelerate innovation, reduces operational overhead, and gives you the control you need to stay ahead of your competition.

### Your users are at the center of the New IP ecosystem.

Every one of your users and every one of their applications can have their own network with the services, quality, and security specific to their needs. And the network can modify itself based on the device and location. There is no network edge, in the traditional sense of that word, in the New IP. The edge happens where the user interfaces with the network, applications, and services. The result? The highest-quality, most cost-effective user experience possible.

In short, the New IP is a modern network, built on your terms.

## New IP Security Principles


Designed In, Not Bolted On
Pervasive, ubiquitous, and abstracted from the underlying network
Open, Not Closed
Multivendor ecosystem working to solve the greater security
Raising the Bar for Security
Four New IP Security Principles
+
Storage Networking Best Practices and Key Security Capabilities
Based on Behavior, Not Just Identity
Making decisions based on what, when, where, and why, not just who
Self-Learning, Not Static
Proactively mitigating threats rather than just responding to attacks

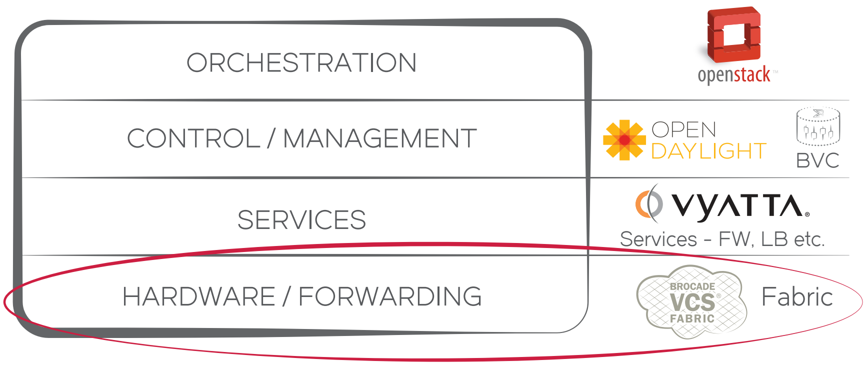
## Getting Started in the Data Center

The New IP allows you to take evolutionary steps to achieve revolutionary results. And to begin, many think they must start with Network Functions Virtualization (NFV) or Software-Defined Networking (SDN). While these are both foundational technologies for the New IP (described in more detail later), a good place to start is building a solid network foundation that allows you to leverage a more relevant step-by-step approach.

### Building a Foundation

The first step in building a strong foundation is defining what you want to build upon it and how fast you need to move. The Brocade® Network Maturity Model (5 Steps to the New IP) demonstrates the evolution from IT primarily being a cost center to IT being the center of innovation and a growth engine for business. It also represents the rapid acceleration toward integration and control of the virtualized network resources that underpin the predictive, self-learning nature of the later stages of the maturity model.

## The New IP Architecture



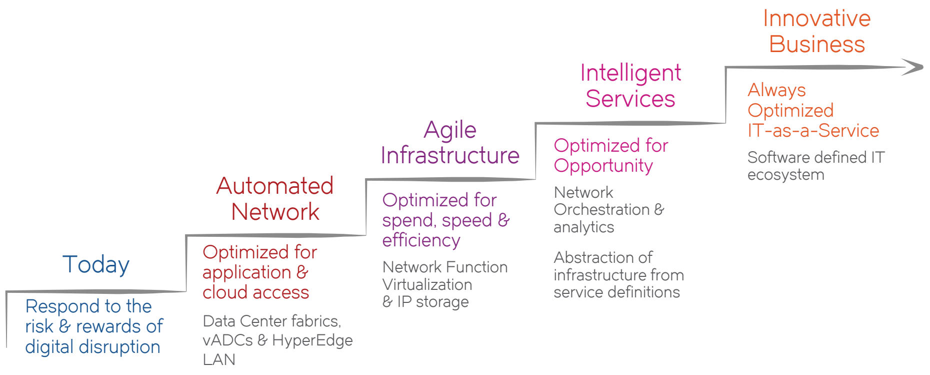
At the starting point, every New IP-ready network ultimately needs to move data and forward packets. The openness, data path efficiency, and automation of a fabric-based network will make any environment run better while also paving the way to new software-enabled innovations. A fabric-based architecture increases agility by reducing complexity and increasing automation. Fabrics easily scale up and out, adapting to handle instantaneous changes in traffic flows, flow sizes, packet sizes, and protocols. This simplified architecture inherently increases security by design.

