Executive's guide to software-defined networking

TechRepublic Pro

ZDNet

Executive's guide to software-defined networking

Published by TechRepublic
June 2013

Disclaimer

The information contained herein has been obtained from sources believe to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TechRepublic
1630 Lyndon Farm Court
Suite 200
Louisville, KY 40223
Online Customer Support:
http://techrepublic.custhelp.com/

Credits

Editor In Chief
Jason Hiner

Head Technology Editor
Bill Detwiler

Head Blogs Editor
Toni Bowers

Senior Editors
Mark Kaelin
Jody Gilbert
Selena Frye
Mary Weilage
Sonja Thompson
Teena Hammond

Graphic Designer
Kimberly Smith

Contents

Introduction

The rising tide of the Internet is putting tremendous strain on public networks, wireless networks, and corporate networks. The proliferation of cloud computing, Big Data, and video—along with the explosion of connected mobile devices—is driving an escalating demand for faster and more efficient networks.

One of the technologies emerging to help meet this demand is software-defined networking (SDN). SDN is still relatively new and it will likely be awhile before we see widespread adoption. But it is poised to enable business transformation and will play a major role in shaping the future of networks.

In this guide, we've collected information that will help you understand what SDN is, what benefits it offers, how it is currently being implemented, and what promise it holds for the future.

Sincerely,

Jason Hiner
Editor in Chief

Getting acquainted with SDN: 10 big questions

By Mary Shacklett

Software-defined networking (SDN) is a way to virtualize networks for ease of configuration and maintenance in the same way that servers and storage are being virtualized. The difference is that SDN as a network solution is not nearly as far along as virtualization in the server and storage worlds.

Nevertheless, SDN is coming—and the more IT decision-makers and business leaders know about it, the better they'll be able to determine where and when to introduce it to their data centers. Here are 10 of the more pressing questions they're asking about SDN.

1: What does SDN do?

Like the server hypervisors used in virtualization, SDN introduces a layer of software between bare metal network components and the network administrators who configure and set them. This software layer gives network administrators an opportunity to make their network device adjustments through a software interface instead of having to manually configure hardware and actually physically access network devices.

2: What does it mean when people talk about SDN decoupling hardware from software?

There are two planes in network devices—a control plane that determines where traffic is sent and a data plane that forwards traffic based on what the control plane tells it to do. With SDN, these two planes have been detached (or decoupled) from each other. The data plane (or *data forwarding plane*) remains with the network hardware—but the control plane (or *controller*) that makes decisions about where traffic will be sent is now executed through software. This separation makes network virtualization possible because you're no longer executing all the command or control rules on the hardware itself.

3: Why would you want to do this?

In today's networks, proprietary firmware on the switch determines where packets of data are forwarded. In an SDN, network administrators can actually shape network traffic. They can do this from a centralized network console that integrates the information and controls of all their network switches into a kind of *network fabric*. They can also change the data traffic rules on the fly if they need to.

The network administrator has complete control over network traffic through a software interface that SDN provides. This allows organizations to decrease their reliance on more expensive switches with proprietary firmware that performs these functions—and that must be set manually.

4: What other benefits does SDN provide?

SDN is an open source product and as such is open and vendor-neutral software. Because SDN adheres to open standards, it can theoretically operate with any vendor's network hardware. From an IT perspective, this gives organizations the ability to avoid vendor lock-in for a host of network products. It also gives IT enormous agility because an open standards solution like SDN simplifies the task of connecting up to different clouds, applications, and network devices—and it allows network administrators to use software for much of the work they used to do manually.

5: What is the difference between SDN and OpenFlow?

OpenFlow is a protocol that uses APIs (application programming interfaces) to configure the switches in a network. SDN is software that gives network administrators a console interface where they can provision, manage, and break down networks without having to physically set up network switches and devices.

6: Will SDN provide end-to-end IT infrastructure visibility?

No, it won't. SDN can be centralized through a single console for an overview of the network, but it is only one of numerous elements that must be linked together into an end-to-end view of an application as the app traverses servers, storage, and the network. Where SDN contributes is by interfacing with an overall IT infrastructure management software that can track an application through servers, storage—and elements of the network.

7: Which technology vendors have embraced SDN?

Most of the big name vendors all have SDN initiatives. Among them are Cisco, IBM, Alcatel, Juniper Networks, Broadcom, Citrix, Dell, Google, HP, Intel, NEC, and Verizon. With this much investment going into product development, SDN will assume a role in IT infrastructure at some point.

8: Why is SDN taking so long to adopt?

In some respects, SDN is a lot like the cloud when people first started talking about it. Enterprises are having trouble getting a handle on SDN and how it will specifically save them on network costs while improving overall network operations. And vendors haven't presented compelling use cases, either. As long as IT decision makers are confused, they will shy away from making the business case for SDN.

9: Can we afford to live without SDN indefinitely?

SDN's promise is in its ability to virtualize IT infrastructure. So far, the biggest portion of infrastructure that remains unvirtualized is the network. From an agility standpoint, enterprises will want to federate networks and move into and out of private and public clouds. This is where a facile technology like SDN begins to pay off. Sure, all these network hookup and breakdown operations can be done "by hand" as they are now. But in the

future, compressed project timeframes will drive IT to look for more efficient ways to configure and break down networks.

