Ashton, Metzler & Associates

How Business Demands are Changing the LAN Architecture

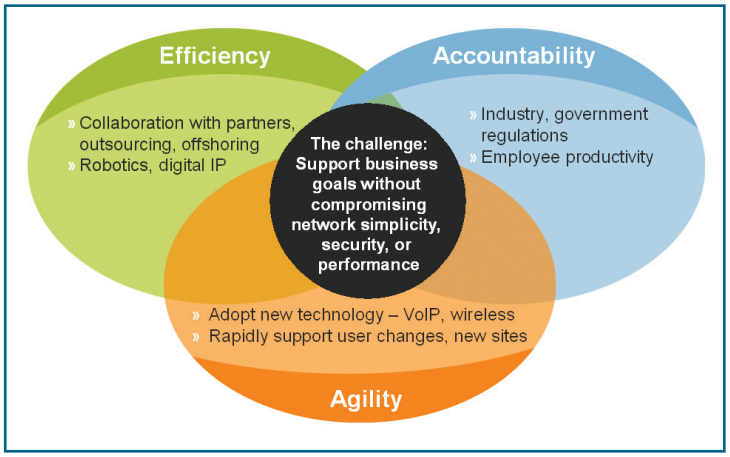
The Advent of Intelligent Switching

Introduction

LAN architectures, and in particular LAN switches, have evolved along a single dimension to date – performance. But today's business climate, with an emphasis on corporate efficiency, accountability, and agility, demands a LAN architecture that helps deliver on those corporate goals. To do so, LAN switches must offer greater capabilities – not just more bandwidth – and those capabilities are embodied in a new generation of intelligent switches that's now begun to emerge.

User and application control are at the heart of this next generation of intelligent switches, which are characterized by programmable hardware with wire-speed throughput, detailed user and application information, dynamic policy enforcement, and simplicity of operation. The legacy switch architecture cannot support these features, making it challenging if not impossible for IT to align network services with business demands. Supporting an ever-more dynamic workforce, rapidly troubleshooting user issues with fewer IT staff, and supporting new services such as voice over IP and wireless quickly and efficiently are just a few examples of tasks made too complex by switches based on the legacy architecture. Since intelligent switching requires a new architecture, switch upgrade cycles will provide the vehicle for organizations to gain this user and application control.

TODAY'S BUSINESS NEEDS



Talking with leading IT organizations makes it clear how updating their LAN architecture is critical to their ability to support today's business demands. To detail the business changes driving these updates, we interviewed four IT professionals: a global director of infrastructure for a technology provider to the financial industry, a director of IT at a medical center, the chief security officer for a division of a major service provider, and the head of information security for a global business process outsourcing company. The interviewees will be referred to in this brief as The Global Infrastructure Director, The Medical Director, The CSO, and the InfoSec Director. In this paper, we'll briefly review the evolution of switching from performance to services, discuss evolving business practices and their impact on the LAN, and outline the switch capabilities needed to deliver required LAN services.

LAN Evolution

In the early 1990s, IT organizations began to deploy LAN switches as a simple and cost-effective means of segmenting shared media Ethernet LANs, to reduce broadcast domains. In the mid 1990s, Fast Ethernet switches boosted throughput and performance and provided aggregation of 10 Mbps segments into collapsed backbone routers. This time period also saw the emergence of edge switches, which were optimized to provide contention-free bandwidth to desktop systems and servers. Vendors who pioneered these developments included Kalpana, Crescendo, and Grand Junction.

The late 1990s saw the emergence of hardware-based Layer 3 switch, which routed packets in ASICs rather than in general-purpose CPUs. This architecture offered a huge performance improvement, pioneered by vendors such as Rapid City, Extreme, Foundry, Packet Engines, Prominet, and Yago Systems.

In the current decade, innovation in edge switches started to become more service-oriented as the fully switched infrastructure made it possible to introduce additional applications on the LAN, including IP telephony, IP video, and mobile wireless connectivity. In the coming years, business practices will continue to undergo rapid change. The move toward a Service Oriented Architecture (SOA)[1] is one way IT is preparing to keep up with the changes – an increased focus on services in LAN switches is another.