This approach to foundational networking is inherently more secure by design. And if you've virtualized your compute environment, like just about everyone else, you need a fabric-based architecture that lets you get more out of that virtualized compute system. The underlying fabric is also Virtual Machine (VM)-aware. The awareness of the VMs, the number of virtualized services, the types of virtualized services, and the behavior of those VMs is important in securing those services.

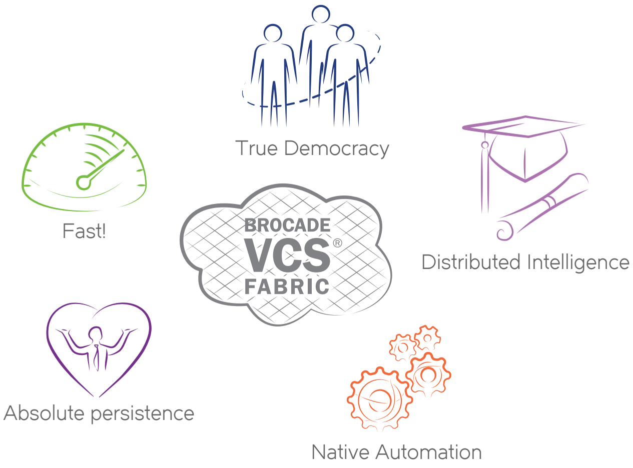
In fact, the right fabric-based architecture is essential and Ethernet fabrics are the most often-recommended architecture, specified by companies such as VMware, Cisco, and Brocade to name a few. In a virtualized environment, you need to track the VMs as you move them, monitor traffic between them, and troubleshoot everything through the virtual layer as well as the physical infrastructure

## Networking Maturity Model

5 Steps to The New IP


Today
Respond to the risk & rewards of digital disruption
Automated Network
Optimized for application & cloud access
Data Center fabrics, vADCs & HyperEdge LAN
Agile Infrastructure
Optimized for spend, speed & efficiency
Network Function Virtualization & IP storage
Intelligent Services
Optimized for Opportunity
Network Orchestration & analytics
Abstraction of infrastructure from service definitions
Innovative Business
Always Optimized IT-as-a-Service
Software defined IT ecosystem

## Brocade's transformational IP Fabric Architecture is based on five principles...



underpinning it. This is a difficult problem to solve with old IP networks, but it's much easier with New IP-ready, fabric-based network architecture. But the fabric alone is not enough. For virtualized compute infrastructures, the fabric needs to have deep integration with the virtualized compute layer. For VMware, this means integration with vRealize, vCenter, and NSX to provide deep insights and visibility end-to-end and top-to-bottom across the fabric-based architecture, with maximum performance enabling increased VM density and minimized downtime through high resiliency and streamlined troubleshooting.

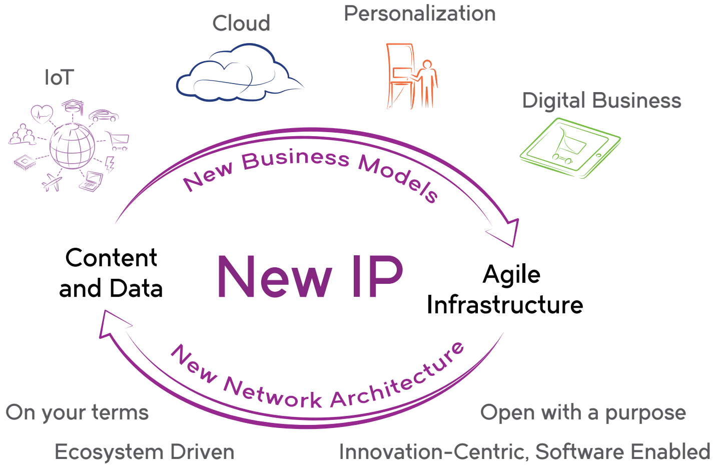
There are five must-have features with any fabric:

