

Tech Outlook



Building a Better Network

HP facilitates software-defined networking with end-to-end solutions.

Legacy networking architectures that rely on tiers of switches, routers and protocols essentially tie applications to specific servers, which require days or even weeks to re-configure when changes are necessary. That approach is increasingly ill-suited

for modern data center workloads that require a more agile and efficient IT infrastructure.

“Traditional networks feature a very rigid architecture designed to handle predictable demand,” said Matt Merriman, VP of Professional Services, ProSys. “But things have changed. Mo-

bile and cloud technologies have made network traffic far more dynamic and less predictable. Networks today need to be more agile and scalable to meet periods of spiking demand.”

This is why software-defined networking (SDN) has become an increasingly popular approach for designing, building and managing networks. Applying the principles of virtualization to the network layer, SDN makes it possible to control all switches and routers through software. This breaks the existing physical boundaries on these devices and opens the door for end-to-end network automation.

SDN technologies have matured rapidly and can now be considered

See SDN on page 2

TECH OUTLOOK

PRSRRT STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

SDN

continued from page 1

mainstream. In a recent survey of medium and large businesses in the U.S. and Canada, Infonetics Research found that 80 percent plan to implement SDN in their data centers by 2017. Additionally, more than 60 percent of the 153 survey respondents indicated they are either already doing lab trials of SDN technology or will begin doing so by the end of 2015.

End-to-End Solutions

HP is leading the way toward network transformation, creating an open ecosystem that encompasses all three tiers of an SDN — the data plane, the control plane and the application/orchestration tier.

“The expectation from users and machines alike to connect instantly to information anytime, anywhere and from any device is driving a major industry transition to what we call at HP the New Style of IT,” said Srujan Sama, SDN Product Marketing Manager, HP Networking. “It’s a world where cloud, security, big data and mobility all converge in comprehensive solutions. Our customers are looking for technology partners that can provide the right technology to create the best business outcome. This is HP’s philosophy.”

HP has long been involved in the testing and development of technologies to streamline functions in the network data plane, which includes network hardware devices such as switches, hubs, routers and gateways. In 2008, HP demonstrated the first hardware-based switch implementation of OpenFlow, the communication protocol that forms the basis for SDN. In recent years, HP became the first vendor to offer a full portfolio of SDN-ready network switches that support OpenFlow.

HP also developed one of the first commercial SDN controllers — essen-

tially, the “brains” of an SDN. Controllers allow applications to communicate with network devices via OpenFlow to choose the best path for network traffic. HP’s Virtual Application Networks (VAN) SDN Controller facilitates automated network management, allows data to be routed based on business needs and enables Internet-scale application communication.

By eliminating thousands of manual command-line interface entries for de-

“To solve the challenges created by legacy networks, organizations need the ability to automate the network from end to end by leveraging SDN to abstract the control plane from the physical infrastructure.”

vice configuration, the SDN controller enables network administrators to easily and flexibly program and scale their network environment for single-touch automated applications. It also provides application program interfaces (APIs) to third-party developers to integrate custom enterprise applications.

Applications Drive Agility

In an SDN environment, much of the automation is delivered by applications designed to perform specific tasks such as network virtualization, network monitoring, intrusion detection and flow balancing. HP has also dramatically expanded the possibilities for SDN apps with the HP SDN Developer Kit and the HP SDN App Store. The developer kit provides the essential tools to

create, test and validate SDN applications, and the app store lets customers browse, search, purchase and directly download SDN applications onto their VAN SDN controller.

“Applications are what will drive SDN technology into mainstream networking prominence,” said IDC analyst Rohit Mehra.

In developing an integrated suite of technologies to implement SDN across the entire network, HP has taken a far more comprehensive approach than other vendors in the space. In fact, the market is already becoming saturated with point products designed for network overlay deployments. The overlay approach involves running a logically separate SDN network on top of existing infrastructure. This creates a centralized control plane but falls short by not enabling automated configuration of network infrastructure or providing SDN applications to roll out new services for campus and branch networks. This incomplete approach creates complexity and unnecessary manual coding requirements.

