IDC TECHNOLOGY SPOTLIGHT

Building the Cloud-Enabled Enterprise Campus to Meet Today's Network Needs

January 2015

Adapted from *Worldwide Enterprise Network Infrastructure 2014–2018 Forecast* by Rohit Mehra, Nolan Greene, Rich Costello, and Petr Jirovsky, IDC #248744

Sponsored by Juniper Networks

Reliance upon cloud applications for mission-critical business functions has heightened network requirements at the edge. Today, many enterprises seek a cloud-enabled enterprise campus network that seamlessly glues the network edge to the cloud. Enterprises increasingly require common converged networks that can recognize and support a diverse set of wired and wireless devices, applications, people, and "things" while seamlessly connecting them to the cloud, datacenter, or WAN. Connectivity must be pervasive, reliable, and scalable, given that it links telecommuters, branch and satellite offices, and corporate offices to cloud and/or datacenter resources. This Technology Spotlight addresses how optimization for cloud applications is critical for modern enterprise network infrastructures and discusses the role that Juniper Networks plays in this important market.

Introduction

IDC is observing a sea change in technology that it has termed "the rise of the 3rd Platform." Whereas the 1st Platform represented mainframe computing and the 2nd Platform represented the client/server paradigm, the 3rd Platform is centered on four major pillars: big data/analytics, cloud, mobility, and social business. Each 3rd Platform pillar is highly interconnected and relies heavily upon the network.

Whether or not enterprise IT managers are familiar with the term "3rd Platform," most are feeling the impact of the 3rd Platform on the network. The network must now support a mix of applications and services, including unified communications and collaboration (UC&C), enhanced security, and myriad mobile applications. Mobility is perhaps the most salient trend challenging today's campus networks. The mainstream acceptance of "bring your own device" (BYOD) in the enterprise has resulted in employees routinely using personal laptops, smartphones, and tablets for business purposes. BYOD, in concert with growing numbers of corporate-owned mobile devices, has transformed the network's role in accomplishing mission-critical tasks. Mobile-enabled cloud applications (e.g., Office 365 and salesforce.com) break down barriers with regard to time and place, allowing employees to seize opportunities to create value as they arise. However, ubiquitous network support for mobility is needed to enable these "anytime, anyplace" workflows.

Further challenging the modern campus network is collaboration — that is, voice, video, and other multimedia applications (e.g., Microsoft Lync). With high-bandwidth requirements and absolutely no tolerance for latency and jitter, today's enterprise does not compromise on the network infrastructure's ability to support collaboration and multimedia. All of this is happening in a more lean and nimble era of IT. As network demands shift, the ability to easily make moves, additions, and changes becomes more critical. Today's enterprise seeks constant optimization from both a technical standpoint and a financial standpoint.

Taking place in the background of (and amplified by) the challenges of mobility and collaboration are initiatives to provide adequate network security for the mobile-connected enterprise while enabling robust security and policy-setting capabilities that protect sensitive data and ensure productivity in a BYOD world. Specifically, organizations must monitor for and prevent "shadow IT," a common term for the unauthorized use of IT applications in the enterprise or the use of authorized IT applications via unsecure access. Also, given the burgeoning ecosystem of mobile applications used to achieve business objectives and the propensity of workers who opt for their own choice of applications and other IT tools, secure enterprise mobile application delivery becomes a critical piece of a mobile security strategy. Furthermore, many verticals must accommodate the heightened industry-specific compliance requirements related to network and device security.

Finally, given that today's campus networks are increasingly mission critical in nature, IT should recognize the growing importance of business continuity and disaster recovery (BC/DR). In terms of campus networks, building resilience into the infrastructure will feature prominently in network upgrades and greenfield deployments. As enterprise IT increasingly turns to cloud services, cloud providers' service-level agreements will play a greater role in the decision-making process.

Market Trends: Prevalent Issues in Today's Enterprise Campus Networks

Enterprise Mobility Infrastructure

Today's enterprise campus networks need to be prepared to meet the 3rd Platform challenges of mobility, cloud, big data, and social business. However, many networks are built on legacy infrastructure that cannot accommodate the diversity of devices and applications, and the resulting security and policy implications, on today's networks. Not long ago, wireless networking served a complementary function to the wired network and was largely used for 1:1 laptop connections. Common 802.11a/b/g standards often provided adequate support for these use cases. However, with the explosion of enterprise mobility, 802.11n — and, increasingly, 802.11ac — is needed to support today's use cases. It is just as important to ensure that the underlying switching and routing infrastructure is also up to date; without adequate switch capacity, newer wireless access points will not be able to deliver maximum throughput.