1. **True democracy:** This means every switch is equal to every other switch. The architecture is flat, without hierarchy, so that there is no single point of failure. The result forms a flat Layer 2 or 3 surface that is a self-forming and self-healing network. All paths are equal and available, and devices of different capacity and design can be mixed together. You can mix and match chassis and fixed configuration "pizza boxes".
2. **Distributed intelligence:** Every port is aware of every other port. This means you can move workloads with their associated characteristics—called Automatic Migration of Port Profiles (AMPP)—without the need for time-consuming, labor-intensive, and error-prone manual network reconfiguration. These characteristics include access control, Quality of Service (QoS), and other port-oriented application characteristics. A fabric should abstract this information and thus provide the ability to move workloads on your terms and timeframe. If a port is lost, the workload is moved to an available port automatically and seamlessly, to continue consistent delivery of services.
3. **Native automation:** Fabrics should be built from the ground up for automation, making them five to ten times faster to deploy than individual elements and providing a wide range of additional capabilities such as AMPP, zero-touch provisioning for VMs, and network self-configuration. Native automation delivers near-perfect load balancing throughout the mesh, at Layer 1. You don't need additional devices, additional programming, or manual configuration. Native automation is critical to getting New IP benefits from the network out of the box for scaling, availability, and performance without human intervention and lost time.

## The New IP Accelerates Service Delivery, Data Access, and Innovation

From

- Proprietary
- Hardware Devices
- Manual
- Silo'd Ops
- High Cost
- Slow Innovation



To

- Open
- Software-enabled
- Automated
- True Democracy
- Optimized Costs
- Fast Innovation

4. **Absolute persistence:** This means optimizing and maximizing the flow of traffic throughout the fabric. You can lose a port, or a whole switch, and the fabric will react in real time and balance itself. You get transparent interconnection of lots and lots of links.
5. **Speed:** This means no compromise between scale and latency. Fabrics take the most efficient path, automatically and continuously. Fabrics combine hardware performance with software programmability. Because a fabric by definition means there is more than one node, you can't be forced to compromise scale or latency if you add nodes. When you need to scale up quickly, that's what a fabric does really well.

The native automation, scale, and speed of fabrics reduces OpEx, increases performance and availability, and lays the foundation for SDN.

### Increasing Agility with NFV, VNF, and SDN

Virtual Network Functions (VNFs), or Network Functions Virtualization (NFV), replace hardware-based routers, firewalls, Application Delivery Controllers (ADCs), and other physical equipment with software versions that run on x86-based hardware. NFV reduces CapEx and OpEx while making it easier to spin up and down resources as needed.

With NFV, services become mobile. You can take all the network services a virtualized application needs, and put them right next to the VM on the same server. Network traffic between applications and NFV services does not need to leave the server, and as a result you reduce your north-south traffic and your costs dramatically. You can also increase security by providing a virtual firewall security layer attached right to each application, and that security moves with the application around the infrastructure.

Software-Defined Networking (SDN) provides the tools to manage and control the network services and infrastructure, whether it has been virtualized or not. OpenDaylight is an open source SDN initiative that allows you to visualize, control, and centrally manage resources. It also allows the network to see and dynamically respond to traffic flows in an automated fashion. Any service in the network that you've created, physically or virtually, can be controlled by one SDN controller in a fully programmable way.

### Service Orchestration

The network is only one important part of the infrastructure. You have compute and storage as well. And that's where orchestration comes into play. OpenStack, an open source protocol for the orchestration layer, can provide the same benefits of OpenDaylight at the network layer across compute, data, and network resources. In addition, because you are likely to have a multi-cloud environment (private and public) you have to make the clouds work together in a predictable, scalable, and manageable way. OpenStack orchestration provides that ability, allowing orchestration to stretch across the entire environment.

If you prefer to start small, focus on the fabric-based architecture and just make sure every network device you purchase is SDN-capable with support for OpenFlow. Even if you don't use the programmability of SDN today, it will be there for you in the future.

## What about the Network Edge?

The network edge isn't always a physical place anymore. Instead, it's a set of activities where users interface and interact with an application. The application lives in the cloud or in the data center. The users can be anywhere they want to be, and the edge moves with the user.

As a user interacts with data or an application, you need to apply the services and policies that control access and manage the user experience. The actions will vary based on who you are, what you are doing, when you did it, why you are doing it, where you are, the device you're using, and what rights you have. Based on those answers, you can apply Role-Based Access Control (RBAC) policies that are expressed through network services such as routing, firewall, QoS, and so forth.

