PIONEERS AND GIANTS: INSIGHTS ON THE FUTURE OF NETWORKING

At VMware's inaugural, invitation-only future:net event, industry pros and thought leaders explored the current and emerging landscape for software-defined networking and more.

Introduction: Setting the Scene

As digital business becomes increasingly important in almost every industry, enterprise IT managers are challenged to deliver infrastructure that is agile, secure, and constantly available. To cope with these challenges, data centers are undergoing a once-in-a-generation architectural shift, from hardware- to software-centric models. Just as virtual machines supplanted physical servers as the fundamental element of modern server applications, software-defined networking (SDN) is now emerging as a more flexible, manageable way to organize a data center's network needs.

SDN can create far greater manageability by enabling network managers and developers to access network resources at a programmatic level, treating network resources in much the way they treat other computing resources such as central processing units (CPUs) and memory. SDN can provide far more detail on what's actually happening within large data centers, which has been difficult for network managers to achieve with older network models. It can enable networks to become easier to scale up or down, shorten setup time, increase security, and reduce costs. And it can take advantage of programmable network hardware, enabling managers to change the behavior of network devices through software upgrades instead of expensive hardware replacements.

> "In 10 years, I've never seen such an assembly of networking talent on stage."
>
> — Martin Casado, Cofounder, Nicira; General Partner, Andreessen Horowitz

However, SDN adoption has progressed slowly in most enterprises because it requires network admins to adopt new skill sets and new ways of thinking. Consequently, it's seen the most uptake to date in the biggest data centers, such as those used by giant cloud providers including Microsoft Azure and Google Cloud Platform. The industry needs to expand the array of SDN tools available and educate network managers on their uses and benefits before SDN can expand to a wider range of enterprises.

Although experiments in SDN date back to the 1990s, many people trace the origins of modern SDN to work done by Martin Casado at Stanford in 2006. Casado, together with Nick McKeown and Scott Shenker, founded Nicira the following year; it quickly became one of the leading SDN companies, creating the technology of network virtualization. In 2012, VMware acquired Nicira for $1.26 billion.

Martin Casado, General Partner, Andreessen Horowitz

Today, SDN is much bigger than any one company. In 2016, 10 years into the SDN revolution, the pioneers of the field gathered, together with some of the biggest names in network technology, to assess the state of networking and to figure out where it needs to go next.

> Speakers returned again and again to the challenge of effective management and the sheer difficulty of getting workable data out of a network.

McKeown and Casado delivered speeches that bookended the first-ever, invitation-only future:net conference, held August 31–September 1 in Las Vegas. In between, about 200 attendees took in technical presentations on the networking technologies deployed by today's giant cloud providers, the future of data-center networking, various open-source initiatives underway in SDN and network virtualization, and the rise of container-based networking.

"In 10 years, I've never seen such an assembly of networking talent on stage," Casado, now a general partner at Andreessen Horowitz, said at the end of the conference, reflecting comments made by many others, both onstage and offstage, during the event.

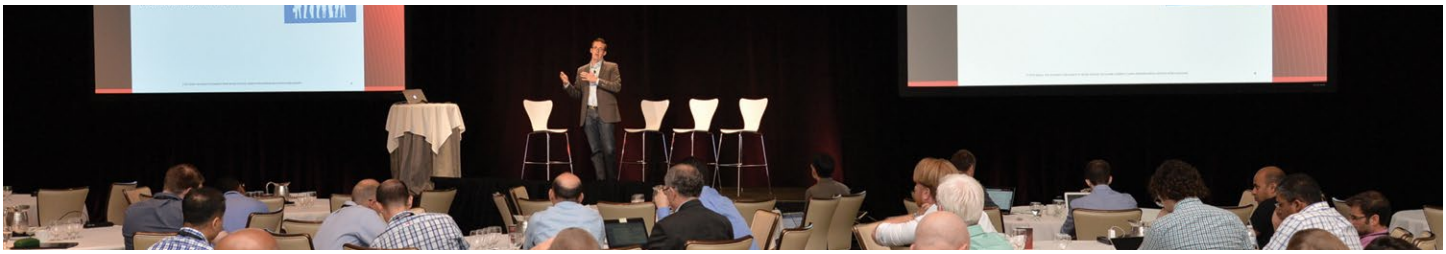
Several common themes arose from the two-day agenda:

- Network-management tools need to improve.
- Networking needs abstraction layers comparable to those in computing.
- Moore's Law is enabling a higher degree of programmability in network hardware.
- Network security is an ongoing concern (and one that SDN can help address).
- Open-source efforts are driving considerable innovation in networking.

Future:net Speakers, Session Chairs, and Moderators

Guido Appenzeller, VMware*
Ethan Banks, Packet Pushers
Mark Bluhm, Thomson Reuters
Truman Boyes, Bloomberg
Martin Casado, Andreessen Horowitz*
Bruce Davie, VMware*
Stephen Dawson, SAP
Kenneth Duda, Arista*
Tariq Elliah, SAP
Inez Envid, Google
Greg Farro, Packet Pushers
Ali Iloglu, Citi*
Sukhdev Kapur, Arista
Tobi Knaup, Mesosphere
Bryan Larish, Verizon
Scott Lowe, VMWare
David Maltz, Microsoft
Kyle Mestery, IBM
Nick McKeown, Stanford University & Barefoot Networks
Suneet Nandwani, eBay*
Justin Petit, VMware
Ashwin Raveendrannair, eBay
Anees Shaikh, Google
Ian Shakil, Augmedix
Rob Shakir, Jive
John Spiegel, Columbia Sportswear
John Veizades, Google
Madhu Venugopal, Docker
Subbaiah Venkata, Google
David Ward, Cisco*

*Also on future:net Steering Committee, along with Albert Greenberg, Microsoft; Rob Sherwood, Big Switch Networks; Marianna Tessel, Docker; and Amin Vahdat, Google



Network Monitoring and Management

One topic that came up repeatedly throughout the conference was the ongoing need for more effective network-monitoring and network-management tools.

It's not for lack of trying: the networking industry has been attempting to improve network management for at least three decades, including efforts such as the Simple Network Management Protocol (SNMP). Such tools haven't exactly solved the networking world's problems, due to scaling and performance limitations, inconsistent implementation, and the lack of effective abstractions.

In short, the major tools for monitoring and debugging network problems remain command-line utilities including ping and traceroute or packet-capture tools such as Wireshark. These tools provide only limited detail and low-level abstractions, making it difficult for network managers to find out what's actually going on in sometimes extremely complicated networks.

Nick McKeown, Cofounder/ Chairman, Barefoot Networks; Professor, Stanford University

That's unacceptable, McKeown said in his kickoff keynote. Packet-level monitoring and management "should be a natural part of the way networks are built—and, in fact, we should scream bloody murder until it is the case," he said. "We should be able to inspect any packet at any point."

Currently, it's difficult for a network manager to tell exactly which switches and routers a data packet traveled through while navigating a complex network. McKeown, now cofounder and chairman of Barefoot Networks and professor of electrical engineering and computer science at Stanford University, suggested that network managers ought to be able to inspect any packet and extract data that would answer several key questions. These include:

- What switches did it visit to get here?
- What rules did it match in each switch?
- What version of the rules table was used?
- Which queue did each switch put our packet in?
- How long did it wait there?

Indeed, solutions to these problems are beginning to emerge. One is the "packet postcards" approach, in which every switch on a network generates a small, time-stamped data digest for every packet it handles, sending that digest to a central server for logging and later analysis. The other is called Inband Network Telemetry, in which switches add state data to every packet's header as it passes through the switch, enabling later analysis by examining the data trail contained in those headers. Both approaches have downsides, as McKeown pointed out. But as network hardware grows in computational power and throughput, they are increasingly feasible.

