Is Your Network Ready for the 21st Century?

An Analysis by Jim Metzler and Steven Taylor

Introduction

IT organizations don't significantly alter their approach to something as critical as network design based on minor changes in either business or technology. For example, no rational IT organization would make a significant change in their approach to LAN design simply because they were in the process of making a modest deployment of WLANs. In that case, they would do what IT organizations always do – bolt a fix onto the existing LAN design.

However, after several "minor" changes occur, there comes a time when it is necessary to reconsider the network design rather than to continue to bolt fixes onto the network. For instance, the need to support new traffic types (such as video) is one of the factors driving the current transition in network design. Other factors include the ongoing need for more effective security, the increasing impact of industry and governmental regulations, the demand for new applications (such as collaboration), and the movement towards Green IT and IP storage.

This need for a fundamental shift in network design is part of an on-going cycle. A decade ago the movement from shared media to switched Ethernet was driven by two fundamental requirements – the need for higher availability and enhanced performance. By contrast, the current environment adds a focus on services and functionality as well. This causes a fundamental paradigm shift from viewing the LAN as a relatively unintelligent factor in a flat network to its being the heart of a hierarchical, extremely intelligent network with full functionality to support a wide range of current and future requirements.

This paper addresses both the factors driving the need for change and the requirement for adopting a more intelligent network design.

Implement Sophisticated Security

It would be difficult to overstate either the dramatic growth in the number of security incidents or the importance of security. Relative to this increase in security incidents, twenty years ago Carnegie Mellon University's Computer Emergency Response Team (CERT) was just being established and now it catalogs roughly 8,000 new security vulnerabilities a year.

Because of this intensified importance of security, Webtorials' Editorial/Analyst Division recently conducted a survey in which one of the goals of which was to identify the importance of various security issues. IT professionals who responded to the survey were presented with

roughly a dozen security issues and asked to indicate the importance of those issues. Table 1 shows the five issues that were the most important to the survey respondents. In Table 1, the phrase *criticality index* refers to the percentage of survey respondents who indicated that the issue was important, very important, or critical.

Issue	Criticality Index
Implementation and operation of the capability to defend against all current security threats	94.7
A disaster recovery plan that enables the organization's key processes to function after a disaster	91.8
Protection against viruses for which there are no current definitions	88.6
Providing secure remote access to both employees and partners	88.3
Applying software patches in a timely fashion with minimum resource and system impact	87.5

Table 1: The Criticality of Security Issues

The data in Table 1 highlights the fact that security remains a top-of-mind issue for virtually all IT organizations.

Attaching to the corporate network is one of the *de facto* methods by which people gain access to a company's IT resources. As such, network access must be secured or else all of the company's IT resources are at risk. The difficulty, however, of securing access to the network is complicated by the rapid deployment of a wide range of computing resources – from Personal Digital Assistants (PDAs) to PCs to smartphones – which are being routinely used for a mix of personal and business computing. Furthermore, the applications on these devices often use peer-to-peer communications that bypass traditional security technologies such as firewalls. And while many organizations have developed personnel policies regarding mixed use of company resources for work-related and personal activities, in order for these policies to be effective, a network that can help enforce them must be in place.

Given the overall importance of security as well as the criticality of securing network access, it is mandatory that IT organizations include security as an integral part of their network design. IT organizations that do not make security an integral part of their network design:

- Do not have effective protection against zero day viruses
- Cannot apply patches in a timely fashion
- Cannot control who has access to the corporate resources
- Are at risk to the over 8,000 security vulnerabilities that are discovered each year
- Can not comply with industry and government regulations

In addition, IT organizations must make security an integral part of their network design so that they avoid incurring the extra cost and complexity associated with bolting security-oriented workarounds onto the existing network.

Compliance with Industry and Government Regulations

There have been thousands of industry and governmental regulations implemented in the last ten years. Some of these regulations are relatively obscure and industry-specific while others are very well known. Table 2 highlights some of the better-known regulations.