10: Is SDN a mature technology?

Not yet. Major technology vendors, while acknowledging that SDN is a future direction, have yet to agree on a common set of interoperability standards for all their network products, despite SDN's open heritage. Until these standards disputes are resolved, only early adopters whose businesses can't afford to live without a technology like SDN (think Google) will move forward with broad implementation. This doesn't mean that SDN shouldn't be on your IT roadmap. Network interoperability through software will come to the enterprise in one form or another. Today, SDN is the best bet.

How networks can keep up with the cloud revolution

By Nick Hardiman

The huge scale of cloud computing forces an enterprise to standardize, extend, and wring all the power out of its resources. Orchestration products like VMware are excellent at taking unused computing horsepower and putting it to work. Unfortunately, enterprise data center topology just won't let VMware get at all the horsepower.

An enterprise with rooms full of computers can't make best use of its resources to deal with its workload. For instance, if two sets of racks are running at half speed, half the resources are wasted. Wouldn't it be better to pack that workload on one set of racks and free up the other to take on more work?

A decade of improvements

The components of the technology stack are often overhauled to provide more capacity, instantly, at less cost. This is what has made cloud computing possible.

We've made a lot of progress in the last 10 years. The cost of a megabyte of memory has dropped from 20 cents to less than a penny. The cost of shifting a megabyte down an ADSL line has dropped from $70 to a few pennies. The number of machines that can be run from one rack has gone up from 30 physical machines 10 years ago to 3,000 virtual machines now. There's more of everything for everyone. And that's causing problems.

Private cloud problems for the enterprise

While some parts of the cloud revolution have raced ahead, some are stuck in the past. The new virtualization layer has been added to an enterprise's IT stack and is changing the way it does business, but the lower networking layer is pretty much the same old architecture. It is creaking under the strain of new demands, it is not controlled centrally, and it is not open to new features.

It's a problem first faced by the mobile phone industry when it moved to Internet technology. Running a secure mobile network on a rigid IP network caused network problems for carriers. Now, cloud computing is causing network problems for the enterprise.

It's not an issue for the hyperscale providers, like Amazon, Google, Facebook, and Rackspace. They have created highly customized networks, so neither their problems nor their solutions apply to the rest of us. And it's not an issue for the small business with four racks of computers, because the scale isn't big enough to stress the network.

But enterprises face network problems like these.

- Adding a new server takes seconds, but configuring the network for that server takes days.
- The network team is the same size, but it must support many more network devices.
- There are many more incident tickets for network problems.
- The server landscape has become dynamic, and the network team can't keep up with policy changes.
- Network devices are struggling to keep up with all the extra decision making.

These problems may come from the way a network has grown. A common way of building new IT horsepower is to fill a single rack. More racks are built using the same one-rack design, repeated over and over. This works fine until you try to spread workloads over several racks. Networking experts have to work hard to spread that load, and the resulting network is fragile, error-prone, and full of customized configuration to keep business flowing.

Fixing the network

The solution is to virtualize the network and provide cloud's OSSM benefits (on-demand, self-service, scalable, and measurable). Somehow manual processes and VLAN barriers must be removed, and controlling software must be centralized and flexible. These are the changes that will allow VMware to put all the computing horsepower to work.

SDN (software-defined networking) takes the decision-making control off the many network computers spread around an enterprise network and puts it in a central location. The ONF (Open Networking Foundation) is promoting the OpenFlow protocol, a way of providing SDN. Many of the big switch manufacturers, like Cisco, HP, Juniper, and IBM, have upgraded their network products to talk OpenFlow.

Big Switch Networks is a young company working to add SDN to enterprise data centers. Big Switch builds commercial solutions using OpenFlow for a client list of early adopter enterprises with between five and 10 thousand servers. Big Switch has extended the SDN idea with its OpenSDN architecture, has open sourced its Floodlight OpenFlow controller, and has encouraged a community to form around Floodlight. The Big Switch company is small, but since two founders of Big Switch and its board of directors have all had ridiculously successful careers, it won't stay that way for long.

What about the rest of us? When do we get a flexible network? The early adopters—certain large industries that can afford to implement this new way of networking—started discussing the changes to be made in 2011 and they are now running pilots. The rest of us—the mainstream enterprises—are a couple of years behind. We may have started talking about more flexible networks last year, and we may run a pilot this year. And maybe we'll enter production in 2014.

Software-defined networking: "Virtualization's last mile"

By Joe McKendrick

Now that server, storage, application, and data virtualization is underway at many organizations, networks are poised as the next great frontier of abstraction. Enter software-defined networking (SDN), which will bring more benefits to organizations than simply more efficient networks.

"The datacenter's resources may be dynamic, but the communications between them are still static and brittle."

That's the word from a recent report (PDF) out of Accenture, which observes that SDN takes two forms—network virtualization and network programmability.

Network virtualization, Accenture explains, "creates a network in the software realm, all the way down to virtual switches and routers. This frees applications from the need to understand the internal intricacies of the physical network." Network programmability, on the other hand, involves "centralizing control of the routers and switches in order to reconfigure them as infrastructure changes."

