CAN SDN SOLVE THE PRIVATE CLOUD BOTTLENECK?

In a flexible server virtualization environment, manual networks only slow things down. Software defined networking may solve the problem.

PLUS:
SDN GOES WELL BEYOND THE DATA CENTER NETWORK
WHY IS SDN THE VENTURE CAPITALIST DARLING?
flowvisor opens path toward open network virtualization

**FlowVisor**, a network virtualization platform that builds on OpenFlow, moves open software defined networking (SDN) up the stack by allowing easy slicing of a physical network into multiple logical networks. This open community development that began at Stanford University gives administrators the power to manage with broadly defined rules rather than by tweaking a collection of routers and switches.

Installed on commodity hardware, FlowVisor is a special OpenFlow controller that acts as a transparent proxy between a network of OpenFlow switches and other standard OpenFlow controllers. While still considered experimental and lacking some basic features, such as command-line management tools, FlowVisor has been deployed in production environments at scale, including powering Stanford’s campus network since 2009. FlowVisor slices up physical networks through an abstraction layer that is equivalent to how a hypervisor sits between server hardware and software, allowing multiple virtualized operating systems to run on one server. FlowVisor sits between a set of switches—and the software defined network or networks—and manages bandwidth, CPU utilization and flow tables.

Just as a hypervisor relies on a standardized x86 instruction set to virtualize servers, FlowVisor manages OpenFlow switches using the standardized OpenFlow instruction set, which sets low-level rules about how packets are forwarded based on characteristics found in the packets’ header tables.

Because all these rules are defined with flow tables, this network virtualization adds minimal or no overhead, either in bandwidth or CPU usage, although separate out-of-band physical controllers that set and modify flow table rules are needed.
Slicing and Dicing Toward SDN

The basic elements of the FlowVisor-enabled network are the network slices, which are defined by a set of text configuration files that contain rules that govern a range of network activity. Possible rules include allow, read-only and deny, while ranges can include a flow’s origin IP address, port number or packet header information.

For example, a network manager can partition secure Telnet traffic (which defaults to port 992) into its own slice, while assigning traffic from the executive team’s IP addresses into another slice. He can then create a third default slice for all other traffic and establish a final “read-only” slice that monitors the other three slices for diagnostic purposes. The network manager can dynamically reassign and independently manage these slices, ensuring that a receptionist browsing YouTube does not negatively affect Telnet-driven applications and executive team bandwidth.

Slice isolation is a critical part of FlowVisor’s virtualization, but it is also an evolving area for the experimental platform. A published academic paper describing FlowVisor’s vision and implementation, for example, calls for tight switch-CPU isolation, a feature that is currently limited at best, since switch CPUs are only indirectly manageable through OpenFlow. Given these evolving limitations and capabilities, FlowVisor works to virtualize and isolate along five key dimensions, as defined by the OpenFlow technical report.

1. **Bandwidth:** Each slice should have its own dedicated percentage of the total available bandwidth.

2. **Topology:** Each slice should have its own view of network nodes, including both physical and virtual switches and routers. The elements of a slice should be unaware of the slicing. To a controller, FlowVisor looks like an ordinary switch; from an OpenFlow switch’s perspective, FlowVisor appears as a controller.

3. **Traffic:** Traffic should be tightly and consistently isolated to a specific slice or slices, based on the rules set as described above.

4. **Device CPU:** Overloaded physical switches can drop slow-path packets. The network manager should update OpenFlow statistics counters and rules, so FlowVisor takes into account CPU resources when rate limiting intensive commands.

5. **Forwarding Tables:** Since forwarding tables are often constrained on physical devices, the network manager should ensure that one slice does not overwhelm any given device’s forwarding table, forcing it to drop the rules of another slice.
Idea Lab

BY TOM NOLLE

SDN Could Make Network as a Service a Reality

BUYERS ARE ALREADY sold on Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), but what about Network as a Service? Despite the fact that the cloud is connected through the network, we hear little or nothing about a new network paradigm for the cloud. Network as a Service is not only real, but it is likely to become universal. However, it may take software defined networking (SDN) in the form of OpenFlow to make that happen.

Cloud computing deploys a public pool of resources that can be provisioned on demand. The cloud also involves connections to its users, storage access, inter-process communications and resource allocation or management.

Typical IP and Ethernet network technologies have shortcomings when it comes to the cloud because of security, QoS and operational cost scalability. At the heart of those limitations is the notion of permissive connectivity. IP and Ethernet presume that all endpoints can be addressed by others.

