HIGH 5: NETWORKING TRENDS IN 2014

Network managers looking to keep pace with evolving technology should focus on five key areas.

READ ABOUT:
• Addressing BYOD security concerns
• Virtualization as a driver for flatter, faster networks
• New approaches to network security
• Prepping for software-defined networking
• Pushing IPv6 deployments forward
Planning for a smoothly operating network requires more than simply maintaining solid operational skills. Change in technology is constant. Whether it’s within or outside the data center, it impacts the enterprise network.

Five key areas to monitor include bring-your-own-device (BYOD) programs, network optimization, data center changes, software-defined networks and IPv6. IT managers have weathered many of these waves previously, but they are back now, hitting heavier than before. Staying ahead of trends, carefully planning for upgrades and enhancements, looking to the horizon — all are valuable business practices that also happen to support successfully operating a network. And a healthy network is an essential element to a healthy business.

**BYOD AND MOBILITY**

While many organizations have embraced mobility, the huge influx of high-performance smartphones and tablets has changed the dynamics of mobile initiatives. Before BYOD, mobility was all about letting staff work when they wanted, where they wanted, and helping them stay productive and connected while away from their work desks. Now, it’s not just when and where they want, but how they want as well.

The consumerization of IT has brought technology into the homes and pockets of users like never before. And users are often able to leapfrog enterprise IT desktop teams by adopting the latest technologies more quickly than their help desks can handle, rolling out Windows 8 on their home networks before the IT department at work has finished upgrading to Vista.

BYOD doesn’t raise performance concerns any more than an in-house mobility project — the choice of device doesn’t significantly change bandwidth requirements. But it does raise huge security issues, and network managers should be prepared for new requirements from security teams as they design their BYOD rollouts.

Network access control (NAC), a technology static for nearly a decade, is suddenly hot again as security and network teams struggle to enable BYOD without opening up the network to malicious software or users. On the wired side of the network, BYOD initiatives have rekindled the need for running IEEE 802.1X on switches. Network managers should take their current switch hardware and firmware into their test labs and be sure they are prepared for a fast 802.1X rollout if necessary.

A second common change for BYOD is increased network segmentation, breaking large networks into smaller pieces with increased access control in the form of firewalls and routers, as well as risk mitigation tools, such as intrusion prevention systems and malware scanners between the segments.

For many IT shops, BYOD equates to wireless LAN access, and this perspective continues to emphasize the need for a dependable alternative to wired connections throughout an organization’s location. While deployment of wireless LAN controllers or controller-less coordinated access points is a start, there is no substitute for periodic wireless audits to ensure that signal levels, interference levels and density levels are adequate wherever users want to work.

Lackluster deployment remains a common problem in enterprise wireless networks. BYOD initiatives are a good excuse to re-evaluate whether an existing deployment is providing enterprise-class service and can truly substitute for wired access.

BYOD initiatives can also put a crimp in remote-access virtual private network (VPN) deployments. Many enterprises rolled out remote-access VPN years ago and haven’t paid much attention to this system since. However, with BYOD, new platforms and higher user counts are inevitable.

Network managers should revisit their remote-access VPN systems to ensure that current firmware is running and that there is capacity for growth. In some cases, hardware generation changes by key vendors, such as Cisco Systems, Juniper Networks and F5 Networks, may require an upgrade to get current on remote-access VPN.

**Network Optimization**

Organizations trying to migrate from private services (such as multiprotocol label switching or even leased point-to-point circuits) to more cost-effective and available public-network services are discovering challenges in their path, as well as services that
don’t work as well in real life as their marketing materials say they do. A 10-megabit-per-second Internet circuit doesn’t really provide 10Mbps of throughput, and carriers that promise cost-effective availability in every market don’t always deliver. At the same time, continued focus on applications running in the public cloud makes the Internet more important than ever.

All these factors push responsibility for building inexpensive, high-performance and high-reliability wide area networks (WANs) back to enterprise IT teams — just as many CIOs are demanding to outsource more services. To balance these demands, network managers are trying to deploy tools to optimize their networks. Their focus continues to be improving the performance of WANs, providing greater visibility into network usage, and enabling better controls on network and bandwidth usage.