The market is fragmented, and no single vendor dominates emerging SDN space. The Accenture report cites high-profile examples of SDN at work. Google, for one, has adopted the OpenFlow protocol "to boost utilization on its internal network." Google anticipates that soon it "will approach 100 percent utilization of the company network" with the programmability of SDN, compared to the industry-wide average of 30 percent to 40 percent utilization of networks.

In another instance, Verizon "anticipates using SDN to relieve loads on individual data centers to redirect traffic to other, less-utilized datacenters in different time zones." Another high-profile operation, eBay, employs SDN "to be innovative faster" the report noted. "Not only can eBay's developers create and test new network-based products and services faster, but eBay can deploy those services faster."

SDN has promise, but Accenture also has some words of caution: "SDN is complex because of all that it touches. It requires tools and frameworks that are still developing. The interim alternative of doing it yourself is time consuming and expensive. There's a difference between virtualizing your datacenter and virtualizing your entire network. But on the former scale, the benefits are too tangible to ignore."

How does SDN affect network security?

By Michael Kassner

You know those stodgy, oft forgotten, work forever with ne'er a complaint switches and routers scattered throughout your network? They're about to get a well-deserved makeover, ensuring their continued status as networking's unsung heroes. And it's all because of software-defined networking (SDN).

What's more, routers and switches will no longer be wimpy passive pieces of hardware, but components of a powerful proactive network—something you'll especially appreciate if you have ever been on the receiving end of a DDoS attack. Type a few lines into your computer, and the network you are controlling alters appropriately, sending all DDoS traffic into a black hole.

Some networking-speak

I was told that if I wanted to understand SDN technology, I'd need to comprehend "control plane" and "data plane" as networking concepts. Seems like a good place to start.

When talking about a router or a managed switch, firmware developers often separate the device into control plane and data plane functions similar to the diagram in **Figure A** (courtesy of Wiki at NIL .com).

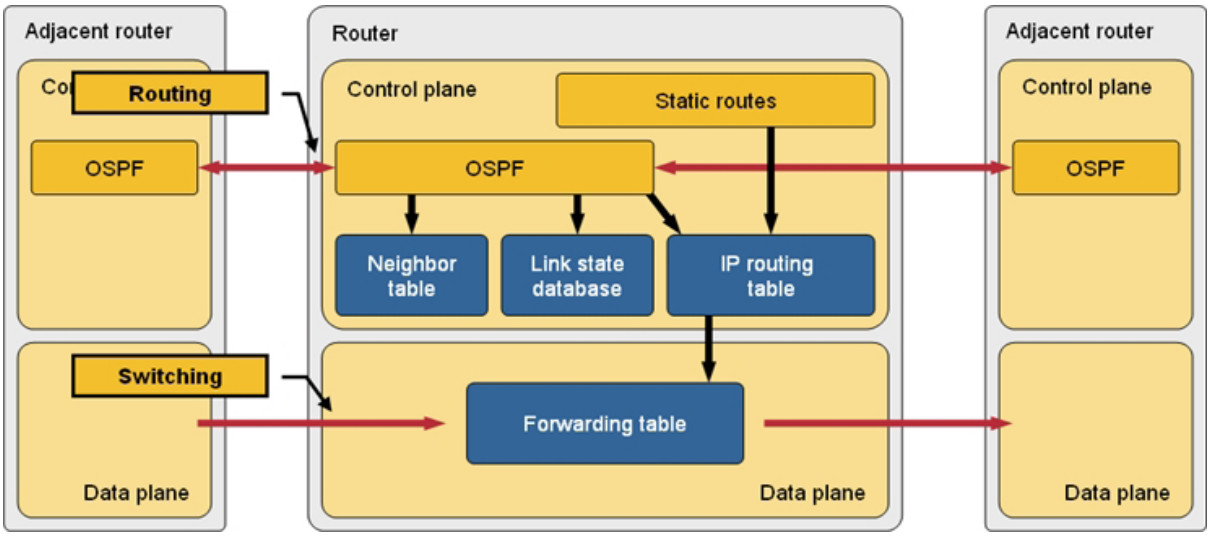


Figure A

The control plane is the brains of the outfit. The router receives information from surrounding routers and network administrators. The control plane's electronics continually process the incoming data, passing appropriate instructions to the data plane's forwarding table.

I liken the data plane to a traffic cop, dutifully directing each packet to the right exit ramp. Something to remember: All traffic entering the data plane is only passing through on its way to a remote location.

Software-defined networking

Leaving routers and switches alone used to be an okay thing. They would just work, pushing traffic down the road. But in today's mobile digital world, there are many more kinds of traffic (latency-sensitive video, for example), so the "one size fits all" scenario is no longer acceptable.

Getting rid of that scenario has been the quest of a Stanford research team since 2008; their solution is OpenFlow Switching. These videos will give you a good idea of how OpenFlow easily alters a network's configuration to fit "any size."

Remember my going on about the concepts of control plane and data plane? Here's why. In OpenFlow, the researchers physically pulled the control plane function ***away*** from the switch, moving it to a PC-based application, as shown in **Figure B** (courtesy of OpenFlow.org).