This presumption of universal connectivity makes it harder to manage security and engineer traffic flows to meet specific application SLAs.

One proposed solution is to centralize a connection policy using SDN. In SDNs, the endpoints have no implicit right to connect, so nothing on the network is connected at first. Instead, a software control function decides what connections to permit and which route traffic will take for those connections. The controller bundles connectivity, security and traffic engineering into a single master-control location where policies dictate how resources are used and who’s allowed to connect with what.

This centralized network resource management is virtually identical with the resource management strategy behind IaaS, PaaS and SaaS cloud services. Therefore, it’s not surprising that SDN-based networking will be the foundation for Network as a Service.

Many major switch/router vendors have expressed support for OpenFlow, an architecture that is an implementation of SDN.

OpenFlow is a combination of a specification and open-source software that runs in a switch or router as part of the central controller. In an OpenFlow network, when a switch or router gets a packet, rather than mak-
ing the forwarding decision itself, it sends the packet to the controller, which then uses policies to make the decision. Those policies then create a forwarding rule, which the controller passes back to the requesting device.

**For Network as a Service, Openflow Has Benefits and Challenges**

The description alone of how OpenFlow works illustrates both its strengths and limitations. Because OpenFlow connections are explicit, Network as a Service is more secure and potentially has more QoS. This is because policies that set routes for packets can use application and even user priority to determine how traffic is allocated to resources, thus setting performance levels. In theory, an OpenFlow network could be safe from denial of service attacks and would be more difficult to hack. In addition, they would support video and critical applications better.

The challenge with OpenFlow is scalability. An OpenFlow network could not work if every packet had to be sent to a central controller to be analyzed. To make Network as a Service work, OpenFlow scalability must be improved or its use must be contained within cloud networking. Both options are already being proposed.

OpenFlow will work best where traffic is made up of a modest number of predictable flows. That way, once the switches/routers learn the traffic rules from the controller, little additional interaction with the controller is needed. When used within a data center to control server-to-server or server-to-storage traffic, OpenFlow is a very important contribution. Even within data centers in a distributed cloud (public, private or hybrid), OpenFlow could be expected to manage traffic within the cloud. The question is whether it can manage traffic between the cloud and cloud users, and if not, how OpenFlow SDNs and Network as a Service will be linked to the users.

**Merging Openflow with IP Networking May Be the Answer**

If a large base of users/workers is visibly beyond the scope of an explicitly-managed connection, what’s needed is a way of somehow merging OpenFlow with traditional IP networking at the edge of the cloud. Luckily, proposals are already in play to interwork OpenFlow and MPLS to generate a new kind of IP network that offers a combination of open connectivity and policy-managed connectivity.

There are also potential ways of making OpenFlow control more hierarchical and scalable. Also, there are initiatives in cloud computing, where the concept of Network as a Service first arose, to manage how we address cloud applications. These initiatives convert applications into “virtual services” of the cloud. It’s too early to say if these will create a scalable OpenFlow model, but if they do, they’ll advance...
Network as a Service by improving how cloud resources are accessed. In the future, all of these developments could create a Network as a Service that escapes the boundaries of the cloud, and moves all the way to the network edge.

Yet, within the cloud, there’s no need to wait. OpenFlow Network as a Service would offer enterprises much more control over data center and inter-data center cloud traffic than would be available today with Ethernet or IP. There is tremendous potential for lowering operational costs by eliminating expensive IP and Ethernet discovery and adaptive topology updating. The time of the Network as a Service may not be now for everyone, but all the indications point to the idea that it’s coming to data centers soon.

BY RIVKA GEWIRTZ LITTLER

Welcome to the SDN Holy War

AT THIS YEAR’S Open Networking Summit, we saw the emergence of a software defined networking (SDN) holy war.

The battle is being fought by two camps. Each camp believes in SDN, but one will go open and the other will fight to hold ownership of the networking world by going proprietary.

The open source camp is home to SDN vendors that believe in placing the brains of a network in centralized software, which will control underlying commodity hardware using the OpenFlow standard. In this camp, companies like NEC and Big Switch will build networks based on commodity hardware. They hope to see the emergence of an ecosystem of third-party applications that run on top of OpenFlow controllers and bring about new kinds network services, including granular QoS and mobility management. The most radical player in this camp is Nicira (now acquired by VMware), which offers virtual switches (vSwitches) that can be woven together in a unified fabric running over any physical network. While Nicira’s switching software isn’t open source, its virtual fabrics will be open for management by an OpenFlow controller.