By covering all layers, HP gives customers solutions that can achieve the full potential of SDN through the abstraction, programming and automation of their network to improve scalability and agility, while simplifying the deployment of applications and services.

“To solve the challenges created by legacy networks, organizations need the ability to automate the network from end to end by leveraging SDN to abstract the control plane from the physical infrastructure,” said Joe Skorupa, vice president and distinguished analyst, Gartner. “For maximum performance, utilization and simplicity, customers must ensure that there is a suite of SDN technologies across the entire network — from the hardware infrastructure to the control plane to the applications, and also from the data center to the desktop — in order to move beyond today’s complexities and improve business agility across the enterprise.”

News Briefs

Unlicensed Software Brings Risk

Organizations using unlicensed software on their networks run a substantially greater risk of experiencing cybersecurity incidents, a new report confirms. The report, commissioned by the Business Software Alliance and conducted by IDC, illustrates the link between unlicensed software and malware on PCs, finding that countries with higher rates of unlicensed PC software generally encounter more malware.

"Malware infections can cause significant harm, and organizations are struggling with how best to protect themselves," said Jodie Kelley, Senior Vice President and General Counsel at BSA. "This analysis shows that the link between unlicensed software use and malware is real, meaning good software management is a critical first step to reducing cybersecurity risks."

The statistical analysis compared rates of unlicensed software installed on PCs in 81 countries, with a measure of malware encounters on PCs tracked by Microsoft. It finds there is a strong positive correlation between rates of unlicensed software and malware incidents. Further analysis indicates that the rate of unlicensed software in a country is a strong predictor of malware encounters in that country.

The report builds upon BSA's 2014 study of global rates of unlicensed software. That report found that 43 percent of the software installed on PCs around the world was unlicensed. It also found that the chief reason computer users around the world cite for not using unlicensed software is avoiding security threats from malware. Among the risks associated with unlicensed software, 64 percent of users globally cited unauthorized access by hackers as a top concern and 59 percent cited loss of data.

Cloud Becoming Essential for SMBs

Cloud adoption has become essential among small and mid-sized businesses (SMBs) in the U.S., with adoption rates reaching 89 percent and expected to grow to 96 percent this year, according to a new study from Techaisle.

The study, "2015 US SMB Cloud Computing Adoption Trends," finds that cloud adoption is part of a larger trend toward deeper use of Software-as-a-Service. Until recently SMBs viewed the cloud as a means for reducing costs, but Techaisle says the predominant view now is that the cloud is an essential technology that contributes to business growth.

The firm says this new trend of SMBs adopting the cloud for business growth creates a "perfect storm" of opportunity for cloud computing. It satisfies the demand for new technology-enabled business capabilities such as mobility, social media, business intelligence/analytics and collaboration by providing a platform for supporting these initiatives. At the same time, as IT continues to struggle with cost control, cloud provides a clear means of reining in capital expenditures and reducing management costs.

Tech Outlook

Copyright © 2015 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:

7360 E. 38th St.,
Tulsa, OK 74145
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosys.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosys.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosys.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosys.com

The Carolinas
Toll-Free: 888-337-2626
chash@prosys.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
pmadden@prosys.com

Lexington, KY
Phone: 859-887-1023
Toll-Free: 800-863-9778
dclmmons@prosys.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
dclmmons@prosys.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivot@prosys.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
midatlantic@prosys.com