Speakers returned again and again to the challenge of effective management and the sheer difficulty of getting workable data out of a network. When running cloud-scale networks such as the data centers for Microsoft Azure, for instance, merely identifying problems becomes a significant challenge. In a session featuring the Internet's "Cloud Titans," David Maltz, who leads Azure's Physical Network team at Microsoft, described several tools that the company had built to address these problems. Those tools include a "PingMesh" view that shows a graphical depiction of how well data is traveling between every server in the network.

> Representatives from eBay, Google, Docker, and Mesosphere all addressed the need for network-virtualization technologies to work in collaboration with containers.

Ultimately, Maltz and others are tackling these problems by redesigning their network architectures in more software-defined ways—moving to flexible (and data-rich) networks that can adapt to changing requirements, provide network telemetry to operators, and enable managers to fix problems more easily.

David Maltz, Azure Physical Network Team Lead, Microsoft

Networks Need Abstraction Layers

In computing, different levels of abstraction make it possible for people to write software or control computers without having to understand a CPU's machine language or the wiring of its circuits. Because this principle is well understood in computer science, it works: you can program in PHP or Java, or you can use Assembler. Each successively "higher" layer of abstraction encapsulates a series of instructions encoded at a "lower" level.

For example, a Java programmer can work with named variables and complex data structures that involve a higher level of abstraction than the registers and memory locations an Assembler programmer would use—and assembly language is itself a higher level of abstraction than the binary signals implemented in a CPU's circuitry. What's more, you can peel away each layer of abstraction analytically, proving that each successively higher layer is functionally equivalent to the functions or processes it abstracts.

That's not the case in networking, as McKeown pointed out in his keynote—an observation that was echoed many times during the rest of the conference. There is a level of abstraction for the data plane in networking, but not for the control plane, which means that it's impossible to control or modify a network without getting your hands dirty with routers, switches, patch panels, and protocols.

> "The idea that the enterprise can protect a boundary is nothing more than sheer stupid repetition of Troy."
>
> — Simon Crosby, Cofounder and CTO, Bromium

As McKeown put it, quoting his Nicira cofounder, Scott Shenker: "The people who run networks today have to keep a superhuman amount of 'state' in their heads, so [networks] are run by 'masters of complexity.'"

In addition, this lack of abstraction enforces a "bottom-up" approach to network design: you start with a switch, which has a fixed set of functions; then you work upward via its application programming interface (API) to implement the network functionality that you want.

Throughout the summit, many speakers discussed the advantages that SDN could bring in creating higher levels of abstraction for networking. Ideally, you'd be able to start with a specification for the network behavior that you wanted and then instantiate that behavior in some kind of high-level network-control language. That program could then be compiled into code that could run on a programmable switch, much as Java programs today are compiled to run on CPUs. Such a programming language is beginning to emerge from the world of SDN, and it's called P4.

During the "Cloud Titans" session, Ines Envid and John Veizades, who are both product managers responsible for networking at Google, described their company's efforts to build layers of abstraction and programmability into its cloud data centers. Google's Andromeda is an SDN management layer that gives managers access to all necessary network functions via a central control panel, and it enables Google to treat its many cloud data centers as one, uniform network fabric—albeit one with many terabits per second of throughput and millions of virtual machines.

Moore's Law Comes to the Network

For networks to be programmable through higher levels of abstraction we will need programmable networking hardware—and that's exactly what many companies are currently developing. Moore's Law—which states that the number of transistors per square inch on an integrated circuit doubles roughly every two years, thus increasing computing power per dollar at the same rate—is at last enabling a greater degree of programmability in networking devices than ever before, McKeown explained. And in contrast to earlier generations of programmable switches, modern programmable switches use application-specific integrated circuits (ASICs) that can maintain blinding levels of performance and data throughput.

Many companies are taking advantage of this performance dividend to build more programmability into their networks.

