IDC ANALYST CONNECTION

Rohit Mehra
Vice President, Network Infrastructure

Nolan Greene
Senior Research Analyst, Network Infrastructure

Software-Defined Network Architectures: A Key Building Block for Digital Transformation

January 2017

As enterprises embark upon digital transformation (DX), IT decision makers are realizing the need for network infrastructure that can support myriad digital initiatives that can include expanded enterprise mobility programs, Internet of Things (IoT), and increased internal application development, all at scale. These efforts are taking place against a backdrop of explosive data growth and a growing, more sophisticated security threat landscape. To address these trends proactively, enterprise IT is increasingly looking to cloud-enabled, software-defined network (SDN) architectures that allow for automation, network domain unification, and real-time context from a security standpoint. Ultimately, these features can allow enterprise IT to move from focusing on "keeping the lights on" to directly working toward achieving business goals.

The following questions were posed by Cisco to Rohit Mehra, vice president of IDC's Network Infrastructure group, and Nolan Greene, senior research analyst in IDC's Network Infrastructure group, on behalf of Cisco's customers.

Q. Why is SDN becoming important to the enterprise campus and branch networks?

A. SDN architectures have been validated in many datacenters as enabling network automation and programmability, reducing time to deployment, aiding security and policy enforcement, and lowering the amount of time network operations staff spends on manual and reactive tasks. SDN also reduces the chance of manual errors while potentially lowering opex overhead. These same benefits translate well to enterprise campus and branch networks.

Because SDN can decouple software functions from the underlying hardware taking on the form of a controller or network fabric, it plays well into the increasing desire of some enterprises to better align their applications with their network resources and to leverage unified management of network elements such as wired and wireless LAN. SDN lends itself well to "single pane of glass" network management visibility and the ability to uniformly enforce policies and have a more efficient network management experience. Overall, SDN promises to reduce the amount of time it takes to deploy, adapt, and secure enterprise campus and branch networks while providing the means to scale faster with fewer resources.

Q. What are some of the pain points that software-defined network architectures can address for today's network managers?

A. The most prominent pain points that SDN can address in the enterprise campus and branch include deploying and managing multiple complex VLANs, managing disparate networks, and scaling the network on legacy infrastructure. As mentioned, SDN can help unify different elements of network infrastructure (e.g., LAN, WLAN, WAN) through unified policy enforcement and visibility. Additionally, SDN architectures can enable integration among network domains (from cloud and datacenter to campus and branch). Many network managers believe that scaling legacy networks is an arduous process and expect the automation and programmability benefits of SDN to reduce the complexity of network scaling.

It can be said that in sum, network managers are pained by the amount of time spent "keeping the lights on" and reacting to problems on the network versus the amount of time they could be spending on innovative network initiatives, collaborating with line-of-business (LOB) leaders to create new business opportunities through the network.

Q. Why is unified networking (wired and wireless and WAN) becoming more necessary in the DX era?

A. Not so long ago, the concept of unified wired and wireless network management was not top of mind for network managers, with wireless perceived as an "overlay" to the wired network. Mission-critical devices and applications were typically deployed on wired LANs, with WLANs functioning more as a complementary network for guests or less integral use cases. In today's digitally transformed campus and branch, wireless is often the primary connectivity method for most mission-critical applications, while wired access plays an important secondary role. Thus, it is imperative to be able to enforce the same rules and policies and guarantee consistent quality of service (QoS) as users may alternate between wired and wireless.

At the same time, network managers need to be able to visualize all wired and wireless network activity in one place to ensure the network is running smoothly and to be able to detect problems faster. With the proliferation of public cloud applications and the recognition of the need for distributed organizations to have standardized, secure WAN connectivity, the WAN has risen to prominence and is considered a key aspect of enterprise network infrastructure. Unified WAN policies are equally important, and there is a need to define policies once and have them follow the user. These integrations — enabled largely through SDN — and the resulting management efficiencies ease scaling, reduce manual tasks, and ultimately help reduce operational complexities.

Q. What can software-defined network architectures enable in terms of contextual data and analytics?

A. The network has an unprecedented ability to generate valuable data about its nodes and users and the applications that traverse it. Network probes have long collected data about traffic, trunking, devices, and network-layer software. However, the generation of usable data from these probes has often been disjointed and lacking proper context. There is a need to correlate network data with IT and business objectives and to do so in a seamless end-to-end manner in real time. Among the areas in which SDN can leverage data analytics and visibility better are security and policy enforcement, change management, workload scheduling, and problem and event management.

Q. What are some of the IT and/or LOB initiatives that stand to be aided by software-defined network architectures?

A. A major element of software-defined network architectures is the use of application programming interfaces (APIs) to allow communication and integration among network and security devices, infrastructure, and applications. APIs also enable native development of network applications aimed at business objectives without silos between network teams and software development teams. APIs ultimately can lead to faster innovation through decreased time to service, without compromising security.

SDN also shows promise to reduce pain points with regard to emerging IoT initiatives such as deploying smart lighting, signage, industrial sensors, and other use cases, which will bring a multitude of new endpoints onto enterprise networks. Manual configuration and provisioning would be time consuming, error prone, and impractical for bringing IoT devices and applications onto the network. The automation and programmability associated with SDN should allow for automated provisioning of IoT devices with the appropriate security and access policies enforced without manual intervention. As recent botnet attacks have demonstrated, there is significant room for error in enforcing IoT security and dire consequences for failing to so.

Increasingly, the network does more than just support the enterprise. Rather, it is the backbone of the enterprise that allows products and services to be delivered. Nearly all future enterprise initiatives depend on a network that not only is agile, scalable, and cost efficient but also can bring new services to bear quickly. IDC believes that SDN is a necessary innovation for enterprises to experience true digital transformation.

ABOUT THESE ANALYSTS

Rohit Mehra is vice president of IDC's Network Infrastructure group, leading IDC's research practice in Enterprise and Datacenter Networks and Telecom Infrastructure. He provides expert insight and analysis into global industry and technology trends as they relate to enterprise, datacenter, cloud, and telecom networks including areas such as Ethernet switching, routing, wireless, application delivery, and WAN optimization, among other technology domains.

Nolan Greene is a senior research analyst with IDC's Network Infrastructure group covering Enterprise Networks. In this role, he is responsible for market and technology trends, forecasts, and competitive analysis in the Ethernet switching, routing, wireless LAN, and adjacent networking markets. While contributing to quarterly and yearly forecast and market share updates, he also assists in survey design and end-user interviews and contributes to custom projects.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com