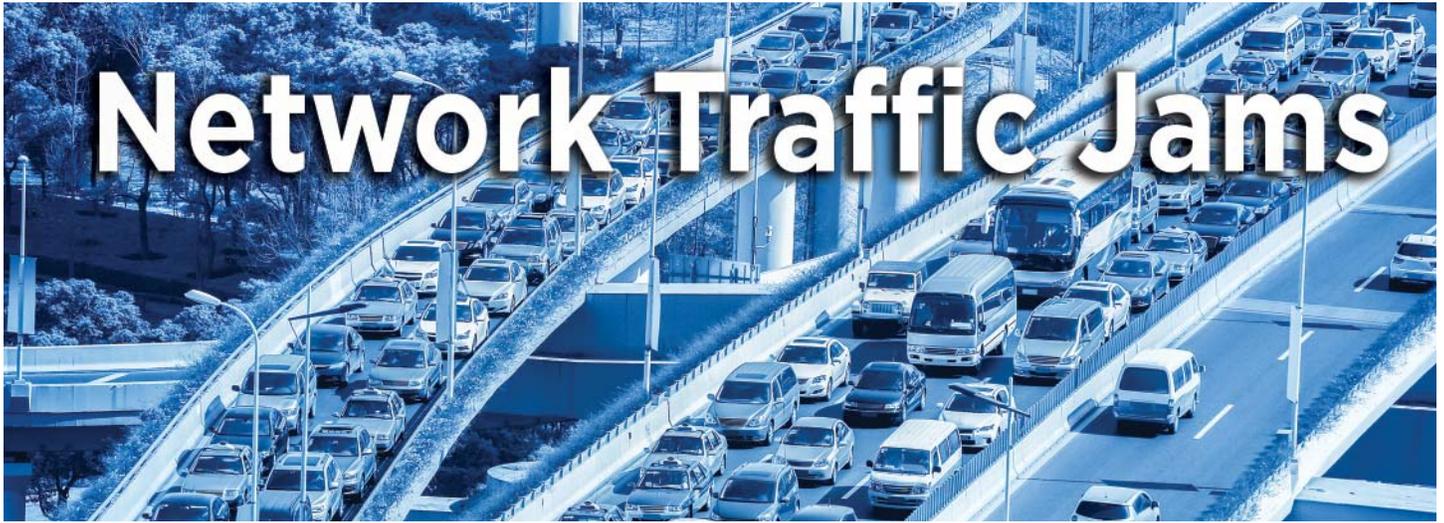
Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
dclmmons@prosys.com

New England
Toll Free: 800-634-2588 ext 1
newengland@prosys.com

New York/Metro
Toll Free: 800-634-2588 ext 3
nymetro@prosys.com

Seattle
Phone: 425-939-0342
sballantyne@prosys.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivot@prosys.com



Sharp surge in DDoS attacks drives networks into the slow lane.

The legendary Woodstock music festival was a watershed moment in 1960s counterculture, famously known as “three days of peace and music.” It is less well known for having created perhaps the worst traffic jam in American history.

County roads and interstate highways became virtual parking lots as more than a half-million people converged on Max Yasgur’s farm in New York’s rural Catskill Mountains. With traffic at a standstill, concert-goers simply abandoned their cars in the roadway and walked to the festival site. Performers had to be flown in and out on helicopters. Governor Nelson Rockefeller declared a state of emergency. The New York Times called it a “colossal mess.”

Distributed Denial of Service (DDoS) attacks have much the same effect on computer networks — minus the music and fun.

DDoS attacks are designed to render servers and/or network resources unavailable by overwhelming them with traffic. This often involves the use of a botnet — a networked of hijacked computers — to unleash a flood of traffic that saps bandwidth, clogs network connections and prevents legitimate traffic from getting through.

Attacks on the Rise

Some DDoS attacks are motivated by “hacktivism,” a desire to disrupt commerce or bring down the web sites of government agencies or large organizations for political or philosophical purposes. Extortion, blackmail, revenge and competitive advantage are among other motives for attacks. Some hackers just do it for the “lulz” — their personal amusement. DDoS attacks don’t require a particularly advanced skillset to execute, either. In fact, they are

increasingly launched by so-called DDoS-for-hire services — cybercriminal operations that charge as little as \$2 an hour to launch an attack.

Whatever the method or motivation, there has been a marked increase in the frequency, volume and sophistication of DDoS attacks. In recent months, the Vatican, the Church of Scientology and the New York City government were all hit, as were Amazon, PayPal, MasterCard and Visa, as well as the PlayStation and Xbox gaming networks. In its Q4 2014 State of the Internet Security Report, Akamai reported that the number of DDoS attacks almost doubled compared to the fourth quarter of 2013, and the average peak bandwidth of the attacks increased 52 percent.

