WHITE PAPER

Next-Generation Networking for the Smart Enterprise Campus

Sponsored by: Huawei

Rohit Mehra

August 2013

EXECUTIVE SUMMARY

Today, network administrators are under pressure to meet demanding business requirements. They must provide users with high levels of application availability, ensure network security, and provide flexibility to incorporate future services and applications as business needs change.

Nowhere is this truer than in the campus network, a critical link through which users interact with applications and data. A variety of trends have placed greater demands on the campus network in recent years, including the explosion in mobile devices in the enterprise brought about by the consumerization of IT and bring your own device (BYOD). Campus networks must handle increasing use of cloud services and data-intensive applications, including video and VDI. As mobile devices become the norm, the environment must incorporate wireline and wireless seamlessly and securely. Yet at the same time, network administrators must introduce simplicity and greater levels of manageability to reduce their own burden.

To address these requirements, Huawei has launched a new series of campus networking products that combines wireless and wireline networks into a single converged network. The series introduces policy-based management at the user level and at the application level so that administrators do not have to worry about specific ports or topologies. It also provides higher quality of service (QoS) through the introduction of new technologies designed to tailor QoS to specific user and application needs and to detect and bypass failures in the network.

With this innovative new approach, the Huawei campus solution not only is designed to improve the user experience while providing support for key trends in today's enterprise but also is intended to simplify the management burden and provide automated monitoring and control while leaving the door open to new network services and application needs in the future and greater levels of programmability and network virtualization. It even provides a direct upgrade path to software-defined networking (SDN) when the organization is ready to take that step. The Huawei campus solution provides enterprise networks with agility to enable rapid changes to services and applications.

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

SITUATION OVERVIEW: COMPLEX DYNAMICS OF TODAY'S ENTERPRISE IT ENVIRONMENT

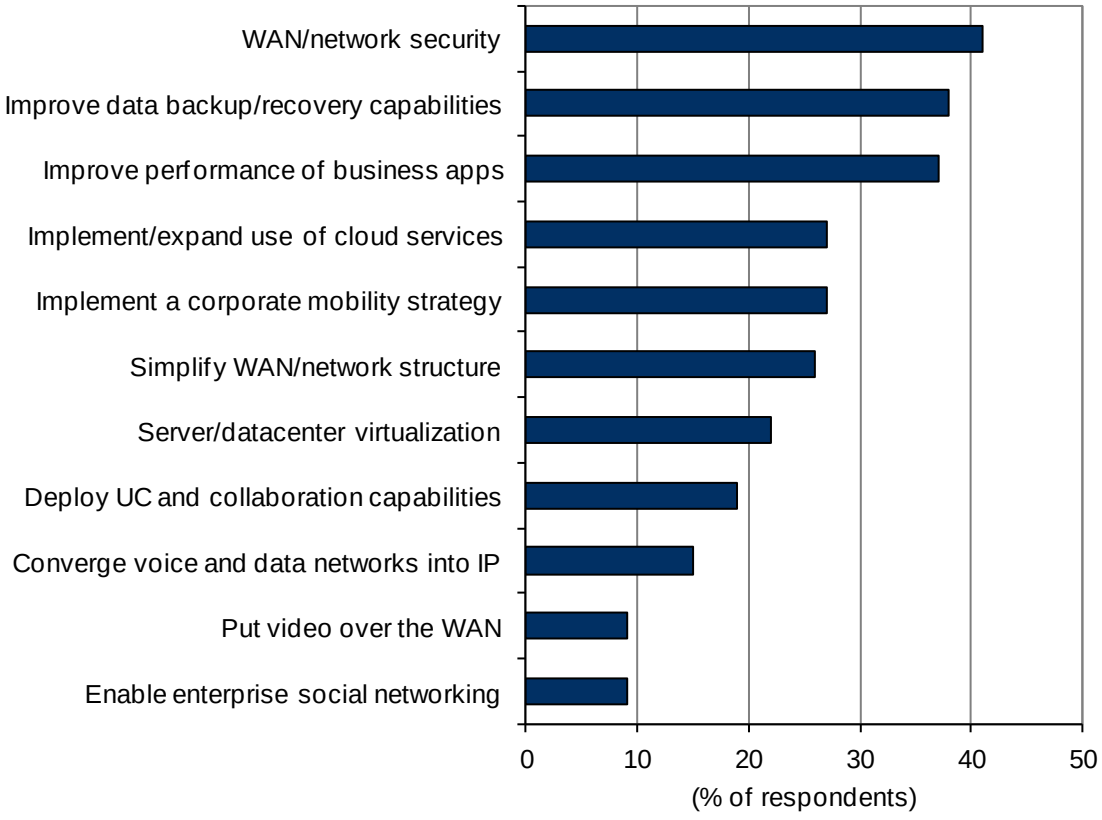
Enterprise network managers must balance a variety of needs, including providing users with high levels of application access and availability in a highly secure environment while still incorporating sufficient levels of flexibility to allow the introduction of new network services and applications as required in the future.