How New Business Practices are Changing LAN Requirements

Businesses are under intense pressure to evolve to stay competitive. The need for greater efficiency has companies adopting globalization, outsourcing, and increased use of temporary workers. IT organizations feel that same push toward improved efficiency – constantly being made to do more with less. Businesses have also needed to become more accountable, both to respond to myriad industry and governmental regulations and to increase employee productivity. In addition, businesses are also under pressure to be more agile in their overall response to opportunities and threats in the marketplace.

[1] *An SOA refers to an application architecture in which applications are composed of discrete Web services which often reside in disparate data centers.*

IT, charged with developing networks that help further these corporate goals, ends up caught between conflicting demands. On the one hand, they must create a network environment that promotes collaboration and mobility for users, for example, so the business can increase employee productivity. At the same time, however, they must vigorously protect critical online documents and assets against being stolen, copied, or misused. And IT must deliver on both these requirements without incurring extra cost, increasing complexity for users or IT, or compromising performance of applications or the network. Fundamentally, the network needs to get smarter about users and applications for IT to be able to satisfy all these competing demands.

The Medical Director, for example, noted that today's situation is very different from the old environment in which you used to trust everybody and you could confidently say "This is your campus and you own it." Part of his challenge is that six thousand people a day access his network – a combination of nurses, doctors, students, patients, visitors, and contractors. Driven in part by HIPAA (Health Insurance Portability and Accountability Act) requirements, the hospital must protect the health information associated with its patients. As The Medical Director pointed out, "The best way to protect a patient's health-related information is to ensure that unauthorized people do not get onto the network."

Visibility is critical not just for keeping tabs on employee activity but also for basic IT troubleshooting.

The CSO pointed out that due to the change in the work force, your environment is not as trustworthy as it used to be. One of the goals of his organization is to "never have a security incident that starts from inside of the network that impacts production." He added that the old laissez-faire attitude of if you can access the LAN you can go anywhere "is an anathema to us" and that his organization makes sure that someone cannot just walk into a building of theirs, plug in their laptop, and gain access to resources that they should not be able to reach.

Another broad-based trend is that many enterprises are beginning to establish and enforce strict accountability policies, in part to meet regulatory demands and in part to ensure strong employee productivity. One common characteristic of regulations such as the Sarbanes-Oxley Act is that they require companies to better assure the accuracy, security, and confidentiality of data. Companies are also looking to ensure that IT resources are not being wasted on non-business related activities such as listening to Internet radio and, more importantly, are not being used for potentially illegal activities such as sharing copyrighted materials. The infrastructure itself must help provide this user accountability for IT to meet regulatory and employee productivity demands without creating too great an operational burden.

The Global Infrastructure Director agreed that managing accountability is important, although he pointed out that the vast majority of internal users are not malicious. "User ignorance causes employees to do things where they have no idea of the consequences. For example, it is very easy for people to get themselves a file sharing application. Now, not only are they using lots of bandwidth, but all they need to do is to click on the wrong file or directory, and suddenly they're sharing very sensitive information," he notes.

Virtually every organization is under pressure to become more agile, which in turn requires organizations to rapidly adopt new technologies and applications and shift where and when they do business. As noted, one approach to increasing business agility is to adopt an SOA. Part of the value proposition of an SOA is that it enables companies to more rapidly deploy new business processes and the applications that are necessary to support them. This agile business and application environment must be supported by an agile, high-performance, services-based network infrastructure or else the network infrastructure becomes a roadblock to the company being able to achieve its business goals.

The InfoSec Director's business process outsourcing company provides back-office functions such as human resources, procurement, accounting, and IT for customers in a variety of industries. The company has grown through partnerships, in some cases taking over existing back-office systems for customers. The InfoSec Director pointed out that, "We need to support a large, constantly evolving set of requirements, and to drive the business forward, the adaptability of the network is extremely important to us."

Dealing with the requirements of efficiency, accountability, and agility is difficult in any environment but is made even more difficult when an enterprise has global operations. The Global Infrastructure Director highlighted that "As networks become more global and dispersed, there is a need to push much wider access to critical resources to the edge of the networks. In many cases we are doing this blind, with little knowledge of the experience of the users. In some cases we are rolling out network access to countries that have not have been connected before and to users that have a very different view of corporate information. For example, we're deploying networks across some continents where the users sometimes have little regard for copyright and intellectual property. As a result, we have to provide network access to unknown users with unknown behavior in unknown environ-

ments, but we absolutely must know what they are doing."