I wanted to dig into SDN, its future, and its potential a lot deeper, so I asked Sarah Sorensen, author (*The Sustainable Network*) and principal at Sorensen Consulting, for her opinion. Besides her consulting practice, Sarah writes extensively on SDN technology and how SDN provides unique network solutions.

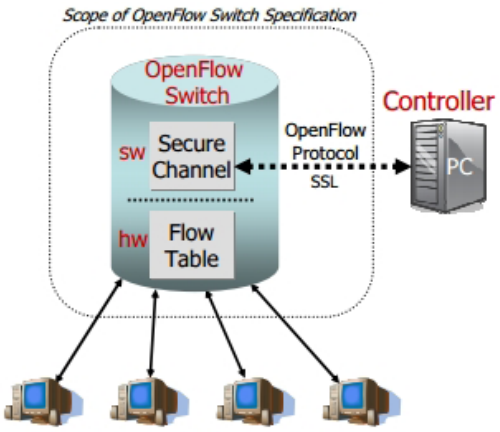


Figure B

I started by asking Sarah to describe what SDN has meant to her.

Sorensen: Over the past few decades, we have seen immense innovation on the application-side (think Facebook, Google+, and Salesforce); however, the underlying network has remained basically the same.

SDN tackles the barriers (complex and proprietary networking devices) that inhibit scale, automation, and agility by separating the forwarding layer (router/switch/network device) from the control layer (network OS, which provides a central view and control over the network) and the application layer (business/software apps).

Next, I asked Sarah why SDN is considered a disruptive technology.

Sorensen: This architecture, combined with open easily programmable interfaces, makes it simple to mix and match solutions from different vendors, create custom management apps, and develop new capabilities. It gives you choice, speed, and agility—all good reasons to be excited about SDN.

I mentioned to Sarah that most of the material I found about SDN was in academic papers, and the only working model I knew of was at Stanford. I wondered whether SDN was still in development stage.

Sorensen: It's true a lot of the bigger deployments are within research environments—for example, Stanford, Berkeley, and Indiana. You can check out this website for a comprehensive list of SDN projects.

There are some SDN pilots in telecom-research networks: NEC and Ericsson come to mind. Google has gone public about its inter-data center SDN deployment. I would say most organizations are still trying to figure out where SDN technology potentially fits in their environment.

Is SDN good for security?

Getting the SDN basics squared away, I began to understand the opportunities referred to by security gurus. For example, SDN technology will simplify extending VLANs (network segments) beyond the building perimeter, increasing the chances of data remaining secure.

SDN technology can also help with the challenge of nebulous network perimeters. Vague boundaries make it impossible to determine where to deploy security devices such as firewalls. SDN technology can help by allowing administrators to route ***all*** (internal and perimeter) traffic through one central firewall. And there's an additional benefit of network traffic flowing through a single point: It facilitates real-time capture and analysis of IDS and IPS data.

SDN's weaknesses

Once again, I'm reminded that "Convenience comes at the price of security," after reading Roy Chua's interview with Phillip Porras on SDN Central: "SDN Security — An Oxymoron."

I listened to what Phillip had to say. His knowledge of IT security impressed me when I was writing about the BLADE project back in 2010. Phillip is currently program director of SRI's Internet Security Group. Needless to say, I quickly reintroduced myself to Phillip wondering the whole time why ***SDN security*** is an oxymoron.

To get a flavor of what Phillip thinks about the security of SDN, particularly OpenFlow, here's a quote from the interview:

"I think the state of OpenFlow security is very immature and would not recommend OpenFlow in highly sensitive networks."

Further, in the interview, Phillip elaborates:

"[T]here are two sides to this coin: a critical analysis of the security challenges posed by SDNs and the exploration of potential new defensive capabilities that SDNs may enable. I expect more work will be published (this year) discussing the underlying insecurities that must be address in the OpenFlow stack."

I asked Phillip whether he was concerned about any issues other than OpenFlow. He emphasized what I alluded to at the beginning: Existing network devices are as close to bulletproof as you can get —offering five-nines in up time. SDNs will have to live up to that standard or they will not make a dent in the networking market.

One area of concern Phillip mentioned was the connection between the controller and the network devices it communicated with. If you remember the earlier diagram, the interconnection was SSL Ethernet. If that fails

or becomes compromised, the network doesn't just lose the connection to the controller—the network goes down.

As I said, one of SDN's cool abilities was diverting a DDoS attack. I thought it best to ask Phillip if he agreed with the SDN Central article mentioning Radware's SDN application, an Adaptive DDoS Protection Solution.

"The potential exists that SDNs offer greater dynamic reprogramability of network flows, and greater flexibility in restructuring a network under significant flooding. I find this aspect of OpenFlow very intriguing."

But Phillip added an example of the other side of the coin:

"Unfortunately, SDN also introduces new potential security challenges. For example, one could imagine an adversary who attempts DDoS-ing the SDN stack itself. Rather than flooding routers or attacking the hosts or applications, an adversary might craft traffic streams simply to increase the interactions between the switches and the controller, i.e., a Control Flow saturation attack. We outline such an attack in our FRESCO paper at NDSS 2013."