Figure 1 illustrates some of these conflicting demands. When asked to list their most important technology initiatives, network managers most frequently cited security and backup and recovery, followed closely by performance of business apps, cloud services, and mobile strategy. They also said it is important to introduce greater simplicity into their network environment. This shows how network managers are being pulled in multiple directions to balance conflicting demands from the enterprise.

FIGURE 1

Key Technology Initiatives: Performance, Security, and Backup

Q. Of the following technology initiatives, which three are the most important to your organization at the moment?



n = 1,212

Source: IDC's *U.S. WAN Manager Survey,* 2012

As the gateway to the enterprise IT infrastructure, the campus network is on the front line to support critical enterprise requirements, including consumerization of IT, cloud computing, and video and VDI. While these technologies have created opportunities for employees and the enterprise alike, they also have created challenges for network administrators.

Consumerization of IT

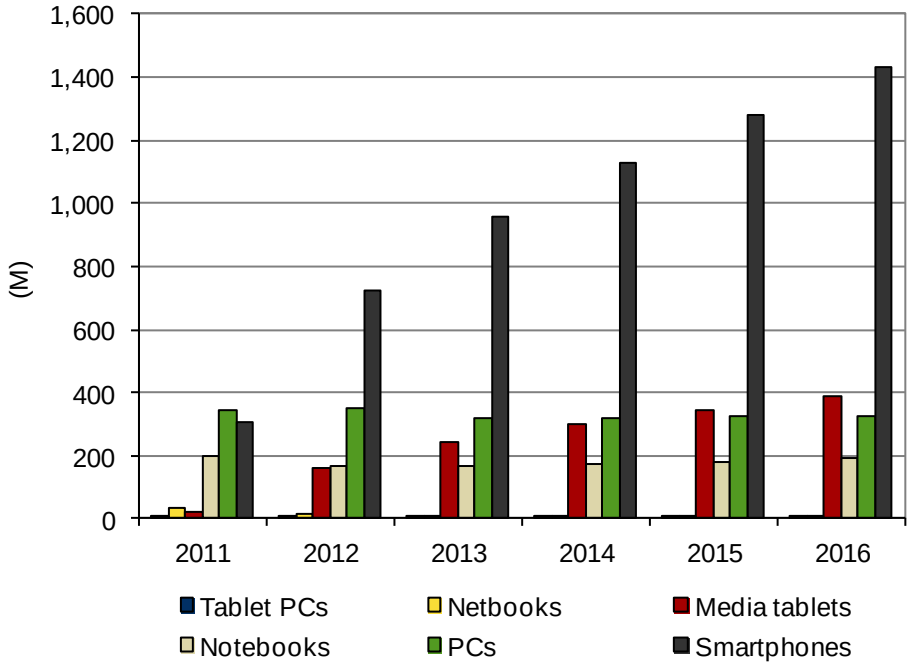
Consumerization of IT, in which technologies originally designed for the consumer market are being adopted for enterprise use, is having a major impact on today's enterprise IT environment. These technologies include mobile devices such as smartphones and tablets as well as applications such as social media and cloud file sharing. Originally brought into the enterprise environment by employees without permission from the enterprise, these devices and applications have become so widespread that enterprises have begun proactively supporting them.

Growth in Mobility and Bring Your Own Device

The poster child for the consumerization of IT is the explosion of smart mobile devices in the enterprise. While IDC research has shown that PCs remain the most important device for getting work done, information workers are increasingly reliant on mobile devices, including smartphones and tablets, for work purposes. Figure 2 shows the growth forecast for these devices.

FIGURE 2

Worldwide Mobile Device Shipments, 2011–2016



Source: IDC, 2013

While some mobile devices are owned and supplied by the enterprise, a large number continue to be employee owned or purchased. A recent IDC study speaks to the magnitude of the impact these devices have on the business: In 2012, 68% of employee-owned devices (i.e., BYOD) were being used to access enterprise applications — up sharply from the 45% that were doing so in 2010.

