PATHFINDER REPORT

Campus Networking Requirements

Evolution of the campus network and essential criteria to support Agile IT

AUGUST 2017

COMMISSIONED BY

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
Phone: +1 617.598.7200
Fax: +1 617.357.7495

EXECUTIVE SUMMARY

Enterprise IT is changing. It's evolving from a rigid, static, manually configured and managed architecture to one where connectivity is dynamic, application services are on demand, and processes are automated. Enterprise networking is evolving along with IT. This has been evident in the past several years in initiatives such as enterprise digitization and as-a-service consumption models, as well as their enablers, including BYOD, IoT and cloud. Add to this, all of the security implications of each initiative. The evolution of IT requires a network that evolves along with IT's changing requirements – a network that continuously adapts to ever-changing security threats, and evolving digitization, mobility, IoT and cloud requirements.

The purpose of this paper is to assess the switching requirements for next-generation campus networks incorporating wired switches, wireless LANs and WAN routers in an intuitive, intent-based network supporting cloud, mobility, IoT and digitization, with pervasive security. As the primary core and edge elements of the campus networks, switches must help process, forward and enforce policy among all of the other network elements – from the wireless LANs that provide access into the network, to the WAN routers that connect it to remote regions and sites, and the outside world. This paper is intended to evaluate the necessary processing, programmability and intelligent management features of next-generation campus switches as they serve as stewards of the entire network in the evolving enterprise.

DIGITIZATION

On every continent, enterprises are digitizing – using technology internally and externally – for higher productivity, lower operating costs and competitive advantage. As more business processes become digital, enterprise networks have to support the increasing digitization through greater scale, application awareness, policy enablement and enforcement, and programmability.

CLOUD

Enterprises are augmenting internal, on-premises IT with cloud, be it on-premises private cloud, colocated private cloud or public cloud services. Cloud infrastructures mix virtual and physical IT elements, and workloads (VMs, containers, etc.) move between on-premises and off-premises resources. Campus networks have to meet user expectations of application performance and administrator needs around security and policy in a common, consistent manner for on-premises and cloud applications. 451 Research forecasts that 60% of enterprise workloads will be cloud-hosted within the next two years.

MOBILITY

Wireless and mobility are driving the enterprise network infrastructure market. Wi-Fi and wireless LANs permeated campuses, and then enterprise mobility took off with the emergence of smartphones. Workers are accessing corporate data from smartphones and smartphone apps, creating challenges for back-end IT infrastructures and creating greater demand for enterprise mobility among workers.

Mobility is now a strategic must-have in an enterprise because it has become the predominant way workers and visitors access the corporate network and the internet. And because of this – as enterprises move infrastructure to the cloud and offer IT and networking as a service – mobile devices are the on-ramp to that private/public/hybrid cloud infrastructure. Cloud access via mobility is now a strategic imperative for enterprises.

IOT

Digitizing business processes and operations includes connecting devices, sensors and machines in an effort to improve productivity, reduce risk and increase security. Billions of M2M connections will emerge over the next several years that require machine-learning intelligence based on analytics and business policy. Enterprise campus networks will be required to support this influx of machine connectivity.

According to our Voice of the Enterprise (VotE) Internet of Things: Workloads and Key Projects 2017 survey, most enterprises will undertake IoT data aggregation, filtering and analysis at the network edge. And the primary drivers for processing IoT data at the network edge are to improve security and speed data analysis.

SECURITY

All of those new connections – digitization, cloud, mobility and IoT – open up profound security implications. Each new connection is a potential attack vector, and attacks are becoming increasingly sophisticated and obscured via encryption and other deceptive means. Campus networks must be able to secure these new connections by detecting anomalies – even encrypted ones – and recognizing potentially malicious behaviors and patterns in real time and at scale. According to 451 Research's VotE Information Security: Workloads and Key Projects 2017 survey, user behavior remains the top security pain point among enterprise IT.