In the "Cloud Titans" session, Microsoft's Maltz described his company's efforts to create an open-source firmware for programmable switches. This effort includes two components: an API layer, called the Switch Abstraction Interface (SAI), which enables people to create firmware for network ASICs, and open-source firmware code, called Software for Open Networking in the Cloud (SONiC), that works with the SAI.

For programmable switches to be usable, however, they'll need programming languages and abstraction layers such as APIs. Kyle Mestery, an open-source cloud-computing architect for IBM, and Justin Pettit, a senior staff engineer

for VMware, addressed that issue in a session on open-source solutions for SDN. Mestery and Pettit described their joint efforts to build Open Virtual Network (OVN), a network virtualization layer for Open vSwitch (an open-source switch standard).

During an onstage audience Q&A, Google's Veizades welcomed the prospect of truly programmable network hardware, saying that it would make building generic solutions to broad problems much easier. Maltz, for his part, was more cautious, worrying that programmable hardware could introduce complexity into networks, thereby increasing the sources of failure or confusion, unless it was paired with a very simple, robust, widely accepted model of switch functions.

And yet change doesn't happen overnight. "We still purchase dumb routers that cost $5,000 and only do default routing," said John Spiegel, global IS communications manager at Columbia Sportswear, during a session on next-generation networking. Spiegel described his struggles to get his company to embrace an SDN approach that would make it far faster and easier to roll out new branch offices. Despite the advantages, SDN has proven a challenging sell because it requires new skills and new ways of thinking.

Bryan Larish, chief IT and networks architect at Verizon, talked about the need to "prepare the runway" and get people used to the new, software-defined way of doing things. "That skill-set shift is not going to happen overnight—and I think that's okay," Larish said during a session on open-source solutions.

Security and the Promise of Microsegmentation

Security is an enormous, ongoing concern for network managers. Network virtualization can help by making networks more compartmentalized and more manageable.

> Rather than trying to protect a nonexistent perimeter, network managers need to look at protecting their networks by giving each application a defined set of behaviors—something more easily doable and enforceable in the SDN era.

Among the biggest sources of network security vulnerabilities is their complexity. Someone forgets to update a password on a little-used, special-purpose router in a secondary data center, and hackers soon discover it's a back door into the whole organization.

Illustrating how network virtualization can beef up security, Thomson Reuters' Mark Bluhm, who runs global data centers for the news and information company, discussed how his company is embracing cloud services to use and manage its enormous global network more efficiently. Speaking in a session on next-generation networking, Bluhm estimated that about 12,000 changes are made to the company's data-center networks every month—and that 8,000 of those are related to fixing security issues.

In another discussion, on the conference's second day, during a live, onstage recording of a Packet Pushers podcast, panelists discussed how microsegmentation of networks can provide security benefits, similar to how putting applications in their own virtual machines (VMs) helps security. If each VM is confined to its own virtual network, and the only traffic that is allowed on that network is defined by what the VM and its application are supposed to be doing, that provides a way of containing any possible intrusions. Hackers who manage to penetrate the application or the VM will only be able to get as far as the virtual network it's connected to. Microsegmentation of networks can go hand in hand with the push among developers and operations teams to embrace containers.

Representatives from eBay, Google, Docker, and Mesosphere spoke during a containers session on the conference's second day, and they all addressed the need for network-virtualization technologies to work in collaboration with containers. Ideally, network resources should be just as programmable and configurable as any other resources in a container, but this isn't yet the case. However, the speakers agreed that reaching that point will bring an additional security benefit by helping to minimize any container-associated breaches within virtual networks.

Marianna Tessel, EVP/Strategic Development, Docker

The container panelists also agreed on the importance of making network configurations simple so developers can more easily incorporate security into their containerized applications from the start. For example, if two containers need to "talk" to one another, it should be easier for developers to create a simple virtual network between the two—and to only allow the actions on that network that their applications actually need. This is another, developer-centric route to achieve microsegmentation of networks.