The interviewees also noted that visibility is critical not just for keeping tabs on employee activity but also for basic IT troubleshooting. IT must be able to rapidly identify the user and application involved in a network issue to solve that problem in a timely fashion, getting that employee back to work and using IT resources efficiently.

Intelligent Switching: Building a LAN that Meets the New Business Challenges

Businesses coping with today's challenges need new services in their LANs to more tightly align the network to the business. This need for intelligence has already driven changes in other parts of the network. For example, data center switches have evolved to become application aware to solve problems such as protocol performance issues. At the LAN/WAN boundary, WAN optimization appliances provide application acceleration by employing techniques that mitigate the inefficiencies of chatty protocols.

That same kind of intelligence is now needed in the wiring closet, with switches that are inherently aware of users, their roles, and the applications they're running. The switches must understand the context of each network flow and then be able to apply policy based on that information. Businesses can then leverage this understanding of user identity and role, tied to applications, to provide:

- Differentiated services to applications and users
- Improved security through controlled user access to the network and its resources
- Collection of the data that can support accountability policies

The link among users, roles, and applications must be made at the LAN edge, where traffic flows initiate, and must also incorporate the policies for what each user is allowed to access. Given the increase in collaborative, peer-to-peer, and other applications that don't follow the traditional "hub-and-spoke" architecture, user and application control require intelligence to be applied at the LAN edge. Also, this mapping of user to role and application as the basis for policy enforcement needs to be as automated and as simple as possible to administer to avoid labor-intensive and error-prone manual configuration of individual user profiles.

A critical way for IT organizations to apply application and user awareness and control is through enhancing the intelligence of wiring closet switches. As pointed out by The Global Infrastructure Director, "You need to be able to be able to see when someone plugs an iPod into a USB port and suddenly copies 8,000 songs to a corporate server." He added that, "Trying to deal with things after the event is not a solution – you need to deal with things in real time." Just as previous waves of LAN advances were driven by groups of innovative vendors, intelligent switching, with its user and application control, has its own set of pioneering vendors including Enterasys, HP, and ConSentry Networks.

LEGACY VS. INTELLIGENT ARCHITECTURE

	Legacy Architecture	Intelligent Architecture
Performance	Wire speed	Wire speed
Latency	Micro-seconds	Micro-seconds
Hardware	Fixed	Programmable
Processing	Packet-based	Flow-based
User context	IP address	Identity, device, role
Application Detail	Limited to L4	Rich L7+ detail
Access Policies	Complex - VLANs/ACLs	Dynamic - by user/role/app
Security	Overlay, external apps	Embedded
Audit/troubleshoot	Sampled L4 Data	Full user/app/resource data

Bottom Line: The legacy switch architecture cannot support intelligent switching.

Requirements for Wiring Closet Switch Upgrades

So given the requirements that have arisen from changing business practices, and the need for newly deployed switches to serve in the network for the next five to seven years, what should enterprises look for in their next wiring closet switch upgrade? The required features fall into two main categories – the set of "table stakes" features, that is the functionality access switches have long needed to provide, and a new set of emerging features to meet the business's changing requirements.

The table-stakes features include wire-speed, low-latency, multi-gigabit performance, irrespective of what services have been configured. Therefore all packet processing in the forwarding path must be done in hardware. Access switches must also support all commonly used L2/L3 features, including QoS, 802.1Q VLANS, link aggregation, and STP/MSTP/RSTP. Standard 802.1p QoS marking for prioritization of latency-sensitive applications and key business applications is needed, as are basic security features, such as authentication. The need for standards-based Power over Ethernet (PoE) on access ports is key to serving wireless and VoIP demands, and basic management via CLI and web interfaces is needed for operations.

The four IT professionals interviewed make clear, however, that this set of basic switch features is insufficient. The Global Infrastructure Director noted that "In today's environment, IT organizations need the LAN to watch employees and, among other things, decide whether the applications

they're using are appropriate." The Medical Director noted that Layer 7 deep packet inspection is something he requires in a LAN switch because "there are just too many attacks and too many security holes in applications."