The other camp is made up of traditional network hardware vendors that place decision making powers in the hardware components themselves. While these vendors are working on strategies for more centralized network pro-
grammability, they’ll do it with proprietary software.

This camp is home to the Ciscos and Junipers of the world that have invested lots of money in closed operating systems, hardware and complex data center networking strategies. They agree that networks should be more programmable, but want to do it by opening up their existing operating systems to users to develop applications that will only work on their networks. They might use the OpenFlow standard as one element of these strategies, but won’t go completely open source or allow for the use of commodity hardware.

In the past few months, those in the open source SDN camp have made big progress. At the Open Networking Summit, NEC released an upgrade to its OpenFlow-ready portfolio, and recently IBM announced OpenFlow equipment, as did HP Networking. Both Dell and Brocade demoed soon-to-be-released OpenFlow environments at the summit. In February, Nicira emerged from stealth mode with its Network Virtualization Platform.

At the same time, the other camp is chipping away at its strategies. While Cisco has said it will release OpenFlow-friendly switches, it is quietly launching a new SDN division that will work on proprietary network programmability strategies. Cisco executives made it clear at the Open Networking Summit that the OpenFlow standard alone would not be enough. Instead, Cisco’s strategy will rely on a combination of distributed network brains and centralized software control.

Most likely, neither camp will fully win. Traditional network hardware will not disappear any time soon. Enterprises will continue to deploy networks they know how to manage and for which they can hire experienced personnel. Cloud providers, for example, that need to manage multi-tenant networks in which each tenant must have its own policy control and security, will be forced to consider new methods of programmable networking.

Eventually, the need for that level of programmability will trickle down to the average company, but by then Cisco and Juniper will have sold their proprietary SDN methods to their installed-base.

Ultimately, it will take a few more generations of computer network graduates to come out of universities trained in open source SDN programming before there is enough talent in the industry to drive change at a mass level. That gives Cisco a little bit of breathing room, but it’s hard to say how much.
Do We Need A Network Hypervisor For Virtualization?

**NETWORK TRAFFIC DOESN’T** function like a server with the OS and apps stuck on a particular host. In fact, network packets are already virtual. In networking, what still needs to be virtualized are the physical components that make up the network—switches, routers and firewalls.

But once these components are virtualized, engineers need to be able to programmatically control the provisioning of these resources. To do that, the limitations of the physical network (VLAN scalability, MAC scalability, VM mobility, and conflicting IP addresses) must be eliminated. In addition, network admins will need the same visibility and functionality into virtual network that they have on the physical network.

Some of these networking capabilities exist in the server hypervisor (VMware has a vSwitch and virtual network adapters), but these server hypervisors aren’t specialized enough. Enter the network hypervisor.

**State of the Network Hypervisor**

Today many networking vendors are working toward technology that manages the provisioning and control of virtual networks, but only a few actually call this technology “network hypervisor.”

Probably the best known is the Nicira solution, which is a distributed software suite that creates scalable, fully featured, isolated virtual networks that are completely decoupled and independent from the underlying physical network. Nicira’s solution can work across any physical network and is compatible with any server hypervisor. Nicira’s open, programmable approach not only delivers Layer 2 and Layer 3 networking, it also supports Layers 4-7 services within virtual networks.

However, just because Nicira (which means vigilant in Sanskrit) has already sold its technology to some of the largest cloud providers and Internet players in the world, it remains to be seen whether this is the approach that will stick in the long term. Many competitors have other strategies.

**Virtualized Network Components Already Exist**

Companies like Vyatta, Cisco, VMware and Extreme Networks are all releasing new network virtualization solutions. Some of these work alongside the server virtualization hypervisor, while others are virtual appliances providing Layer 3 or security services. There are several examples:

- Cisco has gained lots of traction with its **Nexus 1000-V advanced virtual switch for vSphere**, which is solely focused on virtual network manage-
ment and visibility. Using the Nexus 1000-V, engineers can ensure that QoS and security policies can follow vSphere virtual machines as they move from host to host with vMotion. Cisco also recently released the Virtual Security Gateway (VSG) for the Nexus 1000-V, which provides network security for vSphere. The VSG could be compared to a virtualized version of the Cisco ASA security appliance.