Even as the use of mobile devices has made employees more productive and businesses more competitive, IT organizations are scrambling to support these devices while maintaining security and control. Another recent IDC study showed that while 83% of IT respondents believe that tablets and similar devices will be integral to how their organizations will conduct business in the future, 80% believe that IT's workload will increase as employees bring consumer devices into the workplace.

In the few short years that employees have been bringing their own devices to the office for work, the question is no longer whether IT should support them but how it can provide the foundation to manage and secure devices while providing an appropriate user experience for application access. IT needs to put in place device-aware policies at the user level to ensure that users can access applications in the manner most appropriate to their needs.

Cloud Computing

Another major trend in enterprise IT is cloud computing. Most IT organizations realize the benefits cloud can bring, including reducing complexity in their environment, easing the workload for internal IT staff, and reducing the variety of skill sets they need to keep in-house. It can also help IT more rapidly scale compute resources when required and adjust to shifting business requirements.

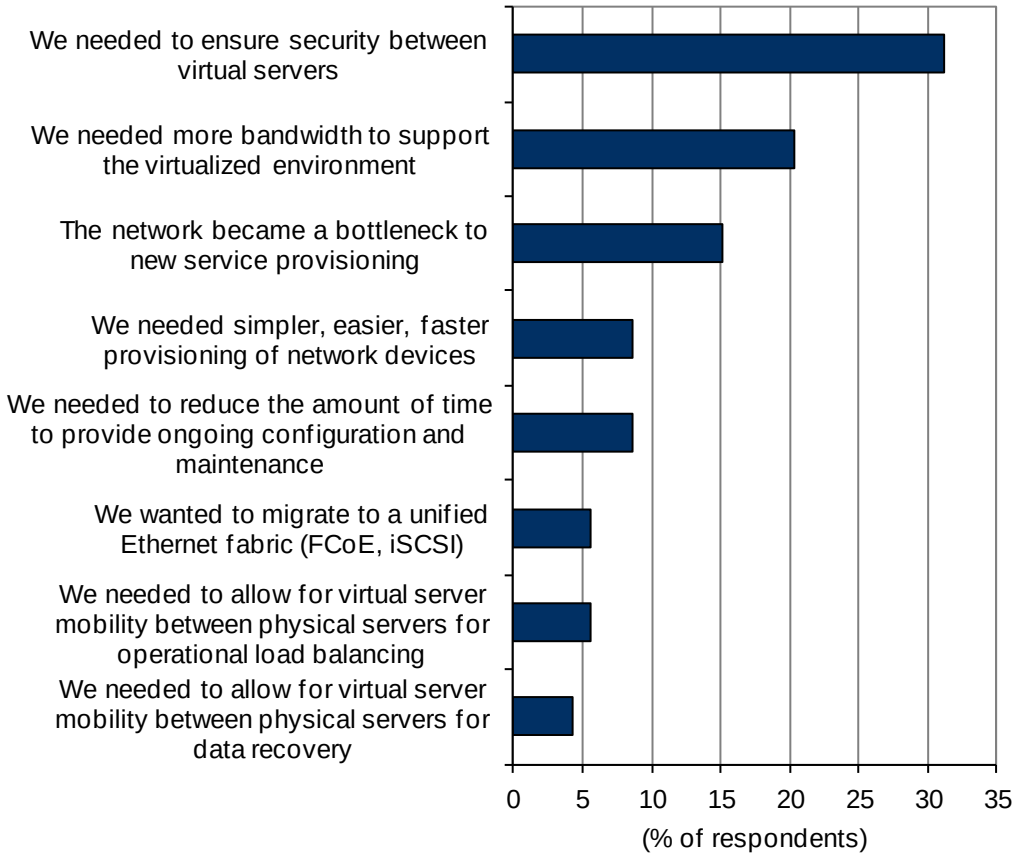
IDC has witnessed significant growth in cloud computing and expects it to continue. Worldwide revenue from public IT cloud services exceeded $21.5 billion in 2010 and will reach over $70 billion in 2015, representing a compound annual growth rate (CAGR) of over 25%. This rapid growth is over four times the growth projected for the worldwide IT market as a whole (6.7%).