Technology discussion

INFRASTRUCTURE ESSENTIALS

The campus network infrastructure that is essential to support digitization, cloud, mobility, IoT and integrated security must be built to accommodate the changing nature of network services that enterprise IT is required to deliver as a result of these trends. Infrastructure essentials begin with programmability at the ASIC, operating system software level, as well as programmable telemetry. Also essential are support for physical and virtual IT resources, as well as physical and virtual form factors of the networking infrastructure itself. Finally, it is vital to embed advanced security into the networking fabric because supported applications and connected resources are no longer isolated in the campus network, nor in the branch offices the network supports.

Programmable ASICs

Programmable ASICs adapt to innovation. They continually evolve to anticipate and meet customer needs with a firmware download, and without a hardware replacement. With programmable ASICs, new features and functionality can be added to the campus switching and routing infrastructure as requirements change, making for a more agile, adaptable network. A programmable ASIC will also facilitate convergence of wired and wireless networks through traffic treatment parity. Features such as wire-speed encryption/decryption, prioritization, rate limiting and shaping, packet queuing, security policy enforcement and flexible traffic forwarding can be applied consistently to wired and wireless traffic.

Open programmability and telemetry interfaces

Programmability applies to campus network infrastructure software as well. Switch and router operating systems heretofore have been monolithic in structure, with operating and monitoring interfaces limited to fragmented, vendor-specific CLIs tied to the networking software version. The changing nature of IT and campus networking requires that network operating systems be API-driven and modular so that feature and function changes can be performed at scale and consistently without a release upgrade or whole new OS reload across the entire infrastructure. Also, telemetry and analytics interfaces – both northbound to automation and orchestration systems and southbound to the physical network elements themselves – must be standards-compliant to support the many multivendor sources of data in the campus network (mobile devices, IoT sensors and M2M processes) and from off-premises cloud workloads.

API-driven modular OS

Network operating systems for the enterprise campus require standards-based programmable interfaces to automate network operations and deliver deep visibility into user, application and device behaviors. There should be one OS for enterprise wired and wireless access, aggregation, core and WAN to qualify and deploy new services faster. Modularity facilitates in-service software upgrades and graceful insertion and removal – requirements to maintain uptime and not disrupt network traffic during updates and debugging.

Adherence to standard northbound/southbound interfaces (REST APIs, NETCONF, Yang, SNMP, LLDP, JSON, CLI, RADIUS, TACACS+, etc.)

Standard interfaces that the API-driven modular OS should support include NETCONF (RFC 6241), streaming telemetry, OpenConfig and IETF YANG data models, and Guest Shell, Linux (LXC) and Docker containers. These interfaces ensure integration with software-defined networking (SDN) controllers and configuration management tools; permit analytics tool integration; support heterogeneous network environments; securely host third-party Linux applications; and automate network device configuration management through DevOps tools such as Ansible and Puppet. Also, support for the Python scripting language automates event-based workflows on network devices.

Physical and virtual instantiations, characteristics

Enterprise IT is becoming increasingly virtual given the broad appeal and penetration of server virtualization, the adoption of cloud, the increasing presence of storage virtualization and the building demand for network virtualization. As a result, campus switching technology and architectures have to support virtualized environments as comprehensively as physical environments, including seamless operation with hybrid physical/virtual IT infrastructures. Campus networking infrastructure itself in some cases has to be virtual in order to be integrated into an enterprise's own public, private and hybrid cloud implementations and virtualized IT environments.

Virtualization and virtualized network services can accomplish many painstaking tasks in campus networking. Virtualized routers, for example, grant the same network, computing and WAN services that you find in hardware routers, now as software. As software, virtual routers allow enterprises more deployment options than with hardware. The router can be centrally orchestrated and managed, and can offer a range of virtual routing and networking services – just as its hardware counterpart could.

Moving to virtual services, such as firewalls, WANs, intrusion prevention and WAN optimization, can consolidate hardware and reduce capital expenditures. Similarly, central automated orchestration of virtual network services can lower operational costs as well. Virtual network services can be deployed in minutes instead of weeks or, in some cases, months.

Virtualized network services can also enable rapid and secure network expansion. From the campus, network services can be more easily provisioned and managed at various places in the network – branch, campus, datacenter, cloud – securely, through device onboarding, network segmentation and multi-tenancy. Network policies and visibility can be extended into the public cloud.