- VMware has continued to enhance and release more virtual network solutions in its vShield product line. When vSphere 5 was released so was vShield 5, which offers vShield Edge for firewall and VPN. Additionally, another innovative vShield solution was released, vShield Endpoint, which offers security compliance and data protection solutions.

- Extreme Networks is offering an XNV network hypervisor, which appears to compete with the Cisco Nexus 1000V but is compatible with Microsoft Hyper-V, Citrix XenServer, VMware vSphere and Linux KVM. However, just because it is labelled a network hypervisor doesn’t mean that it offers the same functionality as Nicira.

- Vyatta offers an enterprise-grade virtual network router, firewall and VPN solution. Those needing Layer 3 IP networking services can install these directly on physical servers and turn them into routers. Vyatta calls its technology a “network operating system” and says it provides similar functionality to a Cisco Layer 3 switch, except using a modified version of Linux.

**Is SDN the True Network Hypervisor?**

As network virtualization solutions emerge, a number of companies are working on SDN strategies that will make the network flexible and yet manageable enough for Infrastructure as a Service and for nimble virtual resource provisioning in general.

Using SDN, engineers can create a separate control and forwarding plane and use centralized software-based controllers that push down forwarding rules and policies. With an SDN strategy, engineers can define how virtual routers and firewalls can be used in conjunction with virtual switches to provision virtual networks as needed.

Nicira’s network hypervisor, as well as some of the other available solutions, can work within an overall SDN architecture.

Only time will tell whether the network hypervisor will reign in networking for massive virtualized environments. What is clear is that virtualization will not stop at server hardware and will get much more complex than basic network component virtualization.
CAN SDN SOLVE THE PRIVATE CLOUD BOTTLENECK?

Engineers have a private cloud problem—they’re working with flexible compute resources that are slowed by manual networks. Is SDN the answer? BY SHAMUS MCGILLICUDDY

YOU’VE HEARD IT before but it bears repeating: Networks are bottlenecks in the private cloud. Server and storage technologies have evolved into pooled resources that cloud administrators can spin up on the fly, but networks remain far too manual. To be more agile, networks must be virtualized, and software defined networking (SDN) offers a cost-effective method for getting there.

“Enterprises need to be like service providers and react as quickly as they can for internal customers. They need to enable self-service IT. The biggest roadblock to that is networking,” said Ben Cherian, chief strategy officer with Midokura, a Japanese start-up that is developing SDN-based network virtualization technology. “Armies of CCIEs are running around making little changes to switches and routers that have requisition times of weeks.” Meanwhile in many cases, cloud providers can click a button to make changes.

Essentially, SDN technology decouples and centralizes the control plane from the data forwarding plane of individual network devices. By centralizing that control plane (usually on a server-based SDN controller) the network becomes more programmable. That leads to a more dynamic and reliable private cloud network.

“The majority of outages that we have are from someone going in and messing with configurations,” said Brent Salisbury, a network architect with the University of Kentucky who has been experimenting with SDN and private cloud technology in his test and development environment. “If I can get that down to where [network changes] are programmatic and reproducible every time, that’s a big value. You’re taking human error out of it.”
The OpenFlow protocol is the best-known means of decoupling and centralizing a network control plane, but mainstream, commercial availability of OpenFlow-friendly switches is limited. Cisco Systems, the most widely installed switching vendor in the world, doesn’t yet support the technology on any of its data center products. So SDN vendors have taken different routes to bringing the technology to market. NEC, for example, makes its own switches for its OpenFlow controller. In another approach, Big Switch Networks and Nicira Networks (recently acquired by VMware) create SDN overlays by centralizing the control planes of hypervisor-based virtual switches and then tunnelling through the physical network with protocols like VXLAN and NVGRE.

One company’s early SDN-based private cloud

Schuberg Philis, a Dutch IT management and consulting firm, once faced the epitome of the private cloud networking problem—the company built internal clouds with flexible pools of compute resources, but it had manually configured networks.

“We were building private clouds for a long time with virtual hosts that had a lot of flexibility, but every time we started to use the flexibility, we found that we had to call the network engineer and say, ‘Hey, before we use this [cloud service], we need another VLAN or another port configured in another VLAN,’” said Hugo Prippaers, a mission critical engineer with the company.