Today, employees are commonly accessing the wireless network with three different devices. Moving forward, the advent of the Internet of Things (IoT) in the enterprise will add to the diversity of network endpoints that must be supported. The IoT not only will add endpoints to the network but also will increase complexity around the volume and variety of data transmitted over the network and will have vast security and management implications.

Also different in today's campus networks is the need to support wide fluctuations in network demand. In the days when stationary devices were the ones most commonly accessing the network, bandwidth and density needs were easy to predict. With mobility, demand on the network is more elastic and less predictable. Networks must be able to scale up or down in a seamless manner. At peak usage, the network infrastructure needs to be able to eliminate latency and jitter.

Management of Security and Access Policies

Given the greater diversity of connected endpoints across enterprises within nearly every vertical and segment, management of security and policy has elevated in importance. Visibility into user, device, application, and operating system through a single pane of glass is becoming table stakes in security and network management solutions. Similarly, the ability to activate security and policy settings as part of a comprehensive security and network management solution is also critical. Adding to the importance of single-pane-of-glass solutions is the fact that many security and networking departments are playing greater roles in the lines of business, but without a commensurate increase in resources, especially in regard to staffing.

Unified Wired/Wireless Networking

Along the lines of more efficient, single-platform network management is the growing trend of unified, end-to-end wired and wireless network management. Building off robust WLAN management platforms that have emerged over the past several years, unified wired/wireless management solutions offer common management for policy, security, and quality of service (QoS), with the ability to enforce application protocols for each respective area regardless of how the network is accessed. The potential benefits of single-pane-of-glass visibility include the increased ability to troubleshoot problems and mitigate security threats. This is especially helpful for lean IT departments.

Cloud Technologies Become Mainstream — Even for the Network

From software-as-a-service (SaaS) to hardware infrastructure solutions, cloud technologies have gained widespread acceptance for core enterprise IT functions. Many enterprises have adopted cloud-based applications for business-critical functions such as customer relationship management (CRM) or enterprise resource planning (ERP). Larger enterprises often build their own private clouds (datacenters) to host these applications. Given the application workloads and their mission-critical nature, IT must continually work to optimize the private cloud network infrastructure. Robust cloud-building solutions are key components, and deploying software-defined networking (SDN) technology for automation, programmability, and customization is becoming a common requirement.

In addition, cloud-based networking is an emerging approach to network provisioning, configuration, and management that leverages cloud capabilities. It enables a network-as-a-service (NaaS) model that can apply to routers, wireless LANs, firewalls, unified communications, and application delivery, as well as other network functions and services. While most of the attention on cloud-managed networking has focused on WLAN, IDC anticipates that the understanding of the benefits for other areas of networking will emerge slowly. Today's cloud networking platforms will be the foundation for future innovation in this realm.

Cloud-Enabled Campus Networks Across Verticals

Often thought of as a tool targeted toward small and medium-sized enterprises (SMEs), cloud-enabled networking shows promise for use cases across verticals and segments. Larger distributed enterprises may see a case for choosing cloud-enabled networking to better manage the entire network consistently from a central location. Cloud networking has also seen traction in higher education, hospitality, retail, and healthcare. However, given that lean IT is extending across verticals, and considering the growing trust in cloud networking's security abilities, we expect to see cloud networking gain steam in manufacturing, utilities, and financial services as well.

Transformative Potential of UC&C

3rd Platform trends such as mobility and social business are changing the face of UC&C while encouraging increased adoption. UC&C has transformative potential for the enterprise, bringing together and streamlining enterprise communication and collaboration with social business applications. Cloud-based UC&C solutions are growing in availability and adoption as well. When organizations are designing, upgrading, and/or deploying an enterprise campus network, it is imperative that they consider how well it can support UC&C. As mentioned, latency and jitter are unacceptable — UC&C on the network allows more business to be conducted in real time. Networking solutions that offer native integration with UC&C solutions (e.g., Microsoft Lync) are a viable option for many enterprises.

Considering Juniper Networks

The Juniper Networks cloud-enabled campus solution is a viable contender for enterprises that are refreshing legacy network architectures and are considering moving to some degree of cloud networking. Built on high-performance EX Series Ethernet Switches and SRX Series Services Gateways, as well as MX Series 3D Universal Edge Routers, this solution provides advanced network management, architectural simplification, visibility, and analytics for performance monitoring, as well as an open framework for integrating with WLAN and collaboration tools. Juniper's solution seeks to meet the need of delivering simple, reliable, scalable, and secure high-performance network connectivity that is available anywhere, anytime, and anyplace for the modern mobile workforce while reducing complexity for enterprise IT.