At the same time, end users don’t care about outsourcing initiatives, cloud application migration or the difficulty of building and managing large-scale data networks. Solid WAN and Internet connectivity are required because line-of-business applications are now running both over WAN connections and in public-cloud data centers. End users need high reliability, predictable performance and easy access to ensure successful day-to-day operations.

The difficulty for network managers is finding the right products and services that can solve their problems. Network optimization doesn’t fit into an easily defined niche, and some vendors of WAN optimization controllers (compression, deduplication and protocol optimization), next-generation firewalls and application delivery controllers (load balancers) have been slow to innovate.

The lack of innovation in this product area has caused an explosion of new products and features elsewhere in the marketplace. This puts network managers in a quandary. In-line devices, such as WAN optimization controllers and edge firewalls, are ideal for improving WAN performance, visibility and control. However, network managers hesitate to jettison existing equipment and jeopardize solid relationships to jump to new equipment, new vendors and new capabilities — especially when new vendors may disappear in the next industry shakeout.

For IT shops, this trend carries with it considerable risk. No one wants to stack three or four boxes in every branch office to optimize the overall network experience, but racking-and-stacking is the path of least resistance. Even so, many products are quickly becoming anachronisms in an era of very rapid movement to cloud-based applications, broad international integration, outsourced network management and Internet-focused data sources. Network managers have to act — not react — quickly when in uncharted territory.

BUILDING THE NEXT-GENERATION DATA CENTER

For most network architects, virtualization was the warning shot across the bow: Organizations shouldn’t build data center networks
today the way they built them even five years ago, because the fundamental building blocks of enterprise applications have changed.

But virtualization is only one of the changes persuading data center managers to abandon the traditional core–distribution–edge architecture in favor of flatter and faster models. Some of the other trends pushing new requirements on data center architects are:

- Jumps in server speed and density, virtualized or not, requiring burst speeds faster than 1 gigabit per second
- The heavy level of interserver traffic caused by changes in software application design (“east–west” traffic flows)
- The increase in high–availability configurations with heavy replication requirements
- The slow decline of Fibre Channel storage systems shifting traffic over to Ethernet networks

Few network managers are in the position to do a rip-and-replace on their data center network. But the installation of new storage and virtualization equipment does offer the opportunity to rethink data center design rather than bolt new equipment onto old structures.

Data center networks are being rearchitected as part of a transition to the next generation of data centers, reimagining how applications and data centers are built. This change extends from the power and cooling to the servers and storage, as well as the networking. The push to rethink how networks support data centers is being driven by four key requirements:

1. **Nonblocking (and high speed):** As devices and storage systems require microbursts up to 40Gbps, the need for a nonblocking switching architecture in data centers becomes critical to predictable application behavior and user satisfaction. The average speed of servers may still float below 1Gbps in most data centers, but engineering for averages will affect application performance. Server network connections are universally moving to 10 Gigabit Ethernet in the next few years.

2. **Lower latency:** Movement away from edge–distribution–core toward spine–and–leaf architectures is the most significant change in current designs, reducing hop counts. The terminology has been around for a decade or more, but the technology is only now becoming widely available.

3. **Layer 2 flattening:** Virtualization and virtual machine migration around and between data centers requires Layer 2 extension to maintain IP addressing. Traditional architectures that fill subnets based on optimized routing need to be rebuilt to support new requirements brought on by virtualization and high-speed data center interconnects.

4. **High availability:** Network managers are becoming serious about end-to-end high-availability designs, from dual-rail power to redundant network connections at every point in the data center. At the same time, the need for failover times measured in milliseconds, not seconds, is driving new protocols and approaches to high-availability switching and routing.

Requirements in the data center for higher security and more distributed management and control have added to the challenge. Network management and configuration control, long decoupled from daily operations, are being pushed away from dedicated network teams and into server managers. This stems from virtual switching platforms and aggressive development and operations teams trying to get network complications out of the way of their applications.