Now the firm is building its internal cloud based on SDN technology. The new cloud infrastructure consists of a high-speed, Layer 2 network built with Arista Networks switches and the Network Virtualization Platform (NVP) from Nicira Networks. The company has started small with two racks of servers topped with dual 10 Gigabit Ethernet (GbE) Arista switches, which all uplink into a pair of end-of-row Arista switches.

“The only thing you need on a physical network using a Nicira solution is fast switching. Arista was the fastest switching we could find.
It’s a completely flat Layer 2 network with just a few VLANs in there to connect to the public Internet, Prippaers said.

The Nicira NVP technology forms an SDN overlay between the virtual switches on the hypervisor hosts in the server racks and the physical Layer 2 network. The network overlay treats the Layer 2 network as an IP backbone, tunnelling Layer 3 traffic and other network services across it. As a result, Schuberg Philis administrators can make single-click changes to the SDN overlay as they spin up cloud services without having to make any changes to the underlying physical network, Prippaers said.

“With the Nicira solution the network guys can build an entire network infrastructure the way we want it, when we want it, without having to go to the physical devices again and again to reconfigure them. It frees up a lot of time,” Prippaers said. “Our network engineers are now able to focus on the core stuff of the network, making sure interconnects are completed to perfection and that the Layer 2 switching is as fast as possible. They just worry about really important stuff rather than changing port configurations.”

**SDN CLOUD SHIPPING: NORTHBOUND APIs NEEDED FOR CLOUD ORCHESTRATION**

While SDN technology can virtualize networks and simplify network administration in a private cloud, network operations can still remain siloed from the rest of the cloud infrastructure team. To streamline operations, experts say SDN must be integrated into cloud orchestration frameworks.

There must be more management sophistication in SDN, said Eric Hanselman, research director for networks at 451 Research. “OpenFlow is okay at a low level, but for Big Switch, NEC and Nicira, the real value is that upper-level control capability. Nobody wants to be out there firing up tons of Python [scripts] to do network control. You want it to be part of your top-level control environment ... that integration at a higher level is the real value.”

The Open Networking Foundation, which governs the development of OpenFlow, recently acknowledged the need for this integration by announcing an
expansion of its SDN standardization scope to focus on northbound APIs. OpenFlow is considered a southbound protocol, which allows an SDN controller to communicate with and manipulate the switching infrastructure below. But northbound APIs connect the controller to applications and orchestration frameworks that sit above. For instance, a northbound API can allow a cloud orchestration system to manipulate a network through an OpenFlow controller.

“The promise of OpenFlow down the road is that the application infrastructure itself... [should] be able to dynamically control what the network looks like, how it’s connected, and what capabilities and capacities are assigned to it.”

—ERIC HANSELMAN, research director for networks, 451 Research

actual applications or the management environment that’s launching the apps, [should] be able to dynamically control what the network looks like, how it’s connected, and what capabilities and capacities are assigned to it,” Hanselman said.

The ability to “decompose network resources into something that is consumable, along with compute and storage, must be done programmatically and [be] agnostic to the hardware,” said Salisbury. “We’re not going to start programming static flows [in SDN]. They’re worse than static routes, only a million times more granular. I think the northbound application is the only way to start integrating [SDN] into cloud orchestration.

NICIRA + OPENSTACK FOR MULTI-TENANT NETWORKS

To solve the problem of northbound APIs in its private cloud, Schuberg Philis has integrated Nicira’s technology with CloudStack, the open source cloud orchestration framework created by Citrix Systems. The integration allows the company to create and manage a multi-tenant network in its private cloud.

“With a cloud management system we can create multiple tenants, and every tenant has ability to create several networks,” Prippaers said.

“We’ve integrated the Nicira solu-
tion so at the moment CloudStack provides you with a network, and it [uses] an API of Nicira to create a logical switch. Then every virtual machine that gets booted into the network will be assigned a logical port and connected to the virtual switch.”

PROGRAMMABILITY WITH PROPRIETARY SDKS HELPS, BUT SDN IS BETTER

Network vendors have tried to offer some level of programmability for years, often through software development kits (SDK) built on top of their operating systems. Cisco’s SDN strategy, for example, includes One Platform Kit, an SDK planned for all of its networking gear that will allow for programmability.

But Salisbury doesn’t want a programmable cloud network based on “proprietary APIs on proprietary software running on proprietary hardware.”

“With OpenFlow, you now start to have better definition and more controllability over the forwarding plane,” Salisbury said.

He wants vendors like Cisco and Juniper to open up their boxes completely to OpenFlow and give customers the freedom to build the networks they want.