Phillip spent some time explaining the real security advantage that SDN affords. For longer than most would care to admit, the only way to fight exploits was *blocking* the attack. With SDN, many other responses are available, including reflector nets, quarantine systems, emergency broadcasts, tarpits, and advanced OpenFlow-enabled honeynets.

Final thoughts

The advantages and conveniences of SDN technology are numerous and more than a little exciting to those responsible for network administration. My question then becomes: Is it enough so to garner wholesale adaption of SDN?

I'm hoping Sarah, Phillip, and other SDN experts will make sure SDN works as well as, if not better than, the stodgy, oft forgotten, work-forever routers and switches that helped get this article from me to you.

HP predicts SDN will go mainstream in 2015

By Larry Dignan

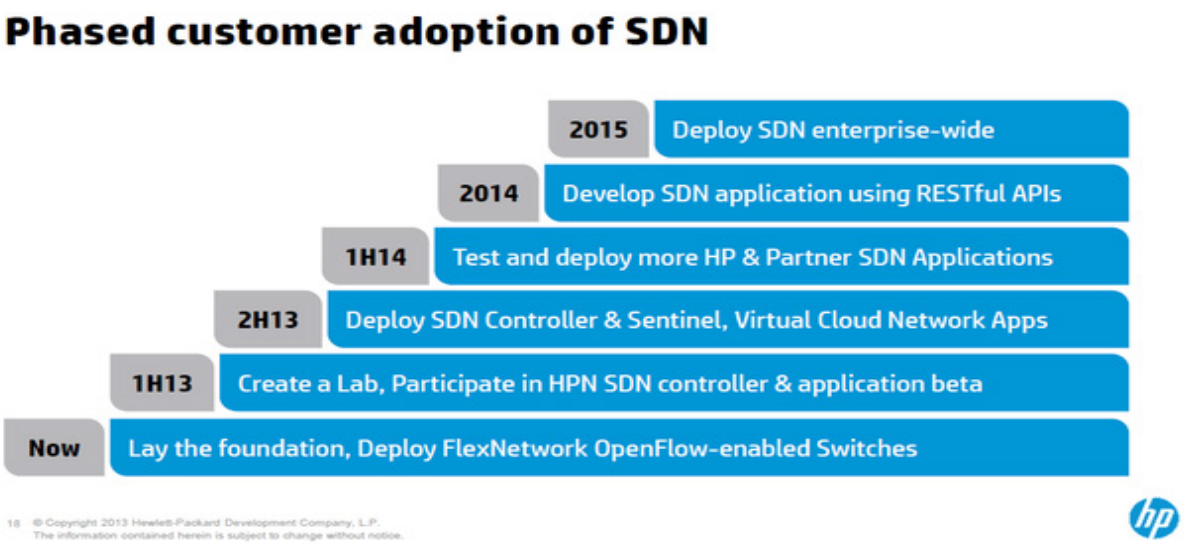
Hewlett-Packard executives outlined their software-defined networking (SDN) strategy and position in the market and made a few bets on when the technology will go mainstream. The bet: SDNs will be deployed enterprise-wide in 2015 and represent a $2 billion market in 2016.

The HP presentation is one in a series of Webcasts designed for customers and Wall Street to highlight key business units, such as networking and software.

According to Bethany Mayer, general manager of HP Networking, the company is planning to utilize its position as a large player in the market to push SDN. VMware made a splash with its acquisition of Nicira, and SDN acquisitions have become common. HP's argument is that its specialty in automating the data center, as well as a large footprint of customers, make it a leading SDN player.

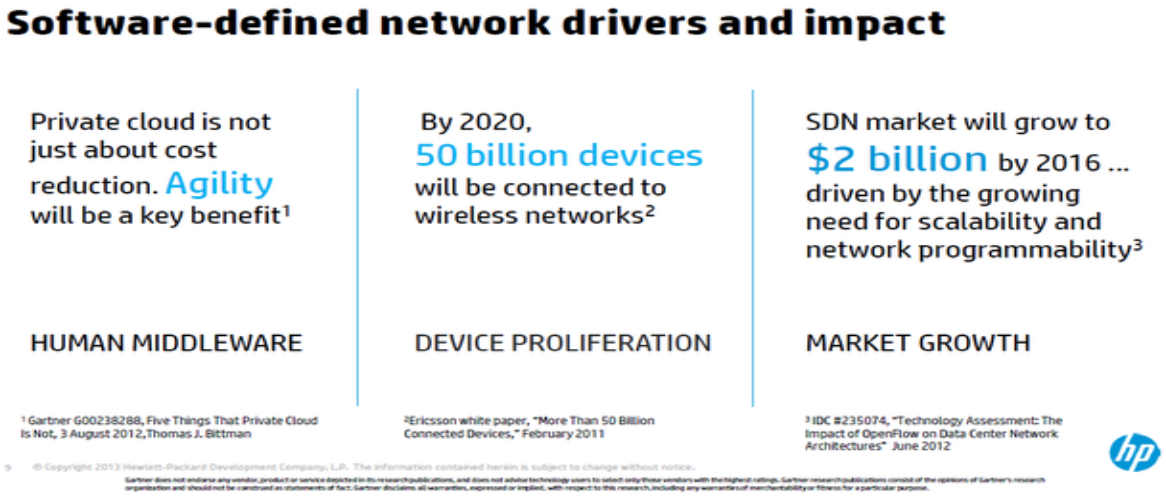
"The network has been for many, many years a very complex infrastructure, very fragile, very difficult to manage and change and as a result, many CIOs have really struggled with making changes to respond to their business using the network, and so our focus within HP Networking and everything we do is focused around simplification of that," Mayer said. "Everything we do with regard to thinking about operating expense for the CIO focuses on ensuring they can automate as much as possible within the network."