Simon Crosby, the cofounder and CTO of Bromium and a panelist in the "Packet Pushers" podcast segment, talked about the futility of enterprise-perimeter defenses in the modern world. "The idea that the enterprise can protect a boundary is nothing more than sheer stupid repetition of Troy," Crosby said; idea that the enterprise can protect a boundary is nothing more than sheer stupid repetition of Troy" -his statement referencing the legend of the Trojan Horse was widely tweeted and retweeted by conference attendees.

In the modern enterprise network, there is no perimeter. Endpoints are everywhere: mobile devices, apps, browsers, even the Wi-Fi network at your local Starbucks. Rather than trying to protect a nonexistent perimeter, network managers need to look at protecting their networks by giving each application a defined set of behaviors—something more easily doable and enforceable in the SDN era.

The State of Open-Source Networking

The promise of open-source efforts for advances in networking is coming to fruition in OpenStack, with its approach to delivering infrastructure as a service (IaaS). OpenStack now comprises a large set of open-source technologies for programmatic provisioning of compute, networking, and storage resources, and it's managed by a consortium of companies that contribute to its many components. Certainly, there have been some questions within the industry about how complete and usable OpenStack is, and its rate of adoption has been slower than many expected. But it was clear from this conference that OpenStack is alive and well in many large data centers, such as those operated by eBay, SAP, and Verizon.

However, not every network manager onstage had seen success with the open-source project. Thomson Reuters shut down a pilot project with OpenStack last year after finding it wasn't meeting its needs, Bluhm noted in the next-generation networking session. Even OpenStack early adopter eBay showed a telling slide of all the things that the company doesn't get from OpenStack (about 90 percent of the services an application needs).

Several related open-source networking efforts received attention, including OpenConfig for network-device management, the addition of OpenStack-related APIs to networking equipment, and the increasing capabilities of Open vSwitch (OVS) and Open Virtual Network (OVN). With the added capabilities of these projects, it may be that OpenStack (and open-source networking, more broadly) is now reaching the point where it is truly ready for deployment in typical (that is, non-cloud-scale) enterprise networks.

Combined with the rise of containers and their concomitant need for container-based networking, a new generation of container-friendly OpenStack solutions is just around the corner. These new solutions could, in turn, boost the project—which is already in wide use for some of the largest data centers—into the realm of more widespread enterprise adoption.

Bruce Davie, Chief Technology Officer, VMware

Guido Appenzeller, Chief Technology Strategy Officer, VMware

Conclusion: Looking Ahead

The future of networking is clear, in broad terms: networking will follow a path toward increasing virtualization, just as compute and storage did before it. With virtualization will come more flexibility and programmability, as well as the potential for whole new classes of network features. Network management—a dream long deferred by the impracticality of previous solutions—may finally reach maturity. Most important, network properties will be definable at higher and higher levels of abstraction, freeing network administrators to create more robust networks and enabling software developers to treat network resources the way they treat other computing resources.

But how we get there is still unclear. Broad trends are emerging on the network-management side, with the rise of an array of open-source efforts including OpenStack, OpenConfig, and OVN/OVS as well as programmable switches and routers, in addition to a growing crop of management and monitoring tools. Containers are spurring their own reinvention of networking from the software-developer side, bringing with them the need for easily programmable network resources.

Exactly how these two needs will converge remains to be seen, but one thing is certain: the deeper computation extends into the network, the more security, power, and flexibility networks will offer to all of us.

Combined with the rise of containers and their concomitant need for container-based networking, a new generation of container-friendly OpenStack solutions is just around the corner.

For More Information

For additional insights from the future:net conference, read VMware CTO Bruce Davie's blog post on the event, and see the media coverage by Networking Computing and SDxCentral. To learn more about SDN and network virtualization, see VMware's Radius magazine.

About MIT Technology Review Custom
MIT Technology Review Custom produces world-class print, online, and live-event solutions that align clients with a trusted 117-year-old brand.
www.technologyreview.com/media