Salisbury said that Google didn’t wait around for this and built its own OpenFlow gear, including switches and controllers.

SOME DOUBT THE SDN CENTRALIZATION CONCEPT

The industry has also been conservative with OpenFlow support because of lingering questions about the centralization of the control plane in SDN. Some vendors and network engineers question both how scalable and how secure centralized control can be.

“Some vendors say we have to stay distributed because centralization will never work,” Salisbury said. But a centralized controller-based network seems to work just fine in the wireless LAN market, he said. To Salisbury, today’s network architectures are too complex to serve the needs of a private cloud environment.

“We’ve taken the architecture of the Internet and stuffed it into enterprise networks,” he said. “We’ve taken this huge stack of protocols, and this huge distributed computing model, and said, ‘OK, this works for hundreds of thousands of autonomous administrative domains. Let’s put the same thing inside one administrative domain.’ It makes it so complicated. I think [SDN is] inevitable. We’re 10 years behind, and we’ve got the road map. The only question is, can we do it faster than the x86 market did?”
SOFTWARE DEFINED NETWORKING GOES WELL BEYOND THE DATA CENTER

With SDN, network engineers will eventually be able to improve security, management and application performance in the LAN and WAN—without costly hardware.

BY MICHAEL MORISY

SOFTWARE DEFINED NETWORKING (SDN) is already changing the data center network, but now the technology could redefine other parts of the network, as well as the network engineering profession itself.

A host of start-ups, academic researchers and other network gurus are exploring the powerful flexibility and programmability of SDN for strategies to make the LANs and WANs of tomorrow simpler to manage, more secure and more powerful than ever before.

At the forefront of many SDN researchers’ minds is security, particularly in environments that already rely heavily on virtualization. SDN will offer better control over network traffic, allowing engineers to differentiate network access for users in order to identify and separate bad actors or simply incompetent users.

“What is talked about most is security and the ability to understand or customize hosts on your LAN network,” said Mat Mathews, co-founder of Plexxi, a networking start-up betting heavily on SDN advances.

Today, those capabilities are vendor dependent. Cisco and Juniper, for example, have gone to great lengths to bake security into their networking hardware, but these solutions don’t necessarily integrate well in a mixed-vendor environment. Nor do these capabilities translate well if you want to manage your security through a third-party vendor that doesn’t partner with
your switching provider. That will change if open, standardized SDN catches on.

**TOWARD A UNIFIED SDN SECURITY SOLUTION**

Researchers are currently exploring how to use SDN to provide segmented, virtualized networks based on the characteristics of the connecting device, such as IP or MAC address. This would allow companies to give authorized users full network permissions while connecting guests to a completely partitioned network that restricts their access to file shares, printers and other sensitive areas.

SDN could also help find and eliminate threats that come from within a network, whether it’s a cloud provider working to prevent malicious users or a university campus trying to stem the tide of a nasty virus. This was one of the exciting avenues of research for Ben Cherian, chief strategy officer of Midokura.

“Let’s say that a DDoS attack is originating from your [public] cloud, and you have no idea who is doing this. You can handle that by having physical people watching the network … or you could set rules on your network, and say ‘I am going to tap all the traffic on my cloud, and if I see something abnormal, I’m going to programmatically shut down the tenants that are abnormal,’” Cherian said.

The latter option not only requires fewer staff, but it scales up more easily. It also leaves network security less prone to human error. Midokura has already developed and deployed a port mirror that clones traffic for analysis, allowing increased security without compromised speed.

**SDN OFFERS UNLIMITED POTENTIAL IN NETWORK SERVICES AND APPS**

As SDN advances, it will enable new applications that are unimaginable today. Instead of buying firewall or WAN optimization appliances, for example, enterprises could work with start-ups that are developing alternative SDN applications that can be installed and scaled on a virtualized network.

Kyle Forster, cofounder and vice president of Big Switch Networks, is building the company around that very idea. “We have 15 apps in the pipeline,” including a firewall, he said. But what’s exciting are the new capabilities SDN applications will have in monitoring and redirecting network traffic in real time.

“The wonderful thing about having a programmable Level 2/Level 3 network is that if you’re a Level 4 or Level 7 application provider, you can do a small adjustment to get the right packets to [your appliance] at
the right time,” Forster said. That’s a level of direct access that used to require pricey, specialized hardware investments. In time you could implement these capabilities on an SDN network quickly and inexpensively, dramatically changing the speed and flexibility of how networks are managed.