Regulation	Impact
Sarbanes-Oxley Act (SOX)	Requires management to make a written assertion stating their responsibility for establishing and maintaining an adequate control structure and procedures for financial reporting.
Health Insurance Portability and Accountability Act (HIPAA)	Requires companies in the health care industry to provide administrative simplification, security, and privacy.
Payment Card Industry (PCI) Data Security Standard	Defines an expanded set of requirements for the protection of credit-card information, including encryption, access control, physical security and operational audits. This standard requires that a certified auditor test public networks and Web sites frequently and regularly for compliance.
System Docket No. R-1128, Office of the Comptroller of the Currency	Requires financial services firms to develop and implement plans for business continuance and disaster recovery (BC/DR).

Table 2: Key Regulations

Many of the regulations that have been enacted in the last ten years have a security focus. As such, these regulations are one more reason why IT organizations need to increase the security of the network by adding functionality such as strong authentication, network access control and encryption of data both in transit and at rest. However, as noted in Table 2, some of these standards also include a requirement to conduct regular audits and for higher network availability and throughput in part to be able to support business continuity and disaster recovery (BC/DR).

Failure to comply with industry and government regulations can result in:

- Heavy fines
- Imprisonment
- Loss of corporate reputation
- Loss of customers and partners

No CIO wants to be responsible for the company failing to comply with industry and government regulations just because security is not tightly integrated into the network, or the network is not robust enough to support BC/DR.

Support Effective Collaboration

One of the reasons that collaboration has become so important is that companies today have a more distributed workforce than ever before. In most instances, the productivity of the workforce depends on the ability to work together on common projects as well as the ability to share knowledge and build consensus as quickly and easily as they could if they were all collocated. In addition, most companies have business models that require them to collaborate with a variety of outside entities. This includes any company that has outsourced one or more key business processes, that performs joint development, or that has implemented processes such as supply chain management.

There is a wide range of collaboration tools, including traditional video conferencing as well as telepresence. In addition, Web 2.0 has ushered in a new generation of collaboration tools including wikis and blogs. Web 2.0 has also ushered in a collaborative approach to application development based on mashups[1].

Failure to design a network robust enough to support collaboration tools such as video conferencing, telepresence and mashups results in:

- Lower employee productivity
- The inability to effectively interact with outside entities

The impact to the business is subtler than the impact of failing to comply with industry and government regulations. It is, however, just as significant.

Implement Wireless LANs (WLANs)

As demonstrated in recent market research[2], the vast majority of IT organizations have already deployed WLANs. When many IT organizations initially implemented WLANs they used an overlay design in which traffic flowed between a non-intelligent access point (APs) and WLAN switches through the wired LAN. In this model, the WLAN switches handle encryption, security and QoS policies.

In order to support an increasingly mobile workforce, today's LAN design must support complex tasks such as seamless roaming in a campus environment. As a result, a given user session may traverse multiple access points and switches. In a growing number of situations, WLANs are being deployed in a metropolitan area. A key component of a successful metropolitan area deployment of WLANs is the use of protocols that enable a mesh network design.

The first generation of WLANs was focused on supporting purely data applications. The design focus of WLANs, however, is expanding and now typically includes the requirement to support voice traffic. This requirement drives the need for network performance characteristics that are fundamentally different from the performance characteristics of a data-only network.

[1] A mashup is a web application that combines data from more than one source into a single integrated tool. http://en.wikipedia.org/wiki/Mashup_(web_application_hybrid)

[2] 2007 Wireless LAN State-of-the-Market Report, http://www.webtorials.com/abstracts/KubernanSOTM07-03.htm

For example, the requirement to support voice dictates the need for implementing Quality of Service (QoS) in the LAN. In addition, it is becoming increasingly common to use dual mode phones. As a result, another requirement driven by the need to support voice is the ability to support a smooth handoff between a WLAN and a cellular network.