Take our virtual router example: a virtual router can allow an enterprise to extend its network to public and private clouds and offer the same routing, security and network management as cloud services with multi-tenancy. It can be hypervisor- and infrastructure-agnostic and programmable across the LAN, WAN and in the cloud. And policies defined for that router within the enterprise can be extended to the public cloud. Extending Layer 3 routing deeper into the cloud can also enhance scalability, or the router could be used to build a VXLAN network that avoids the limitations of IEEE 802.1q VLAN tagging.

Software overlays allow enterprises to rapidly connect users to their needed applications over the most optimal path with minimal, if any, manual intervention at the device level. Virtualization software allows for the implementation of a logical switch fabric in which wired and wireless networks are converged into a single operational, management and security environment with consistent behaviors, policies, and service levels and assurance parameters. The fabric can also serve as a single platform with multiple services. This allows enterprises to the improve customer experience and realize business outcomes by securely connecting groups of users to the applications they need.

Integrated advanced security

Embedded security is essential in the next generation of campus networking. As more devices are connected and workloads no longer confined within the perimeter, ensuring security in the agile, dynamic, on-demand network is imperative. It calls for security to be deeply integrated into the infrastructure and at multiple levels.

Identity-based access

It starts with identity-based access. Knowing who, what and how access is granted to the enterprise network is the first defense of the infrastructure. Policies granting or denying access based on user and device ID profiles, and the applications they are permitted to work with are key to building a first line of defense against intrusion. Authentication and

access control for mobility, cloud, and bring-your-own-device (BYOD) access based on IEEE 802.1X for managed devices and users, web authentication for guests or non-802.1X users, and MAC authentication bypass for unmanaged or non-802.1X devices can be starting points, but security should not end there.

Group-based access control and segmentation policy management

Software-based segmentation based on security groups is a simpler, more practical approach to this new age of campus network security policy than traditional VLAN-based segmentation. It involves the assignment of security group tags (SGTs) to enforce access policies for users, applications and devices. A central policy engine is employed to define and manage SGTs in the network, and share SGT information with other group-based policy schemes. This allows enterprises to streamline security policy management across domains, and quickly scale and enforce policies consistently across the network. Lateral movement of threats can be restricted with micro-segmentation. Group-based policies can also control access to regulated applications and reduce the scope of compliance for regulations such as PCI, HIPAA and DFARS. In short, SGTs enable user and device segmentation without redesigning the network and enable easier management of access to enterprise resources.

Streaming telemetry for behavior-based security analytics

In addition to identity and group-based access control, campus network infrastructure needs to perform real-time streaming telemetry and analytics that learns from and provides insight into user and application behavior. This capability allows the network infrastructure to continually collect network telemetry and process it into contextual user and device metadata. Such metadata could include geolocation, peak time, business unit, technology touchpoints and other relevant contexts. This data can be combined with collected data on device types, topology, capabilities and OS versions to:

- Onboard clients and assign connectivity privileges via authentication, authorization and accounting; DHCP; RF; and roaming.
- Provide network metrics on availability, health, coverage, capacity, connectivity and throughput.
- Measure end-user application statistics for service-level and performance experiences.
- Enable machine learning through in-line monitoring of flow data, like that done with NetFlow.

For security analytics, NetFlow should be enabled at the access layer to ensure complete coverage of all internal east-west traffic and accurately discover suspicious activity internal to the local network. Unsampled NetFlow statistics help ensure maximum fidelity in representation of the actual network activity and of alarms from the analytics solutions that use this data. This also helps detect 'low-and-slow' attackers who may try to reduce the rate of malicious activity in order to stay under the radar.

NetFlow should be hardware-based to ensure that the network devices do not get overwhelmed in generation of NetFlow records, especially as unsampled NetFlow gets enabled. This also ensures continual delivery of high-performance network connectivity, while at the same time enabling security outcomes.

Streaming telemetry on behavior and contextual network analytics, including NetFlow, can provide insight into threats in encrypted traffic, resulting in faster time to response and containment of infected devices. It can also allow the campus network and its security assets to essentially function as a security sensor.

Trusted infrastructure

Key to enabling advanced integrated security and open, programmable interfaces and ASICs is a trusted infrastructure. A trusted infrastructure includes authenticated network infrastructure and software, security baselines – including the latest cryptography technology with public key infrastructure (PKI) storage and updates – and secure runtime.