At the same time, administrators are reconsidering security. Traditional approaches in data centers that assume a trusted status of systems are being upended. The daily news about breach after breach of “secure” applications clearly contrasts the costs of security with the much higher costs of insecurity.

This particular trend is being collectively driven by technical requirements, equipment replacement, virtualization, security and changing views of network management.

**SOFTWARE-DEFINED NETWORKING**

Software-defined networking is still building toward critical mass through testing and experimentation. However, major networking vendors are beginning to deliver products that touch on SDN. IT managers and network architects need to put SDN on their radar and consider if and when they will want to deploy it to their networks.

Because SDN is a hot topic, many networking vendors are shipping...
products they describe as SDN-ready. IT managers must be careful in implementing these products, because no technical associations have established SDN interoperability standards, which means that SDN components from different vendors may not be compatible.

IT managers looking seriously at SDN technology in data centers — the main application for enterprises — should be building out labs and test networks to see how and where SDN may fit. But at the same time, they can prepare for SDN and improve their networks in three key ways:

1. **Solidify infrastructure services:** SDNs generally involve abstracting the network on several levels — thinking less in terms of ports and patch cables and more in terms of flows and applications. IP address and name management tools, such as domain name servers and reverse DNS, dynamic host configuration protocol, and address management and control, will all be critical abstractions to help remove network dependencies and move toward SDN. An important first step is to solidify these services so that no administrator has to type an IP address again.

2. **Focus on applications:** SDNs make the network fit the application, and this means understanding applications deeply, both client-server and server-server communications. Application focus also includes middle boxes (such as load balancers, firewalls and security applications) that link the networking equipment used to support the application. Having a complete service catalog and application descriptions to fill out the details is necessary to begin to migrate applications over to a software-defined and software-controlled networking infrastructure.

3. **Decentralize hardware and centralize control:** SDNs use centrally controlled hardware, but no one in the SDN industry is thinking in terms of the massive do-everything boxes that have served as the Swiss Army knives of networking. Instead, functions such as user access, wireless, Internet, inter-data center and wide area networking need to be separated to their own domains. This involves more hardware and more potential points of failure to worry about, but more discrete functional units are on the horizon for SDN.

**IPv6**

Internet Protocol version 6 has been on every list of networking trends for the past 15 years. The standards date to the mid-1990s, and now IT managers are realizing that everything in their data centers, from wiring closets to their desktops, already support IPv6 natively.

Microsoft Windows, Apple Mac OS X and Unix have had it for almost a decade. And infrastructure equipment from every major vendor is IPv6-compatible. The missing piece, until recently, had been a stark shortage of Internet service providers with IPv6 services, but even that is changing.

The Internet has run out of public IPv4 address space. Both the Asian and European registries exhausted their supplies before the end of 2012, and only the African registry has enough unallocated space to handle requests past the end of 2014. North America and Latin America will hit critical points near the end of this year.

IPv4 isn’t going away anytime soon, but the world of IPv4 is increasingly connected via address and protocol translation gateways. More devices are online at any one time than the IPv4 address space was designed to support.

For any enterprise serving content on the Internet, this shortage means that servers should be offering both IPv4 and IPv6 to capture all possible users, especially those with mobile devices. Similarly, organizations that make heavy use of Internet content should give end users IPv6 connectivity to ensure that no corner of the Internet will be blocked.

In other words, the demand is light, but it’s there from both client and server. The only blockage now is IT teams who have reprioritized IPv6 again and delayed yet another year. For IT managers thinking about pushing their IPv6 deployment yet again, it’s time to stop delaying and start configuring.

As with any new technology, early adopters of IPv6 faced all the usual challenges, including high-priced and still-maturing technologies and a general lack of expertise. But organizations that implement too late will be playing catch-up.

For IPv6, the sweet spot is now: IPv6 will never be easier to deploy than it is today. IT managers looking at either rearchitecting their data centers or expanding user access with higher desktop speeds, BYOD or Voice—over—IP projects are in a great position. Throwing IPv6 into the mix won’t be difficult — but trying to wedge it in later will be.