“An incredible number of DDoS attacks occurred in the fourth quarter, almost double what we observed in Q4 a year ago,” said John Summers, vice president, Cloud Security Business Unit, Akamai. “Denial of service is a common and active threat to a wide range of enterprises. The DDoS attack traffic was not limited to a single industry, such as online entertainment that made headlines in December. Instead, attacks were spread among a wide variety of industries.”

Internet of Things Targeted

It is no coincidence that the increase comes at a time when more and more devices are becoming interconnected through IP networks in the so-called “Internet of Things.” As more devices become IP-enabled, it increases the number of devices that can be compromised and used in distributed attacks.

“By its very design, the Internet of Things is built with lightweight security,” said Terrence Gareau, Chief Scientist, NexuSGuard. “These devices rely heavily on shared libraries and a rapid development cycle. Because of their constraints, many IoT devices have limited options for firmware upgrades and other risk management features.

The fact that they are also always online makes them highly susceptible to intrusion and attacks.”

Some of today’s attacks leverage an intimate understanding of the Internet routing topology. So-called Distributed Reflection and Amplification Denial of Service (DrDoS) attacks exploit common network protocols inherent in network devices. DrDoS attacks using these protocols can be difficult to trace back to the malicious actor because they often involve spoofing the origin of the attack. Requests to the victim are reflected to the primary target, making it appear that the target is being directly attacked by the victim.

Many organizations wrongly assume that their existing defenses will stop DDoS attacks, or believe their network will not be targeted. According to the results of a study conducted by Kaspersky Lab and B2B International, 43 percent of large enterprises and 28 percent of small businesses suffered a DDoS incident in the preceding 12 months.

Serious Damage

These attacks can cripple a business. According to the Kaspersky/B2B study, a DDoS attack can cost anywhere from \$52,000 to \$444,000 depending upon the size of the company. In addition to causing serious financial damages, DDoS attacks often harm the victim company’s reputation due to the loss of access to online resources for partners and customers.

According to the study, 61 percent of DDoS victims temporarily lost access to critical business information, 38 percent were unable to carry out their core business functions and 33 percent reported the loss of business opportunities and contracts. In 29 percent of DDoS incidents, a successful attack had a negative impact on the company’s credit rating while in 26 percent of cases it prompted an increase in insurance premiums.

The rapid increase in this attack vector indicates that businesses, both large and small, need to take steps to protect vulnerable devices. Firewalls, intrusion protection and other devices may mitigate very low-level attacks, but high-volume attacks launched from large botnets can easily overwhelm the capabilities of traditional solutions. In fact, security devices can become the attackers’ unwilling allies because they are unable to separate legitimate from illegitimate traffic.

As DDoS attacks have become more complex, sophisticated and frequent, organizations must rethink their security measures. A defense-in-depth posture with a combination of on-premises equipment and cloud-based mitigation offers the best protection against advanced DDoS attacks and will help keep network traffic moving smoothly.



SOURCEfire®

what a next-generation firewall should be

CONTROL WITHOUT COMPROMISE

Sourcefire Next-Generation Firewall adds robust access and application control to advanced firewall capabilities in a universal, high-performance security appliance. No other solution brings together control and effective prevention in a flexible, high-performance engine to satisfy the larger need for complete enterprise visibility, adaptive security, and advanced threat protection.