An overlay WLAN design with non-intelligent APs will not support demands such as:

- Roaming
- Mesh networks
- Dual mode phones
- QoS
- New technologies such as 802.11n

Deploy Network and Application Optimization

A recently released extensive report[3] highlights that application performance is a top-of-mind issue for virtually all IT organizations. One of the factors that complicates the task of ensuring acceptable application performance is the fact that the majority of IT organizations are consolidating servers out of branch offices and into centralized data centers. In addition, many organizations are also reducing the number of data centers they support.

The combination of server consolidation and data center reduction results in the vast majority of users accessing an application over a lengthy WAN link. Typically, lengthy WAN links have high levels of delay, jitter, and packet loss, all of which can contribute to poor application performance. Further complicating the issue is the fact that server consolidation typically results in protocols such as CIFS (Common Internet File System) running over the WAN. CIFS, which was designed to run over a LAN, is a chatty protocol. In particular, CIFS decomposes all files into smaller blocks prior to transmitting them. The server sends each of these data blocks to the client where it is verified and an acknowledgement is sent back to the server. The server must wait for an acknowledgement prior to sending the next data block. As a result, opening a file that would take a fraction of a second before consolidating servers would take tens of seconds after the server consolidation.

Historically IT organizations have responded to performance problems by adding WAN bandwidth. While there are situations in which that is the right approach, adding WAN bandwidth does have two significant limitations. First, adding WAN bandwidth can be expensive. It might, for example, be less expensive to add compression and caching functionality to the network. The second limitation is that in many cases adding WAN bandwidth does not result in acceptable performance. For example, assume that a file was being opened over a WAN and that CIFS decomposes the file into 200 blocks. Further assume that the round trip WAN delay is 100 ms. Then, independent of the bandwidth of the WAN link, it will take at least 20 seconds to open the file. The time it takes to open the file, however, can be reduced significantly by adding functionality such as look-ahead and spoofing to the network.

[3] The 2008 Application Delivery Handbook, Jim Metzler, http://www.webtorials.com/abstracts/Kubernan2008handbook.htm

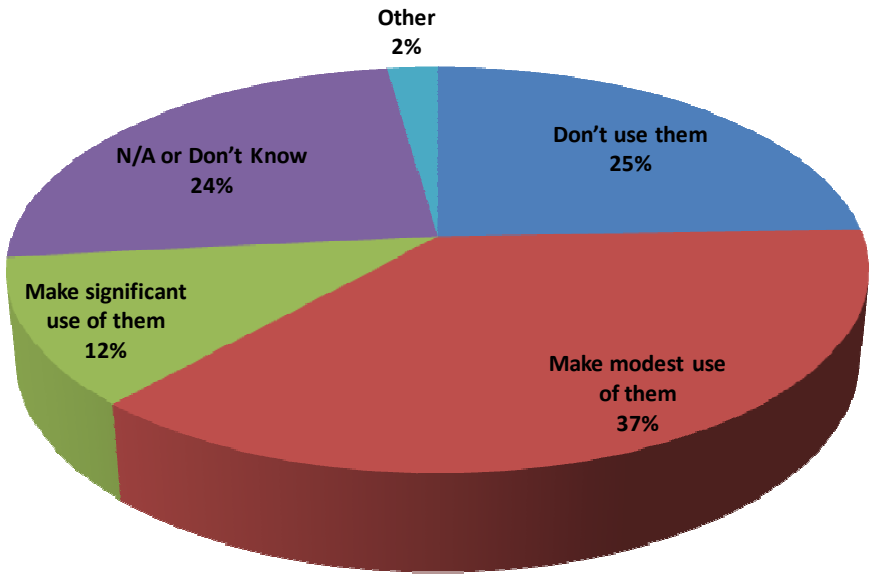
As noted, the majority of organizations are consolidating servers and reducing the number of data centers. The network needs to be upgraded with functionality[4] that will allow it to support BC/DR and collaboration. This functionality includes having the network be able to recognize applications and prioritize them based on their business criticality and time sensitivity. Not upgrading the network with this functionality creates the real possibility that the organization will:

- Overpay for its WAN
- Be unable to consolidate its servers into centralized data centers
- Be unable to reduce the number of data centers
- Experience degraded application performance
- Be unable to control what applications transit the network
- Pay more to support initiatives such as BC/DR
- Experience degraded server availability and performance
- Be unable to support collaboration