Mayer's case revolved around HP's partnerships and focus on open standards. She also noted that HP is a large No. 2 to Cisco and can serve as a counterweight.



What's unclear is whether SDNs will ultimately curb hardware sales. HP seemed to indicate that it will be able to sell more converged systems, but the wrinkle is that router and switch sales could take a hit. What if SDNs enable companies to offload networking intelligence on a cheap server?

Mayer said the differentiator would be the networking intelligence software and virtualization. Of course, HP would then run into VMware.



The Linux Foundation unifies software-defined networking powers

By Steven J. Vaughan-Nichols

In a recent debate, I argued that while there's been a lot of software-defined networking (SDN) hype, it's also real and will redefine corporate networking in the coming years. The Linux Foundation and—in its OpenDaylight Project—has introduced a community-led and industry-supported open source framework to accelerate SDN adoption, foster new innovation, and give it a more open and transparent approach.

That sounds nice, but without industry backing, it doesn't mean much.

OpenDaylight has the support it needs to transform SDN. Big Switch Networks, Brocade, Cisco, Citrix, Ericsson, IBM, Juniper Networks, Microsoft, NEC, Red Hat, and VMware are all founding Platinum and Gold members of the project. It will donate software and engineering resources for this open source framework, and help define the future of an open SDN platform. Yes, that's right: Cisco and Juniper, Microsoft and Red Hat, and other major industry rivals are all joining forces.

Specifically, OpenDaylight will be supporting already existing open standards, such as OpenFlow. The project's goal is to deliver a common open source framework and platform for SDN across the industry for customers, partners, and developers. The customer win: a single multi-vendor and open source SDN platform.

The first code from the OpenDaylight Project should be released in 3Q13; expected donations and projects include an open controller, a virtual overlay network, protocol plugins, and switch device enhancements. What makes it in will be determined by the OpenDaylight Technical Steering Committee (TSC).

"This is a rare gathering of leaders in the technology ecosystem who have decided to combine efforts in a common platform in order to innovate faster and build better products for their customers," said Jim Zemlin, executive director at The Linux Foundation. "The world has learned that collaborative development can quickly drive software innovation, especially in fast moving markets. We are excited to be working with OpenDaylight and expect truly amazing things to come."

At this point, we know that Big Switch Networks is planning to contribute open source elements of its Open SDN Suite to the OpenDaylight Project. This will include controller code, advanced data store with high availability, distributed virtual routing service applications, network virtualization, network overlays, and other applications.

Cisco has contributed controller technology, including an application framework and service abstraction layer (SAL). This provides basic controller functionality with support for southbound plug-ins to communicate with network devices using various protocols, including OpenFlow, the ability to integrate controller applications as modules, and a set of REST APIs (representational state transfer application programming interface) to expose the controller capabilities.

Cisco's archrival Juniper Networks is planning to contribute a number of technical elements, including extensible messaging and presence protocol (XMPP) client and server protocol code and a flexible data model.

For its part, Citrix is contributing an application controller that integrates Layer 4-7 network services into OpenDaylight Project. Citrix has also committed to contributing a plug-in for OpenDaylight into the Apache CloudStack project.

IBM intends to submit an open source version of its Distributed Overlay Virtual Ethernet (DOVE) technology as its initial contribution. According to IBM, DOVE is designed to work on top of existing network infrastructures to help simplify the process of setting up, managing, and scaling virtual networks for faster and more flexible delivery of cloud, analytics, mobile, and social business services.

Red Hat will be working on building and delivering an SDN solution that integrates with OpenStack and Linux's built-in Kernel-based Virtual Machine (KVM) hypervisor.

Microsoft hasn't spelled out what it plans to contribute to the project yet. Brad Anderson, Microsoft's corporate VP for Windows Server and System Center, said in a statement, "Microsoft is pleased to be a member of the OpenDaylight Project and to work with industry leaders to create a common framework and platform for SDN. The OpenDaylight Project aligns with Microsoft's commitment to open standards-based development and enables the industry to benefit from Microsoft's deep experience running global, large-scale data-centers and delivering flexible, elastic cloud-scale services."

All the OpenDaylight code will be operating system independent and is expected to be available on multiple platforms. It will be licensed under the Eclipse Public License (EPL). This is an Open Source Initiative approved license.

These companies are taking on a monster of a job. The problem isn't so much the standards or the code; it's getting everyone on the same page. The mere fact that The Linux Foundation has brought together essentially all the major players in the SDN space and has gotten them to agree to work on a common, open framework is remarkable in its own right. If they're successful in actually creating the OpenDaylight framework, SDN will be one giant step closer to becoming the new datacenter and corporate networking standard.