IDC expects that a significant number of new cloud rollouts will consist of private cloud deployments as enterprises look to realize the complementary benefits of keeping some cloud resources in-house while leveraging public cloud services for the remainder. As shown in Figure 3, security, bandwidth, and provisioning are major concerns for enterprises looking to implement private cloud.

FIGURE 3

Drivers for Rearchitecting the Network to Support Private Cloud

Q. What was the main reason you needed to rearchitect the network to support private cloud?



n = 251

Source: IDC's *Virtualization Survey,* 2012

Cloud services complement and reinforce the trend toward BYOD and mobile device growth in the enterprise. Cloud-enabled enterprises provide application access over BYOD in a secure manner. It is important to note that BYOD itself is not sufficient to enable enterprise mobility; rather, cloud-based applications and services that are connected with mobile devices enable workers to conduct critical business functions.

Businesses cannot afford cloud services to become inaccessible for any reason — including the network. As more employees depend on the cloud for day-to-day activities, the campus network must deliver consistent, high-quality performance. This is particularly true for mission-critical cloud-based applications for which quality of service and availability cannot be compromised.

Wired and Wireless Convergence

Traditionally, wired and wireless networks have operated in separate realms. Wireless networks have been deployed as overlays to the wireline network, with separate policies, tools, and management. This introduces risk as policies and practices can be applied inconsistently across wireline and wireless networks, increasing the administrator's burden and driving up management costs and complexity.

The growth of mobile devices has placed greater demand on the wireless network. As more business-critical applications are accessed across the wireless network — through both mobile devices and laptops — enterprises can no longer afford to treat wireless networks differently than wireline networks. By unifying wired and wireless networks into a single converged infrastructure, businesses can gain greater levels of manageability and improve user experience. They can improve levels of performance and flexibility and improve their security and policy stance.

Increasing Video and VDI

The use of video on the enterprise desktop is quickly becoming a common method for employees to communicate with each other as well as with customers, partners, and suppliers. In a recent IDC survey, over one-third of all organizations reported that they currently use some type of video, such as desktop videoconferencing or telepresence, and another one-third indicated that they plan to do so within the next one to two years. Yet video introduces specific challenges into the network, including large data flows, bursty traffic, and high degrees of sensitivity to packet loss.

The virtual desktop is also seeing increased growth within IT environments, with the worldwide market expected to exceed $2 billion in 2013. By enabling desktops to be managed and administered from a central location, organizations can achieve significant operational cost savings and greater levels of security because they can maintain greater levels of control over desktop patches and upgrades.

Security

IT must provide users with seamless access to applications and services, whether housed in the enterprise datacenter or delivered via the Internet. But at the same time, IT needs to maintain security and control over its network. This becomes more challenging as more data and applications move to the cloud and a greater number of enforcement/demarcation points are introduced into the network.

Security must be provided on multiple fronts from business practices and policies to provisioning, management, and operations. Organizations must ensure that policies are constantly kept in sync and up to date across their networks so that, for example, once an employee leaves the organization, IT can quickly act to deny access to any sensitive data.

Impact on the Campus Network

The campus network is a vital link enabling communication and collaboration both across and outside the enterprise. To enable users to access the applications and resources they require and support the emerging trends discussed previously, the campus network must adhere to a number of requirements:

- **Cloud readiness.** The network must support the ability for users to access compute resources via public cloud or in a public/private cloud model in a secure manner while still providing high quality of service.

- **Content awareness.** Users accessing different applications via different devices place different levels of demand on the network. The network should understand which applications and users represent mission-critical needs and/or are highly sensitive to latency and adjust the service quality accordingly.

- **Flexibility to support advanced network services.** To ensure flexibility and organizational agility, the network must support new applications and services as needed. Campus networks must be architected such that they are neither a hindrance nor a bottleneck to introducing new applications.

- **Simplified, automated management.** IT organizations must manage increasing complexity in the network in the face of limited budget and staffing. Campus networks must incorporate features that ease the deployment and management burden so they can focus their efforts on higher value-added activities.

- **Policy-based approach to supporting business applications.** To reduce manual effort and ensure the most effective use of administrative staff time and resources, the network should support delineated policies to control access and priorities for the use of network resources.

- **Network automation and programmability.** To provide investment protection, the network architecture must enable introduction of new network services and features without having to rip and replace the current network infrastructure. One of the best ways to do this is through automation and programmability, which enables networks with greater agility to adapt to new changes and services in the future.