Authenticated network infrastructure and software provide product assurance and serve as a foundation for protecting customer networks. Authentication of the infrastructure starts with standards-based technology and adds security functions and features to enhance product protection. Standards such as NIST specifications (NIST SP 800-90A and B certifiable random number generation, for example), RSA public keys and X.509v3 certificates are foundational elements of trusted infrastructure.

Security baselines start with secure initiation of signed images. This protects the boot code in the hardware and provides the immutable secure unique device identification. The signature is encrypted and stored on the system along with the code. Signed code is checked at runtime to verify that it has not been changed.

This runtime check also establishes trust in the hardware systems running the signed code. The hardware components can perform proactive monitoring of the startup process and shut down the process if tampering is detected. This is essentially a 'chain of trust' in which the integrity of each element of code on a system is validated before that piece of code is allowed to run. It starts with the immutable root – the signed image – and then each element thereafter is validated in succession before the system is allowed to start.

A trusted system must also provide highly secure storage for keys, passwords, customer credentials and other critical security information, as well as the latest cryptographic technology. Highly secure authentication and management of PKI using the identity and current status of the PKI, helps to secure devices upon installation. If the key is outdated, next-generation encryption capabilities can be employed, which use scalable cryptographic algorithms to address evolving security requirements. A critical element to creating cryptographic keys is random number generators. They also play a vital role in opening highly secure communications between users and websites, and in resetting passwords for email accounts.

ARCHITECTURE

Next-generation campus network architectures require five essential elements when supporting new modes of IT and operational models: wired/wireless convergence, IP convergence of non-IP networks, enhanced performance and high availability, support for different connectivity models, and automation.

Wired/wireless convergence

As stated previously, wireless and mobility are now essentials to network access; indeed, they are the primary modes of network access. As such, wireless traffic must be treated the same as wired traffic – policies for security, QoS, bandwidth requirements, application performance and packet treatment must be consistent across both media. That consistency is assured through a single fabric defining and enforcing consistent operation, administration, management and security through policy.

IP convergence of non-IP networks

Other connections on the enterprise campus – media networks, physical security, utility networks and other non-IP infrastructures – could similarly benefit from a single IP-based fabric. Convergence of these disparate campus infrastructures onto a single IP fabric would enable consistent operation, administration, security, management and visibility into each service. Not only would operation and management be consistent, it would be easier because individual networks dedicated to each service would be converged into one. And those discrete network elements would be abstracted into service elements connected by the same network fabric and managed as components of the overall IP fabric for the enterprise's IT infrastructure.

Requirements for enhanced performance and high availability

Campus switches designed for the adaptability of cloud, IoT, mobility and continuous security need multi-terabit scalability, with 10G and 40G ports in a range of densities to support the varied requirements and deployment options in the campus, and 25G soon on the horizon. Chassis and per-slot bandwidths in the hundreds of gigabits per second are essential to meet the demands of the new IT, and the analytics required to monitor, secure and ensure the network connecting all of its elements.

Switches also need to be resilient and highly available, supporting high-availability patching, graceful insertion and removal, features such as nonstop forwarding and stateful switchover, N+1/N+N redundancy for power supplies, and redundant fans. VXLAN-based fabrics with routed access inherently provide increased high availability and performance, with all uplinks in active forwarding state. This further simplifies high-availability design because no additional HA or loop-detection protocols need to be run in this case.

Other high-availability and resiliency features should include:

- Uplink resiliency.
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) provides for rapid spanning tree convergence and Layer 2 load balancing.
- Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning tree (IEEE 802.1w) re-convergence on a per-VLAN spanning tree basis.
- Switch-port auto recovery to automatically reactivate a link that is disabled because of a network error.

Connectivity models

With the variety of devices connecting to the network increasing – mobile devices such as smartphones and tablets, IoT machines and sensors, etc. – campus networking has to evolve to support an increase in the types of connectivity required from these new endpoints. Gone are the days when connectivity was primarily desktops, laptops, IP phones and printers; these new endpoint devices need forwarding of a Layer 2 advertisement over Layer 3 networks. And as user mobility increases and lines of business start introducing their own custom applications, IT may request that they span a certain network address range across the campus or WAN, and sometimes even mandate that all those endpoints be in the same broadcast domain.