Cisco's legacy hurts its virtual networking strategy

By Jack Clark

Cisco's commitment to hardware has forced it to take an Oracle-like approach to the disruptive technologies of software-defined networking. Fiscal year 2012 earnings were better than expected for the networking giant, but trouble may lie ahead for Cisco as businesses, universities, and start-ups begin adopting software-defined networking. That technology decouples the management and orchestration of a network from switches and onto commodity hardware, making it easier for data center operators to spend much less on data center kit.

Cisco's chief executive John Chambers gave an agenda-setting answer when asked on last year's earnings conference call about the company's strategy around software-defined networking (SDN).

"We think the future is going to be hardware and software combined. We think when you have knowledge of the network, and are able to know what's going on in the network, you can program to it," he said, according to a transcript on SeekingAlpha.

Cisco's approach makes sense for the company, but then it would, to a hardware incumbent. "If all you have is a hammer, everything looks like a nail" pretty much sums it up.

Software and hardware together

Reading between the lines, Chambers' answer suggests that to get the most out of SDN, Cisco believes a thorough understanding of the hardware layer is needed. In turn, this means the software and hardware should be developed by the same company and linked together.

To that end, Cisco has so far sought to boost its SDN credibility by embedding more sophisticated software in its switches. While this doesn't fit the exact definition of SDN—which moves control from switches up into a central management plane, probably using some form of commodity x86 server—it has roughly the same outcome. Switches become more manageable via a central interface.

This sounds good. But if you analyze Cisco's view, it suggests the company is keen to make sure a more software-focused approach does not threaten its longstanding networking hardware business.

For one thing, it lets Cisco keep the prices high on its networking equipment: By using its Cisco ONE (Open Network Environment) technologies to put more software on its switches, it can give customers SDN features while encouraging them to keep on buying its "smart" equipment, which is priced at a premium.

The approach means Cisco wants to embed information about the network at the hardware layer and have it flow up to a more flexible software control plane. This differs from the approach taken by SDN-like technologies such as OpenFlow and Nicira, which see intelligence originate and reside in the control plane, with decisions pushed out to the hardware.

This strategy is akin to Oracle's "software and hardware, engineered together" approach, a tactic the company committed to after it gained a huge hardware division in its Sun Microsystems acquisition.

Both Cisco and Oracle are trying to embrace new technologies, but on their own terms. This would be fine if they were smaller companies. But both have such dominance of their respective markets that the decisions they make will influence the rest of the IT industry.

A different direction?

There are signs that major IT organisations are going in a different direction from Cisco. Take Google, for example. It built its own networking gear and then announced that it implemented an all-SDN OpenFlow-based networking system to run on top of it. As a result, Google expects network utilisation of nearly 100 percent, compared with the industry's typical 30 to 40 percent.

This is all made possible by the efficiencies in traffic routing that can be squeezed out when all the intelligence comes from a central control plane giving orders to underlying hardware, rather than the other way around.

OpenFlow was developed at Stanford University and has gathered huge interest in academic circles. For example, Indiana University is building a US-spanning OpenFlow-enabled network under the name Internet2.

Furthermore, Cisco's rejection of this type of SDN could put it on a collision course with virtual computing environment allies VMware and EMC, now that EMC-owned VMware has acquired network virtualisation company Nicira for $1.3bn.

VMware is expected to integrate Nicira's technology with its virtualisation software to help move information around and between data centers. Crucially, Nicira's approach does not care about the underlying hardware. This means that Nicira-based networks are not tied to any one supplier and are capable of an SDN-style central control plane.

Competition with old pals

Chambers acknowledged on the conference call that this could lead to competition between Cisco and VMware.

"With VMware and EMC, it's been a very strong partnership," he said. "We've both benefited greatly from it... but we are going to be an open player, and we've shown in the marketplace when we compete, we can be really tough."

Ultimately, Cisco's approach is good for investors but potentially bad for innovation, as the company will likely seek to use its influence to make its particular view of SDN the industry standard. If this happens, businesses will have to keep spending large amounts of money on IT equipment that dovetails into proprietary software, which then has API compatibility or NIC-support for OpenFlow. Though this may make SDN slightly more accessible to smaller businesses, it could lead to larger companies giving Cisco the cold shoulder and taking the Google route.

Cisco SVP hails software-defined networking as game changer for data centers

By Rachel King

Connected devices are profoundly affecting data centers and IT infrastructures—but they're also presenting huge opportunities for software-defined networking, according to Christopher Young, senior vice president of Cisco's security and government unit.

Citing Cisco's forecast that there will be 50 billion devices connected to the Internet by 2020, Young said that as the number of connections increase, so too will the number of applications running in and for the cloud.

"Further extension to these trends around mobility and cloud is the Internet of Everything," Young said, while speaking during a keynote session at the 2013 RSA Conference in February.

As we move into this era, the network itself is going to become increasingly programmable through APIs and data analytics at all layers, he said.

"It's great to see a lot of our CIOs planning to adopt cloud-based applications over time, but the reality is most CIOs are being dragged to the cloud by their users and lines of business."

Young said that public cloud apps are actually the ones leading the charge and that the Internet of Everything revolves around a network of networks where billions—or even trillions—of devices are going to connect to one another.