- **A path to supporting software-defined networking (SDN).** SDN takes automation and programmability to the next level. By separating the control plane from the switching plane and providing network virtualization and programmability, SDN has the potential to transform the networking world much like virtualization transformed server computing. Companies introducing networking equipment today should ensure that the equipment is able to support SDN if and when their requirements demand it.

HUAWEI'S NEXT-GENERATION CAMPUS NETWORK

In August 2013, Huawei introduced a new series of next-generation campus networking products that consists of:

- **Smart Campus Controller.** The controller delivers policy-based coordination and control of the campus networking environment. It handles unified authentication and path computation and keeps track of network topology and resources.
- **S12700 Agile Switches.** These programmable Agile Switches provide routing and policy execution based on the commands received by the campus controller. They are based upon the Huawei Ethernet Networking Processor (ENP) chip and are available in two models — S12708 and S12712 — in 2013. ENP will also be available in S9700, S7700, and other access layer switches in the near future.

Unlike traditional networks in which policies must be implemented and managed at the device level, the Huawei campus approach enables network administrators to coordinate and control the network as a seamless whole — both wireless and wireline — with no need for management down to the device or service level.

User Policy-Based Approach

The traditional network view is based on devices, ports, and topologies rather than users. If different policies have to be applied for specific users, the administrator must manually translate users to ports and assign permissions, a very cumbersome process.

In contrast, with the Huawei campus approach, administrators don't need to know the details of the network topology or devices. Administrators set policies defining permissions and application access priorities at the user level. These policies are stored in a user/application database, which is referenced by the Smart Campus Controller to send appropriate instructions to the Agile Switches. When a user comes onto the network, the controller automatically applies all control and configurations to the network devices for that user.

Unified Wired/Wireless Approach

The Huawei campus solution combines wireless and wireline networks into a single converged wireless/wireline network with unified authentication, permissions, and automatic deployment of QoS. Its built-in broadband remote access server (BRAS) technology provides unified user management capabilities and greater control over the user environment.

With traditional campus network topologies, the wireless network is treated as an overlay with its own set of policies, permissions, management, and controls. In contrast, the innovative Super Virtual Fabric (SVF) functionality found in the Huawei campus networking solution virtualizes both wired switches and wireless access point (AP) ports into a single network with uniform forwarding, control, and management of data.

With SVF, administrators can treat their wireless and wireline network as if it were one big switch. Huawei calls this a "Super Switch." A single, unified set of policies can be applied and administered on a per-user basis. Whether the user is accessing the network by wireline or wirelessly, the same policy is applied, which means the administrator doesn't have to configure the policy in two different places.

Providing Policy-Based Quality of Service

One of the hallmarks of the Huawei approach is its use of dynamic flow control and dynamic path planning to provide tailored quality of service to users. Policies can be set for groups of users and applications, and the network customizes the forwarding path to control latency as required.

The campus controller is aware of the user and the application, and the controller can automatically deploy virtual networks so that bandwidth and policies are applied to users and applications on an individual basis. For example, video traffic can receive higher priority than email, or development teams can receive higher quality of service than guest users. Policies can even be configured based on the location of the user, the time of day, and/or the device the user is carrying. By provisioning the network with certain minimum QoS parameters for certain users and applications, and appropriately reserving the required bandwidth, the organization can improve the perception of service quality for users and applications.

Automated Monitoring and Control

Another primary feature of the Huawei approach is the ease of network monitoring and control. In traditional networks, the administrator sees the topology of the network consisting of physical ports and devices. As the number of nodes and users increases, management of ports and devices becomes difficult and complex. With the Huawei campus approach, the administrator's view is of the users and applications as well as the policies and permissions that are specific to each of them. The network understands which users are hitting which ports and automatically applies the policies to the devices. This reduces the effort to configure and manage the network considerably.

Further, Huawei has introduced an innovative new technology it calls Packet Conservation Algorithm for Internet (iPCA), which is designed to determine the experience of the user, including packet loss and slow network performance. Traditional monitoring technologies such as bidirectional forward detection (BFD) and network quality analysis (NQA) are designed to perform only single-in/single-out detection and cannot be used to identify where failures lie between two points. In contrast, iPCA provides multi-in and multi-out quality monitoring and can be recursively applied to portions of the network, all the way down to a single device. This enables the network to detect failures and isolate them very quickly, improving quality of service to the user. All of this happens nearly instantaneously from the user's perspective.