Key capabilities include:

- Stateful firewall inspection
- Routing, Layer 2-4 switching
- Static and dynamic NAT
- Access control
- Application control
- NGIPS threat prevention
- Network behavior analysis
- User identification
- URL filtering
- Advanced malware protection
- High-availability clustering

Contact ProSys to learn more



www.prosys.com 888-337-2626



Sourcefire is now part of Cisco

© 2015 Sourcefire. SF-02

Down to the Wire

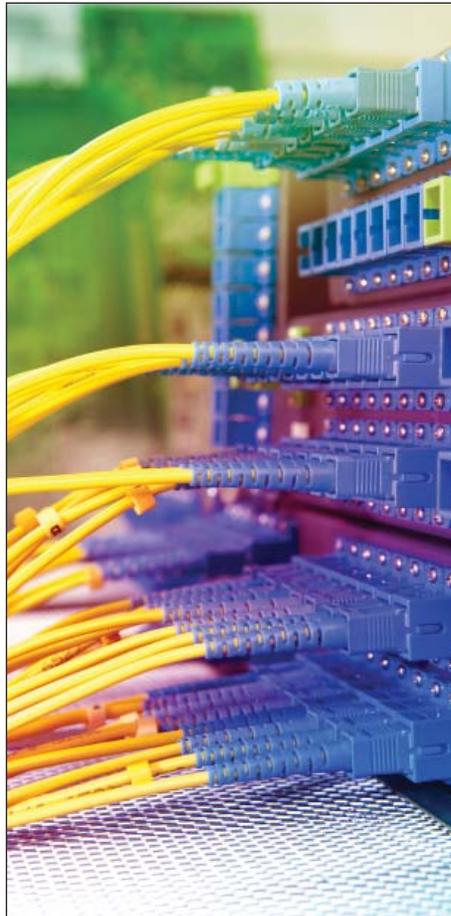
Why high-quality cabling is more important than ever.

Wireless networks have evolved from a “nice-to-have” feature to a mission-critical component of the IT infrastructure. Organizations that depend upon mobile devices are equally dependent upon Wi-Fi — sometimes more than they are the wired network.

But even organizations that rely primarily on wireless still require a high-performance, back-end wired network. In fact, the wired network becomes even more critical. Popular applications such as IP telephony, videoconferencing, digital signage, video surveillance and streaming video require significant bandwidth for a high-quality user experience. The influx of mobile devices onto the corporate network — devices seeking to simultaneously access these applications — can push bandwidth demands to the limits.

When people think about network upgrades they generally consider switches, routers and other gear. Structured cabling is an often-neglected component. It is the foundation that supports and connects most of the network infrastructure, yet it garners just 5 percent of IT investments.

Many organizations expect their cabling plant to last almost indefinitely. But every time an application is added to the network, bandwidth demands increase. If the demands placed on the network go beyond what the infrastructure was designed to deliver and users notice declining performance, it could be a sign that



the cabling plant is in need of an upgrade.

There are many myths and misconceptions surrounding structured cabling. Organizations often view cabling as a “commodity” to be purchased as cheaply as possible. Unfortunately unscrupulous online suppliers promote low-cost cables that do not meet applicable codes and standards requirements. The stakes are high — noncompliant cabling creates a fire risk, particularly when used for Power over Ethernet (PoE) applications.

Proper installation is another concern. Organizations often ask their electrical contractor to pull network

cabling along with other wiring. Just because the cabling is neat and organized, however, does not mean it meets structured cabling standards.

What Is Structured Cabling?

Structured cabling is a comprehensive system of cables and related hardware that provides a flexible, future-ready infrastructure for business communications. This system enables the continuous flow of information, from data and voice to security and wireless connections.

The Electronic Industry Alliance/Telecommunications Industry Association (EIA/TIA) has developed standards for structured cabling in conjunction with the American National Standards Institute (ANSI). Standards are important because they establish technical criteria for the design, installation and documentation of a structured cabling system. This ensures consistent performance, simplifies maintenance and makes it possible to build modular, vendor-agnostic environments that are capable of accommodating new technology and changes to the network.

As IT infrastructures have become denser and more complex, the value of structured cabling has been magnified. Structured cabling uses a modular design that supports new equipment and applications regardless of vendor, making it easier to expand the network to meet growing demands.

Structured cabling also establishes consistency in the network infrastructure, simplifies maintenance and troubleshooting, and reduces total cost of ownership. In fact, the

International Engineering Consortium found that standardizing cabling components and consolidating cable delivery methods reduces initial construction costs by up to 30 percent. It can also cut network maintenance costs by up to 40 percent.