While he said that this will create plenty of opportunities, Young admitted that's going to generate a lot of risk too. From a security perspective, Young said this shift is giving way to the "any-to-any problem," which he defined as having any user on any device going to any app running on any data center or any cloud. Increasingly, he predicted, end users will connect to apps to get their jobs done without ever going through the company's controlled network.

The answer to these changes for networks and data centers that underpin this any-to-any model are SDNs, Young said. He added that Cisco refers to this as "application-centric networking" because the company is introducing programmable APIs that allow apps to draw intelligence (and value) directly from the network itself.

Through SDNs, Young said, we'll get a far greater convergence between network and data center infrastructures, which have been historically disparate.

"Software-defined networking is going to bring the cloud model that we're all starting to focus on more and more, and put it on steroids." In particular, he said, we're going to see lower operational costs, be able to scale applications and network services more quickly, and do more cloud bursting on-demand.

Young said we're experiencing an evolution of programmable networks, which doesn't necessarily require a "fork-lift upgrade" to get the benefits. A simple operating system upgrade might be all that's needed to get the value of SDN.

Still, Young acknowledged that we will need to secure networks differently due to SDN architectures, requiring advancements around authentication and more flexible levels of encryption.

"The threat landscape is also changing. You all know the headlines," Young said." What's old has become new again." He cited denial of service attacks on financial systems as one example.

Young said we need to act in more real-time with more pinpoint accuracy and with a greater ability to act on all our knowledge. "The big opportunity here is to make security the key application for software-defined networking."

HP boasts its SDN fabric cuts provisioning down from months to minutes

By Rachel King

Hewlett-Packard is stepping up its data center game with a recent announcement of a new suite of solutions for software-defined networking. Built on its FlexNetwork converged networking architecture, HP boasts that it can offer up to two times greater scalability with "75 percent less complexity" compared to other networking fabrics on the market. Furthermore, HP asserted that its data center fabric will reduce provisioning timeframes all the way down from months to mere minutes.

HP's portfolio of SDN services is quite substantial, with products aimed at addressing various issues, from dealing with legacy infrastructures to simplifying operations. For example, the HP Virtualized Services Router is designed to cut back data center footprints by delivering services on a virtual machine, which should eliminate "unnecessary hardware."

In addition, the HP HSR 6800 Router Series aims to simplify network service delivery by consolidating routing, firewall, switching, and security onto one device that supports thousands of users.

It's a busy time in this space, as many tech giants are turning away from their old staple products (notably PCs) toward building up their data center businesses—especially through open source technology (see: Hadoop) and software-defined data centers.

For instance, Dell recently introduced its own new software-defined networking fabric for deployments of converged, virtualized, and private cloud environments. That particular SDN fabric supports networking virtualization overlays using hypervisors from the likes of Microsoft, VMware, and OpenStack, while supporting programmatic interfaces, such as Telnet/CLI, TCL, REST, SNMP, Perl, and Python scripting.

HP's suite of SDN offerings will be rolling out over the course of the year. Only the HSR 6800 Router Series is available worldwide now, and it holds a starting price of $46,000.

SDN gets a commercial boost from Big Switch Networks

By Jack Clark

Big Switch Networks pushed out a major software-defined network (SDN) product suite last fall, giving SDN a commercial boost. The Palo Alto-based startup, along with a large set of partners that includes Microsoft, Citrix, Dell, F5, and Juniper Networks, launched the Open Software-Defined Networking suite in November. The suite consists of the Big Network Controller, the Big Tap monitoring tool, and the Big Virtual Switch, which allow network administrators to cram more virtual machines onto servers. They do this by increasing the efficiency of the overall network and giving the servers advanced monitoring capabilities.

Software-defined networking (SDN) is causing disruption in the networking industry, as it lets businesses move many networking features off expensive networking gear and onto cheap servers. It goes hand in hand with virtualisation as a key technology for making efficient, easily configurable private and public clouds.

In a press release, Guido Appenzeller, the chief executive and co-founder of Big Switch Networks, said, "SDN is the most disruptive and transformative trend to hit the networking industry in over 20 years."

For example, SDN allows businesses to change the structure of a network via its software without having to move physical equipment around. It also gives admins greater insight into a network's traffic flow, meaning they can spot and remedy bottlenecks earlier, and it lets them avoid proprietary networking technologies.

OpenFlow savvy

The fundamental technology beneath Big Switch Networks' suite is the OpenFlow network communications protocol—something the company knows a lot about, given that Appenzeller led the Stanford University team that developed the first version of the protocol.

OpenFlow technology lets servers communicate with networking equipment, making it possible to shift some network gear duties to servers, allowing for both cost savings and more efficient, flexible network structures.

The Big Network Controller is an application platform that communicates with OpenFlow software switches embedded in hypervisors and OpenFlow-compatible network interface cards (NICs). This enables admins to use advanced software tools to manage both the physical and the virtual network.

The Big Tap has monitoring capabilities for an SDN, while the Big Virtual Switch helps create and manage the physical network.

Big Switch Networks' main SDN competitor is Nicira, which was acquired by VMware last summer for more than a billion dollars. However, Nicira's products are designed to manage virtual networks rather than physical ones, giving Big Switch Networks an edge in terms of the breadth of IT environments it can cover.