To address the requirements of anywhere, anytime, anyplace network connectivity, Juniper's cloud-enabled campus solution supports the increasing number of devices that BYOD brings about through its port density and scale. Automation capabilities (through Juniper's Zero Touch Provisioning, Junos PyEZ, Chef, and Slax) allow enterprises with limited budget and staffing resources to speed up deployments and changes and enforce network policies. Features such as active and backup routing engines, graceful failover, and ISSU ensure high availability with nonstop packet forwarding. Additionally, Juniper supports options such as Multi-Chassis LAG to provide a dual control plane in distribution networks, enabling availability and resilience. Furthermore, Junos Space Network Director provides a single-platform management tool that supports multivendor environments.

Juniper's portfolio is evolving in concert with the changing needs of today's campus. For example, Juniper's cloud-enabled campus solution offers 40GbE switching to support the growing number of enterprise applications demanding greater amounts of bandwidth. Additionally, Insight Technology analytics are offered to optimize network connectivity and application performance. Meeting the challenge of the proliferation of network endpoints, Juniper's solution provides high logical scale of MAC and IP addresses. Juniper offers the option for multivendor interoperability, which includes standards-based management of wired and wireless (802.11n or 802.11ac) infrastructure through integration with Aruba Networks, including Aruba's ClearPass solution for policy management. Additionally, Juniper offers MPLS L3VPN and EVPN for secure and reliable datacenter-to-branch office connectivity. Finally, Juniper supports potentially transformative UC&C technologies and belongs to the small set of networking vendors that are certified for Microsoft Lync for both wired and wireless deployment.

According to the company, Juniper's Virtual Chassis technology, which enables up to 10 interconnected EX Series switches to operate as a single, logical device, simplifies the enterprise distribution layer by flattening the network and eliminating the need for Spanning Tree Protocol (STP), Virtual Router Redundancy Protocol (VRRP), and other complex VLAN configurations. The corresponding decrease in the number of devices reduces power consumption, as well as capex and opex, and promotes better application throughput. A Virtual Chassis configuration reduces the number of devices to manage and eliminates network switching layers. The resulting simplified management reduces cost of ownership, which is also supported by a reduced learning curve using the Junos operating system. Adding switches to a Virtual Chassis configuration makes a network highly scalable, which in turn enables an organization to increase the number of switch ports without increasing the number of devices to manage.

With the number of security attacks on the rise, securing the network has become a critical and challenging task for IT professionals. A comprehensive layered approach consists of several distinct technologies, including next-generation firewalls, virtual security for datacenters and clouds, virtual private networks (VPNs), antivirus scanning, antispam, intrusion detection/prevention systems, and application security. By employing a layered security approach, customers benefit from a system of barriers that is many times tougher than each of the individual components. The Juniper Networks SRX Series Services Gateways are purpose-built platforms that can perform these essential networking security functions.

Juniper's cloud-enabled campus supports all types of cloud deployments — private, public, and hybrid (through Contrail Cloud, WAN EVPN/MPLS technologies, and integration with VMware in the data plane and control plane). Through its comprehensive portfolio, Juniper can support high-density wireless connectivity from the core to the edge, from the datacenter to the WAN to cloud networks (using MPLS or VPNs). Robust SDN capabilities round out Juniper's cloud-enabled campus offering.

Challenges

Challenges abound for enterprises that are considering making a new investment in cloud-enabled network infrastructure. Given that many enterprises are still exercising caution in IT spending decisions, any new investment — capex or opex — will likely be subject to close examination. Making the ROI case early for a new technology proposal is of critical importance — the potential reduction in capital investment through cloud technologies will be especially relevant here. Large enterprises, as well as networking "traditionalists," may want to stay with more tried-and-tested delivery models. Moreover, in any cloud-managed environment, there is the rare possibility of a cloud connectivity failure, which can disrupt access to mission-critical cloud-based SaaS applications. Thus, it is imperative to closely examine any cloud vendor's SLAs and redundancy strategy. Finally, in evaluating Juniper's unified networking solutions for the first time, organizations should consider the implications of the Aruba partnership and the ongoing development of interoperability standards. Organizations should assess these challenges as part of a thorough evaluation of their enterprise networking options.

Conclusion

As mobility, multimedia, cloud applications, and other 3rd Platform trends have rendered many legacy networks inadequate for supporting mission-critical application requirements, organizations across different segments and verticals need more nimble and flexible networks. Innovations in campus networking enabled by the cloud, unified wired/wireless network access, and SDN can build a bridge from legacy network architectures to the architecture needed to meet 3rd Platform challenges. The flexibility that cloud-enabled networking provides around application deployment, policy management, and scalability can be a critical business enabler for enterprises struggling with legacy infrastructure. These enterprises should consider cloud-enabled campus network architectures as a viable option. If Juniper can address the challenges outlined in this paper, IDC believes the company has a significant opportunity for success.

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