With the New IP, you can virtualize just about any network service, so this wrapper of policy can be anyplace. This is where virtual edge software and services fit into the picture, often called virtual Consumer Edge (vCE) in Communication Service Provider language, or virtual Customer Premise Equipment (vCPE). For example, consider replacing your stack of equipment, such as physical routers, firewalls, and/or load balancers, at remote offices with a suite of software instances running on existing servers at any site and manage it remotely.

One immediate benefit of this architecture can be path optimization right at the branch location using a virtualized application delivery controller, dramatically reducing monthly MPLS/Ethernet backhaul costs to the data center. This savings alone can more than pay for the server and virtualized network services at each site. After you have the New IP edge in place, it becomes a platform for self-service delivery to further reduce costs as well as a platform for new service innovation.

The point is, there are many ways to get started on your journey to the New IP, including data center fabrics, NFV, SDN, orchestration, evolving security mechanisms, and the new edge. Each can deliver strong business value today, alone or in combination.

## Why Brocade?

Brocade was founded in 1995, which coincides with the start of the last big compute transition. Unlike other networking companies, Brocade started with a focus on the data center with an understanding of how to control packets and move data as efficiently as possible.

Today, Brocade is a $2.3 billion company with the highest market share in the SAN switching market and the #2 overall company in the data center. Brocade is a clear leader in these areas because no vendor is better in helping companies connect heterogeneous data storage environments and move their data among these different devices and protocols. EMC, HP, IBM, Dell, HDS, and others sell Brocade products and technologies as part of their data center storage portfolios—a key reflection that partnering is at the core of Brocade. And partnering is a mandatory requirement for building an open security ecosystem and enabling a higher security posture today.

In fact, nearly every Fortune 500 company and major organization in the world relies on Brocade technology in the data center. We support their businesses, with a focus on the applications that require the highest levels of performance, availability, and security in mission-critical environments.

Brocade understands that the market pressures on you and your teams are mounting. Cloud, mobile applications, the drive to be a digital business, and security concerns have strained old IP networks. These same factors are also constraining business innovation, forcing companies to rethink their infrastructure strategies.

Simply put, Brocade is better positioned than any other networking vendor to lead the way to the New IP. Why? Because our business isn't based on the old IP. We made an early investment on open technologies and software networking, and we are focused on leading this market transition.

The Brocade strategy is built around the New IP, with hardware and software that is designed to take full advantage of the trend towards secure, open, virtualized IT infrastructure.

The Brocade virtual services platform includes a virtual router, stateful firewall, VPN, and NAT in a single software suite. Brocade also offers application delivery controllers and load balancing for virtual and cloud services, including scalable Layer 7 application security and performance tools, and the industry's first multivendor OpenDaylight SDN controller. You can download them for free from www.brocade.com to start gaining experience and immediate value. You won't be alone: More than 1.5 million virtual routers have been downloaded so far, with an estimated 100 million hours of production time. It is the most widely used and deployed virtual routing software suite in the world.

Brocade has the only vRouter and network software suite built from the ground up to run on the Intel chip, and not just ported to it after original design. This is why it has the industry's best performance, independently verified to perform at 80 Gbps line rate on a single server using three Intel cores. This level of performance can also be used to power dozens of individual network services within the same server, allowing you to run your east-west traffic between applications and network services within the same server. This also significantly reduces the hardware and network costs of the north-south traffic that is left to transport outside the server. It's a huge and immediate savings to the bottom line, providing the agility of a software-enabled network architecture that you can provision and manage from anywhere.

The Brocade Virtual Application Delivery Controller (vADC) solution is also designed for NFV deployment, with a complete set of application security and performance tools to make applications more efficient and reliable. With fine-grained control over users and services through open APIs, this solution can automate the deployment, licensing, and metering of application delivery services in high-density, multitenant environments

Brocade also offers the industry's only OpenDaylight controller that can manage multivendor equipment using open APIs as the northbound interface to ensure your orchestration layer can translate business policy into machine language. The Brocade SDN Controller plays an integral role in the security principles of the New IP, which focus on security being open and designed in from the start, based on user behavior and complete with self-learning capabilities.