The CSO stated that, "Having intelligence in the local infrastructure is clearly becoming essential not just for security but also for providing visibility and the ability to tune the environment. So automated role derivation is key. If we do not understand who is talking to whom and what traffic is legitimate, how can we possibly identify an anomaly?" The InfoSec Director commented on the rapid rate of change, noting that "programmability in a LAN switch is important to us. We want to make sure that any switch we acquire has enormous potential for expansion."

The four interviewees collectively named several additional features needed to provide user and application control on the LAN. But they also stressed the need for maintaining simplicity – interoperating with existing identity stores, for example, or automatically discovering non-user devices such as robots and applying intelligence about what those devices are able to do on the network. Intelligent switching, therefore, cannot come at the cost of increased complexity in the deployment and operation of the LAN.

Having intelligence in the local infrastructure is clearly becoming essential not just for security but also for providing visibility and the ability to tune the environment.

The features the interviewees cited include:

- Layer 7 Deep Packet Processing is needed to perform the per-flow analysis that tracks traffic flows and ties them to both the application and the user. Packet processing up to Layer 7 at multi-gigabit wire speeds requires extensive hardware-based horsepower.
- Extensibility/Programmability of the packet processing engine is necessary to allow the switch vendor to keep pace with changing requirements for application intelligence and network security. So the switch's packet processing needs to be based on programmable ASICs and/or multi-core CPUs that support wire-rate performance but can still be modified to support new services.
- Automated Role Derivation identifies users and devices and maps those identities to roles based on data in existing identity stores. This mapping then serves as the foundation for applying policies for which servers and applications the users and devices can access.
- Automated Enforcement of Policies for QoS and security ensures that the switches can enforce policies without IT needing to manually change VLAN memberships or ACLs.
- Anomaly Detection allows the switch to determine when user behavior or application traffic is sufficiently outside the norm to warrant IT attention or even to block the flow. Anomaly detection requires Layer 7 DPI, flow tracking, and automated role derivation.
- Simplicity of Operation leverages automation and other productivity features to ensure that intelligent access switches are as easy to install and run as those using the legacy switch architecture, despite their enhanced functionality. In addition to offering simple user and application control, they must also make visibility into and tracking of what's happening on the LAN much more accessible, with users and applications named and business context readily clear.

In talking with the interviewees about their business challenges and their need for these features to address them, it's clear that many of the features interrelate. For example, role and application and QoS policy all must intersect, so that new forms of prioritization can happen. Calls into the customer service staff should be given higher priority access, for example, than internal calls or playback of training videos.

Summary and Call to Action

Business practices are constantly changing. The need for greater efficiency, the drive toward stricter accountability processes, and the demand for better agility are just a few current examples. To support continually evolving business practices, IT organizations need to migrate to intelligent switching to gain user and application control. The legacy switch architecture cannot support the capabilities fundamental to intelligent switching, so IT organizations intent on delivering infrastructure that better supports the business must use switch upgrade cycles to gain the needed features and make intelligent switching the building block of their LAN.

ABOUT ASHTON, METZLER & ASSOCIATES

Ashton, Metzler & Associates is an industry leading consulting group focused on assisting organizations improve their performance by leveraging Information Technology and Human Talent for Success.

ABOUT THE AUTHOR

Dr. Jim Metzler

Dr. Jim Metzler is a widely recognized authority on both network technology and its business applications. In over 28 years of professional experience, Jim has assisted vendors in refining their product and service strategies, and has helped numerous enterprises evolve their network infrastructure. He has been a compiler writer for a branch of the US intelligence community; created software tools for designing customer networks for a major IXC; an Engineering Manager for high-speed data services for a major Telco; a Product Manager for network hardware; as well as managed networks at two Fortune 500 companies. He also directed and conducted market research at a major industry analyst firm; and has run a consulting organization.

Jim holds a Ph.D. in Numerical Analysis from Boston University. He has co-authored a book, published by Prentice Hall, entitled "Layer 3 Switching: A Guide for IT Professionals". Jim teaches a course at Interop entitled "Running IT as a Business". He has been the keynote speaker on seminar tours produced by Network World, Cisco, Nortel, DEC, Cabletron, and NetScout.

Ashton, Metzler & Associates
P.O. Box 1640
Sanibel, FL 33957
239-395-3152