**RETHINKING THE SPEED AND STYLE OF NETWORK ADMINISTRATION**

While being able to access data streams in new and innovative ways could provide a wealth of new networking applications, the most lasting change could be in how networks are managed—and the skills required to manage them.

“As networking gets more integrated into the virtualized part of IT, the software people will be running things,” said Dan Pitt, executive director of the Open Networking Foundation. “If people can write automatic scripts for configuration and dynamic management, they don’t have to get their fingers dirty with ports and VLANs and other problem areas.”

That doesn’t mean the network engineers of the future should forget everything they learned studying for the CCIE and start brushing up on their Python (yet). It could mean that they should start thinking about new services that can be delivered and have a positive business impact. With the right frame of mind, engineers could help move the network from being a cost center to a business driver.

“We like to say, ‘What can we do to make network engineers heroes again?’ It’s been a long time since we’ve seen that,” said Forster. “[SDN] increases their ability to grab applications when they need them to make their networks more useful.”

Plexxi’s Mathews echoed that assessment. “What has happened is that the toolkit available to sys admins to maintain, operate and orchestrate compute resources has expanded,” Mathews said. “They’ve changed their position to be more like DevOps.”

So what can forward-thinking network engineers do to prepare for the coming wave of SDN? “I would counsel them to be the advanced scout for their enterprise; show their enterprise how they can exploit SDN and do it [in] conjunction with the current installed base,” said Pitt. “Some [networking] jobs will be going away, and the people who lead the charge in how you [transition] in a productive way will be the ones the enterprise want to retain.”

Staying open-minded might not hurt, either. “I don’t think the network is going away or this role is going away, but there’s a different breed of person who needs to manage it,” said Cherian.
WHY IS SDN THE VENTURE CAPITALIST DARLING?

It has been at least a decade since the network has seen technical innovation and new venture investment, but SDN has changed all that. By Rivka Gewirtz Little

In a tough economy, venture capital dollars don’t flow easily. So the fact that software defined networking (SDN) companies aren’t having a problem getting funding says something about how disruptive investors expect the technology to be.

Venture capitalists are willing to take a chance on SDN because customers have made it clear that they need a new network strategy to handle server virtualization and complex cloud environments, says Mike Volpi, a partner at Index Ventures. Index was one of the first firms to put a check in the bank account of Big Switch Networks, now considered an acquisition target since its lead competitor Nicira was snapped up by VMware last summer.

But while the VM-

Why are venture capitalists investing in SDN right now?
[The reason we decided to invest in] the SDN opportunity almost two years ago fundamentally came
from the belief that networking as it stands today isn’t working quite right for customers. SDN offers a range of unique ways in which to address those customer issues. Probably the most important [factor] was that SDN offers far better programmability of the network, particularly in the data center world. But it also has potential in almost every part of the networking world. In SDN, the controller essentially acts as a platform layer, which allows networking applications to operate across a multitude of different switches and networking environments uniformly. SDN also has the opportunity to more closely bring together the traditional hard switch world and the virtual switch world, which is really a software task.

**Cisco has such a large hardware installed-base. Do you see SDN replacing existing hardware, or will it play into the existing infrastructure?**

It definitely won’t replace the hardware. We still need those switches. SDN acts as a layer above those switches. [But currently] applications reside as extensive software inside those switches. SDN allows network operators to abstract out [the software and applications] into the SDN layer. It allows for simplification of this very broken up network architecture.

**But isn’t it the case that for an SDN layer to work, traditional vendors like Cisco will have to support OpenFlow or some other common, open standard? Is there concern in the investment community that their lack of willingness to standardize will inhibit innovation?**

Not really. The lowest hanging fruit is the virtual switch market, which is not much of a play for Cisco. Also, there are a lot of other network vendors that do support OpenFlow. HP has been positive about it; Juniper has shown keen interest; and others, including Extreme and Dell, have also shown interest. In the beginning, Cisco said it wasn’t going to happen, but now they are saying, ‘We already do that and have been doing it for a while.’ I think Cisco will probably be a relatively reluctant participant, but at some point in time, they too will [support] this.

**Do you believe that OpenFlow must be the protocol behind SDN?**

I don’t think there is any mandate as to what specifically the protocol is. The nice thing about OpenFlow is that it is open source, so it’s a level and fair playing field for everyone. The protocol itself has an interesting specification to it, but it’s not rocket science. The idea of SDN is bigger than OpenFlow. Ultimately if there are variants or newer versions of OpenFlow, that’s fine. The...
key idea is to abstract the software out of the switch or router and put it into the server environment.