What's needed is an architecture flexible enough to accommodate any connectivity requirement without having to introduce new technologies to address the requirements of the individual endpoint type. Overlay networks such as VXLAN-based fabrics introduce a single architecture that address these requirements for very large Layer 2 domains, along with the ability to establish IP address ranges anywhere in the network without requiring contiguous subnets.

Automation

With so many connected devices, so much data and analytics, and so much security necessary, an adaptable, always-learning network requires precise automation and orchestration for optimal operation. Open REST APIs on the northbound side of an operating system allow applications to access the OS services or the services of another application, such as an SDN controller or an analytics program. REST APIs can instill automation in application processes by facilitating communication and interoperability between applications, or between applications and operating systems. Common automation and scripting languages, such as Puppet, Chef and Ansible, can utilize REST APIs to communicate with operating systems and controllers to share policy definitions for application services, physical and virtual network configurations, and security profiles and instructions.

Use Cases

CLOUD INTEGRATION

As enterprises increasingly adopt cloud as an integral component of their IT infrastructure, campus networks have to support workload mobility between private and public clouds. And IT has to deliver the best possible application experience regardless of where users are and where workloads are placed. Enterprises require highly secure direct connections from their distributed sites to their cloud-hosted applications, with predictable application response time and consistent network operation, as if the cloud were a seamless extension of the enterprise network. VXLAN fabrics allow the campus network to scale beyond the limitations of 802.1q VLAN tagging, and virtual routing can allow the enterprise to extend Layer 3 routing deeper into the cloud environment.

Workloads destined for the cloud also require the same level of security as if they stayed on the enterprise campus infrastructure. So gateways or routers connecting the private cloud to the public cloud require VPN capabilities identical to those on an enterprise WAN: Route-based IP security (IPsec) VPNs, dynamic multipoint VPN (DMVPN) and secure sockets Layer (SSL) VPN, along with firewalling and access control.

One of the drawbacks of public cloud use is a lack of visibility into workload performance and security in the public cloud. Enterprise networks need to be able to evolve and provide a single consistent way of administering and ensuring application performance and security policy enforcement for both on-premises and cloud-hosted workloads. That necessitates virtual network analysis tools and instrumentation that combine application awareness with the ability to look deeper into various network overlays such as VXLAN. Virtual network analysis and monitoring of cloud workloads needs to be able to analyze network usage by application, host or VM to identify unusual traffic patterns or bottlenecks that may affect performance and availability. It should also troubleshoot performance problems consistently across physical and virtual environments, validate infrastructure updates and policy changes, and deliver meaningful analytics that help ensure service levels and accelerate operational decisions.

CONSISTENT POLICY, UNIFORM OPERATION

The explosion in the number of wireless endpoints indicates that enterprises expect wireless to be a dynamic, mission-critical medium that is able to support business applications seamlessly while roaming across very large domains. Advances in wireless standards are progressing rapidly. Standard bodies are already looking beyond 802.11ac Wave 2, and there is discussion around Wi-Fi over optics and seamless handoffs between 5G cellular networks and 802.11 WLAN networks.

This implies that the network infrastructure and architecture needs to be able to accommodate the scale and performance requirements that can only be achieved by distributing the forwarding to the wired networking infrastructure so that the wireless network can scale without performance degradation. This becomes even more critical as advanced, compute-intensive services to guarantee application performance analytics, QoS and security are enabled for the wireless traffic.

To achieve this, the network must interweave wired and wireless control and forwarding into a single, uniform fabric. The goal of the fabric, as mentioned previously, is to provide consistent operation for wired and wireless networks through automated workflows, and to perform policy-based network segmentation to secure users, devices and applications according to identity. VXLAN and LISP are optimal abstraction overlays for converging wired and wireless networks into a Layer 2/3 fabric.