Security

The Huawei Agile Switches include built-in support for firewalls, NAT, IPSec, and IPS in the company's next-generation value-added service cards and IPS, ADC, and ASG in its open service platform (OSP) cards. In the future, Huawei plans to support ASG, SSL VPN, and prevention of DDoS (distributed denial of service) attacks on its next-generation value-added service cards.

One of the innovative aspects of the Huawei approach is its treatment of DDoS attacks. In traditional networks, when one point in the network is attacked, the whole network could collapse. With the Huawei approach, when a DDoS attack is detected, automatic safety rules are issued at the access layer, blocking the attack. The controller isolates the affected resources and routes traffic around them so the rest of the network is not affected.

Another innovative security feature is location-aided authentication (LAA). LAA enables includes geolocation as one aspect of the authentication process. This can be used for a variety of purposes — for example, to block network access to users currently outside the campus, regardless of their log-in credentials.

Key Benefits of the Huawei Campus Networking Approach

The Huawei S12700 series was designed to support today's campus network demands and to adapt as business needs change. Some of the key benefits associated with the Huawei campus networking approach are as follows:

- **Support for BYOD, cloud computing, and video.** The policy-based approach at the core of the Huawei campus networking product family is designed to meet the needs of today's enterprise, with appropriate QoS provisions for cloud computing and video. Its unified approach to wireless and wireline networks is designed to address the needs of mobility and BYOD.

- **Adaptability for changing applications, users, and devices.** With the rapid pace of change, network administrators must ensure they have a network infrastructure that not only meets current needs but also offers flexibility for the future. While it is often difficult to extend traditional networks to accommodate new technologies, the Huawei programmable approach allows new technologies to be incorporated using software upgrades.

- **Simplified management.** The traditional network view is based on devices, ports, and topologies. In contrast, with the user- and application-based view of the Huawei campus network, the administrator doesn't have to know topology details. Traditional networks require manual configuration to deploy user-specific policies, but Huawei enables policies to be deployed automatically with a smart control mechanism.

- **Improved user experience.** Traditional networks can't detect user experience degradation or determine the causes of it. With its innovative iPCA technology, Huawei enables the network to automatically detect network failures and isolate their location.

- **Smooth evolution to SDN.** This approach takes advantage of Huawei's innovative ENP chip technology and a fully programmable architecture to enable the network to adapt with agility, responding to evolving business requirements today. It also provides investment protection by enabling a smooth transition to SDN technologies, including POF, SDN VPN, and parallel panel architecture (controller panel and routing panel), in the future.

OPPORTUNITIES AND CHALLENGES

IDC sees a number of opportunities and challenges for Huawei as it rolls out its new campus networking products.

Opportunities

- **Demonstrating thought leadership for the next-generation campus.** These products allow Huawei to paint its vision of where the next-generation campus is going. Instead of being just another set of boxes with higher feeds and speeds, this solution demonstrates Huawei's commitment to the next-generation campus, where the best of wired, wireless, security, and management can be brought together.

- **Establishing a foothold in the enterprise wireless market.** Huawei's presence in the pure wireless LAN enterprise market has been limited to date. The launch of this new converged campus wired/wireless offering provides the opportunity to command increased mindshare from the IT community and gain increased traction in the wireless space.

Challenges

- **Introducing programmability and smart infrastructure to the campus LAN.** To date, network programmability, virtualization, and SDN have focused on the datacenter, whereas the Huawei smart infrastructure product suite focuses on the campus. Huawei will need to educate the market about the need for and benefits of introducing intelligent networking into the campus environment.

- **Establishing leadership presence across geographies.** True to Huawei's geographic origins, the primary focus of the company to date has been in China and other Asian markets, with more limited presence in other geographies. Huawei's current geographic footprint could limit the ultimate take rate, despite the innovative, service-rich nature of Huawei's campus networking products.

CONCLUSION

The enterprise campus network is the gateway through which users access applications, data, and services. Network administrators must ensure that campus networks can support trends such as consumerization of IT/BYOD, cloud services, video, and VDI while incorporating flexibility to meet future demand. In addition, they must do this while simplifying the network and minimizing their own management burden.

Huawei recently introduced a new series of innovative campus networking products incorporating the concepts of programmability and control, policy-based management at the user level and the application level, and wireless/wireline convergence. Consisting of a Smart Campus Controller and a series of Agile Switches, the Huawei campus networking solution is designed to improve the user experience, reduce the management burden, and increase network security, all while future proofing the campus network to enable the introduction of greater levels of virtualization and even SDN when required.