In addition, Brocade VDX® data center switches, Brocade ICX® campus switches, and Brocade MLXe core routers are all OpenFlow-enabled and support the

Brocade SDN Controller. Brocade has uniquely delivered OpenFlow in a practical approach using a true hybrid port mode on the Brocade MLX and ICX devices, where traditional Layer 2/3 and OpenFlow forwarding can work on the same port, at line rate. This unique capability provides a pragmatic path to SDN by enabling you to non-disruptively integrate OpenFlow into existing networks, giving you the programmatic control offered by SDN for specific flows while the remaining traffic is forwarded as before—with no physical change to the infrastructure. No separate network is required for SDN. SDN-enabled networks support application-aware dynamic resource allocation use cases, and can dynamically allocate network resources in real time to meet the needs of applications. SDN applications can use input from many sources, including application-specific security and QoS requirements, network statistics, user activity, and security threat analysis, to allocate and protect network resources, set access control rules, and dynamically prioritize traffic in real time.

For example, the Brocade Flow Optimizer application allows you to gain insight into network traffic, enabling policy-based detection and management of large Layer 2 through 4 traffic flows. This SDN-based application addresses real-life network performance challenges, which is critical to enabling cloud services. The application enables proactive network visibility and control while providing new levels of programmability and network automation. With this network intelligence, you can increase network efficiency through better network capacity planning and resource utilization, mitigate network attacks, and eliminate network congestion through policy-based traffic engineering—thus improving the overall customer experience.

Among many things, the Brocade VDX family includes a new high-density 40 Gigabit Ethernet (GbE) switch that will soon scale to 100 GbE in a 1U configuration. It can translate to and from VXLan protocols using an NSX Gateway solution, allowing you to integrate your installed environments and connect them to your controller. (This is called VTEP, and Brocade does it better than any other technology provider.)

In addition, Brocade has the leading fabric in the industry based on Brocade VCS® Fabric technology running on Brocade VDX switches. This software is in its fifth generation, with rich support for SDN and virtualized environments at both Layer 2 and 3.

The Brocade MLXe core router not only provides high-performance routing and forwarding for intra-data center applications, but it forms the foundation for critical IP/MPLS inter-data center connectivity solutions. Its programmable network processors are ideal for many types of software analytics applications for network traffic. In addition, the Brocade MLXe provides the industry's highest security (military-grade AES 256 Suite B encryption) without any performance impact for data privacy encryption for inter-data center and WAN links.

All of the promises of SDN and the associated agility require a network that just works. It has to be reliable, it has to be available, it has to be secure, and it must support new requirements without wholesale changes to the infrastructure. That's why fabrics are the recommended choice of so many analysts and vendors.

If you're running VMware, no fabric networking vendor has done more to integrate its products and management into VMware's tools and environment than Brocade. This includes integration with vRealize, vCenter, and NSX. Brocade fabrics make VMware environments run better and give you the resiliency, efficiency, and simplicity unavailable in an old IP environment—ensuring that you extract maximum value from your VMware investment.

You don't have time to hand-craft your network anymore. It's more important now than ever to have an automated network that self-forms, self-heals, is managed centrally, and works well with all the major components of your VMware deployment.

For example, you can provision a VM in vCenter, and Brocade VCS fabrics automatically configure the port profiles across the entire fabric. You can move a VM, and VCS fabrics automatically update the appropriate ports. You can deploy NSX, and the Brocade VCS Gateway delivers the scale and traffic visibility for fast troubleshooting. Simply put, dynamic virtual networks need dynamic physical networks. Brocade VCS fabrics are agile, automated, and cost-efficient.

When you purchase Brocade products, you have the option of Brocade Network Subscription, which allows you to pay for networking based on your actual use, without a term commitment. You also have the ability to upgrade at any time. For most organizations, the monthly OpEx savings on existing maintenance contracts for old data center or campus IP networks will get you a brand new network—one that provides the familiarity of the old IP but with the clear benefits of the New IP.

Only Brocade is conflict-free in its commitment to the New IP. Brocade has the leading virtual routing platform, the most effective OpenDaylight controller, and the industry's leading fabric—all of which help you evolve to the New IP, on your timetable and on your own terms.

The only question is, "What are you waiting for?"

## Think Big. Start Now.<br>Welcome to the New IP.

For more information, visit www.brocade.com/newip.

**Corporate Headquarters**
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

**European Headquarters**
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

**Asia Pacific Headquarters**
Singapore
T: +65-6538-4700
apac-info@brocade.com

© 2015 Brocade Communications Systems, Inc. All Rights Reserved. 11/15 GA-WP-1950-06

ADX, Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, The Effortless Network, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision and vADX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment features, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This information document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.