**What does the VMware-Nicira acquisition mean to the rest of the SDN market? What does it mean for Big Switch, which has similar technology?**

The highlight is that the value that was placed on Nicira accentuates how real and how credible SDN has become. I think the acquisition definitely fortifies the market movement toward SDN. Obviously now VMware is a step ahead because of its commitment to SDN. But other vendors will be equally keen on supporting it, so I think it’s a step forward. Big Switch and Nicira had a similar heritage and some elements overlapped, but I think they’re different enough that we are confident at Big Switch about our approach.

**How does Big Switch differentiate from Nicira or a newer start-up like Plexxi or Midokura?**

From day one, Big Switch was very focused on being able to serve both the hard switch and the virtual switch market. We think that for a lot of customers, being able to bridge the two worlds is very important, and that’s a critical point in the architecture and the controller. We also use true open source, which has been very successful. The product is Java[-based], which has given us flexibility, and which Nicira has done differently. We have also taken a partnership-oriented strategy where we integrate into their ecosystems. Relative to the other players, our heritage out of the original OpenFlow work at Stanford, and the fact that we’ve spent two years developing product and working with customers, gives us a unique position in the marketplace. We have the expertise and the know-how both technically and with customers.

**In the big picture, SDN is going to be part of multiple different parts of the network in multiple different ways.**

Looking at the SDN market as a whole, will a lot of the action be driven by applications, such as firewall management, as opposed to an overall network virtualization architecture?

In the big picture, SDN is going to be part of multiple different parts of the network in multiple different ways. While Big Switch is focused mostly on the enterprise, a lot of
service providers are interested in doing tunnelling and traffic-engineering techniques. Then you have a wide range of other applications, from load balancing to firewalling, that are thought of as enterprise or data center applications.

Applications are what make the SDN market transformational, not just technically but for the industry. This is an industry that has been inside that piece of hardware vertically integrated, with every vendor working up and down the stack. The SDN application really opens up the universe. You don’t need to go to the box to do a firewall or traffic engineering.

Secondarily, you can think of your network as a singular system rather than having to implement services in a box on the network. Your firewall no longer has to be placed in this little location. Firewalling becomes an abstracted process that you can manage from a policy perspective and then implement it as you see fit.

That opening of the ecosystem to app developers and the universality with which you can [direct] the services in the network make it extraordinarily powerful. That’s the true vision of SDN.

**Is there concern that there is a lot of activity around point products and less so around the overall architecture change?**

It’s not atypical in an early-days market for vendors to grab onto different small pieces. I think as the market evolves, there will be broader solutions. At Big Switch we focused on a universal platform and then having applications reside on it. But SDN is such a comprehensive technology that solves many different problems, you’re going to find lots of companies jumping into one corner of it. That’s going to happen for a while.

**Will there be a shortage of SDN-savvy engineers to support market growth?**

I don’t think so. This is not necessarily a situation where every engineer that used to work at Cisco can transition over, but I do think there are plenty of engineers that come from the virtualization universe that are very knowledgeable and can be leveraged to do this. Also, there are plenty of people with good solid software knowledge. Certainly from Big Switch’s perspective, there hasn’t been a shortage of top people that want to come work for us.
David Davis is a virtualization evangelist at TrainSignal.com, the global leader in video training for IT pros. He holds several certifications including VCP5, VCAP-DCA, and CCIE #9369. He has been awarded the VMware vExpert award three years running. Additionally, Davis has spoken at major conferences like VMworld and authored hundreds of articles for websites and print publications, mostly around virtualization. Davis has authored 10+ video-training courses at TrainSignal including vSphere 5, vSphere Troubleshooting, and vCloud Director Essentials.

Tom Nolle is a strategic egghead—someone who first wants to know the truth, no matter what it is, and then wants to explain it in a way that reaches everyone who cares to know it. He’s an analyst in telecommunications, media and technology, and a former software architect who now works to blend technology detail and business reality. He has more than 30 years of experience as an author and analyst, covering the most complicated and important developments in the industry. Nolle is president of CIMI Corp., a strategic consulting firm specializing in telecom and data communications since 1982. He is the publisher of Netwatcher, a journal addressing advanced telecom strategy issues.