SECURE ONBOARDING, ACCESS CONTROL FOR MOBILE DEVICES, HEADLESS IOT DEVICES

With the single fabric for wired and wireless endpoints integrating streaming telemetry and behavior-based analytics, enterprises can securely onboard mobile devices and sensors – including embedded 'headless' IoT devices unreachable through a GUI. The network itself can serve as a 'security sensor,' providing in-depth security context based on user, device, posture, location, etc., for improved situational awareness and response capabilities. The campus network infrastructure is also uniquely positioned to monitor lateral movement inside the network not seen by other solutions, and track the spread of malware and external attacks across the network.

As a security sensor, the network can perform user, device and sensor discovery and then define security profiles based on these endpoint types and their posture within the enterprise. With these profiles, the network can then authenticate the user, device or sensor and apply policy, including assignment with an SGT for segmentation within the network. Through streaming telemetry and behavioral analytics, the network as security sensor can provide continuous threat protection and restriction.

Conclusion

Cloud, mobility, IoT, digitization and security are changing IT, and campus networking must change along with it. The network needs to be adaptable to the changing requirements of IT and evolve along with these changes. That adaptability depends on continuous monitoring, streaming telemetry and behavioral analytics to instill machine learning and uninterrupted protection. It requires a single, policy-based fabric for wired and wireless endpoints so that groups and workloads can be segmented and secured, and those policies shadow workloads as they move from on-premises private clouds to off-premises public clouds.

SUMMARY AND OVERVIEW OF KEY FINDINGS, RECOMMENDED NEXT STEPS

Campus LAN infrastructure constitutes a critical piece of the overall IT infrastructure for connecting the users and devices in an environment that is rapidly changing. Vendor, product and architecture selections are critical due to the scale and longevity of the technology investments – five to seven years or sometimes even more – and due to the central role campus networking plays in the overall IT architecture.

We encourage enterprises to take a forward-looking view of evolving campus environments, and consider them in architectural and procurement decisions they make today.

- Identify how switching infrastructure aligns with overall strategy around automation and SDN. If the environment has a fixed set of use cases and the strategy is to develop an internal automation infrastructure, then primarily focus on support of modern network programmability and networking feature sets.
- Ensure that the switching infrastructure is coupled with a comprehensive controller that provides the necessary applications for key networking services – whether it be zero-touch deployment, network infrastructure monitoring, application performance optimization, etc. Also, ensure that the controller provides a rich set of open, northbound APIs that enable development of an orchestration architecture between various vendor or network-based domains in the environment.
- The demands for simplicity, application awareness and endpoint flexibility need to be supported by high availability. Fabric architectures such as a VXLAN that support a redundant, centralized control plane for connectivity resolution help provide inherent high availability without the complexities associated with a distributed control plane. Consider an equal-cost multipath forwarding model for maximizing available bandwidth and eliminating network downtime in cases of network adds/moves/changes.

- Ensuring that the campus network is ready for the demands introduced by convergence requires a campus architecture that is capable of supporting network segmentation at scale, given the diverse applications and types of devices that will need network access. That same architecture should not introduce operational overhead to create and manage network segments, and should support flexible network topologies and connectivity models, offering any-to-any connectivity over large domains with a flexible addressing mechanism, as the types of devices and applications requiring connectivity in particular manners are expected to be introduced over time.

About the Author

JIM DUFFY

Senior Analyst, Networking - New York, NY

Jim Duffy is Senior Analyst for the Networking Channel at 451 Research. He covers enterprise network infrastructure and associated software, and network performance management. Jim has been covering technology for over 30 years, including 25 at Network World. His coverage focused predominantly on enterprise networking infrastructure, including routers, switches and associated software.

Jim is widely recognized in the industry for three decades of enterprise networking coverage. He broke several major stories over the course of his journalism career, and received awards for news, analysis and opinion pieces on numerous industry events and developments.

For decades, Jim has overseen, coordinated and driven coverage of a variety of enterprise and telecommunications equipment and services events, issues and developments. He determined story ideas, angles, emphasis and tone on breaking news, trend and analysis pieces, executive Q&A interviews, market forecasts, user case studies, and product and service announcements on a daily and weekly basis.

Prior to his previous position as managing editor at Network World, Jim held senior editorial positions at Computer Systems News, published at the time by CMP Publications, and MIS Week and Electronic News, both owned by Fairchild Publications. Jim is a graduate of Utica College with a Bachelor of Science degree in public relations/journalism.