Up-to-date cabling is a must for organizations looking at technology upgrades. For example, 10 Gigabit Ethernet (GbE) technology enables efficient data exchange, simplifies connectivity and administration, and expands bandwidth capacity. This requires a solid cabling plant to take full advantage of the benefits. For organizations making the jump to 40GbE or 100GbE, the performance of fiber-optic cabling is critical.

10GbE is an important consideration for organizations planning to take advantage of the 802.11ac Wi-Fi standard to improve performance and handle increasing wireless traffic volumes. That means the cabling plant often must be upgraded to support the latest wireless network technologies.

Planning Is Key

Many technological upgrades offer only modest performance improvements, but that's not the case with the latest cabling standards. For example, the Category 5 cabling still common in many installations can handle throughput of up to 100Mbps, while Category 6a cabling can handle throughput of up to 10Gbps. To put that into perspective, it takes 10 hours to download a 450MB file over Cat5 but just 6 minutes over Cat6a.

As a result, it's important to understand current cabling trends before moving forward with the design and installation of a structured cabling system. Many organizations are moving from copper to fiber-optic cabling in order to increase data transmission speeds. Thinner, lightweight cables can help improve airflow and make installation and cable management easier.

Proper planning is essential. Cabling systems have a much longer life-cycle than most other components of the IT environment — typically 15 to 20 years. It's important to think about the number of users, the location of those users, and how much bandwidth will be required to meet growing demands. Organizations should also consider the need for additional wireless access points, and PoE support for IP telephony, video surveillance and other devices attached to the data network.

A certified structured cabling contractor can provide invaluable input during the planning stage, helping to develop bid specifications, conduct a planning, budgeting and engineering review, and ensure that the construc-

tion plan is EIA/TIA-compliant. Organizations should look for engineers who are Building Industry Consulting Service International (BICSI) certified and carry the Registered Communications Distribution Designer (RCCD) designation. Installation should be handled by manufacturer-certified technicians.

Although many organizations are increasing their reliance on wireless technologies, the cabling plant plays an increasingly vital role in network performance, manageability and scalability. Whether moving to a new location or upgrading existing facilities, organizations should lay the proper foundation by investing in high-quality structured cabling.

The Six Subsystems of Structured Cabling

Structured cabling standards subdivide each system into six components:

Horizontal Cabling. Most cables are part of this system, including voice, data, multimedia, security and others. The horizontal cabling system is comprised of components between the telecommunications rooms and the work area outlets, including telecommunications outlets and connectors, cross connects, patch cords and consolidation points.

Backbone Cabling. Serving as the core information channel, backbone cabling includes cabling that connects telecommunications and equipment rooms and entrance facilities within the building. It also includes cabling that connects separate buildings.

Telecommunications Room. Termination equipment that connects horizontal and backbone cabling is typically housed in the telecommunications room, which should be on the floor it serves. This includes intermediate and main cross-connects, patch cords, connecting equipment and auxiliary equipment

Work Area. This area is comprised of the components that connect the telecommunications outlet with the user's workstation equipment, including outlets, patch cables and adapters. This may also include workstation devices such as computers, phones and printers.

Equipment Room. This room houses telecommunications systems such as servers, routers, switches and mechanical terminations. The equipment room can replace the telecommunications room and serve as the entrance facility. Each facility should have at least one equipment room.

Entrance Facility. Cable from the outdoor plant meets the building's backbone cabling in the entrance facility. Essentially, this is where the service provider system ends and the system owned by the organization begins. Cables, connecting hardware and protection devices are included in the entrance facility.



Networks that work for you

A complete portfolio of transformational technologies that drive network simplicity.



Campus Networking

Wired and wireless solutions with unified management.



Data Center Networking

Network fabric that provides connectivity for virtualized compute, storage and cloud.



Software-Defined Networking

A complete solution with apps, infrastructure and technology to enable network automation.

Contact ProSys to learn more.



www.prosys.com 888-337-2626