Enable New Application Architectures

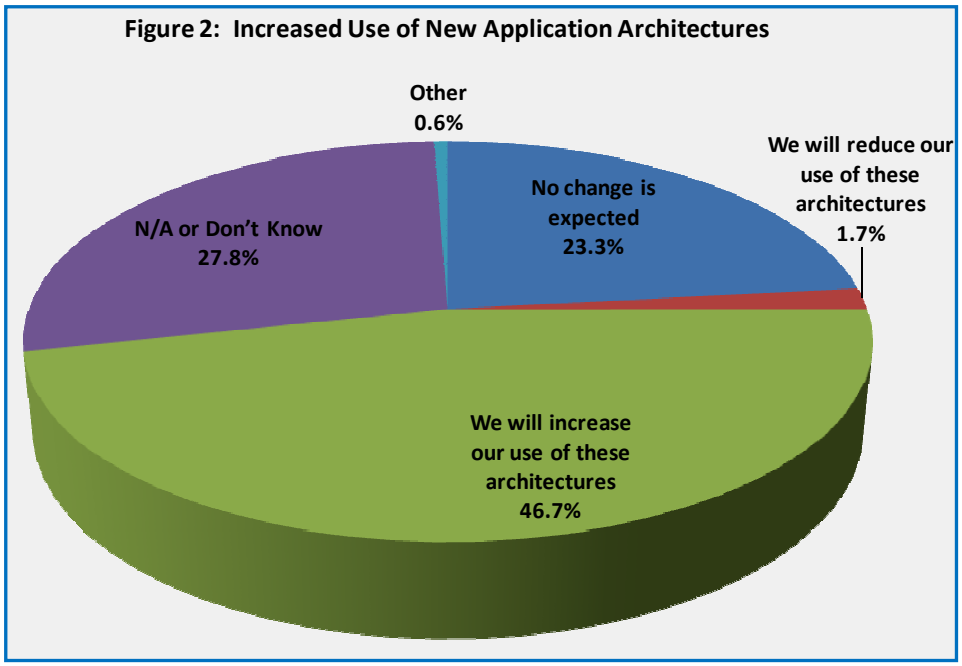
Webtorials' Editorial/Analyst Division recently presented over 200 IT professionals with this question: "Which of the following best describes your company's approach to using new application architectures such as Services Oriented Architecture (SOA), Rich Internet Applications (RIA), or Web 2.0 applications including the use of mashups?" Their responses are shown in Figure 1.

Figure 1: Current Use of New Application Architectures



The same group of IT professionals was then asked to indicate how their company's use of those application architectures would change over the next year. Their responses are shown in Figure 2.

[4] An extensive discussion of the required functionality can be found in The 2008 Application Delivery Handbook, pages 24 – 42, http://www.webtorials.com/abstracts/Kubernan2008handbook.htm



The data in Figures 1 and 2 demonstrates the great interest in the emerging application architectures. These new application architectures will make significant demands on the network. For example, a Rich Internet Application is typically designed around multimedia. The associated network challenge is to redesign the network to support multimedia in a way that allows an RIA to achieve its goal of creating a personalized experience to both increase customer satisfaction and make users more productive.

One of the reasons why companies deploy an SOA is that it helps make the business more agile. As part of an SOA, an application comprises a number of Web services. These Web services typically reside on separate servers that may or may not all be in one data center. In order to not degrade application performance, the network must provide a level of performance to those Web services that is equivalent to what they would receive if they all resided in a single server.

Similar to the SOA challenge, the network must provide a level of performance to Web 2.0 mashups that is similar to what it would receive if the components of the application resided in a single data center.

If IT organizations fail to upgrade their networks to provide the performance and QOS required to support emerging application architectures, their companies will not be able to reap the benefits of these new applications. In particular, these companies will not be able to:

- Increase customer satisfaction
- Become more agile
- Increase customer productivity

Migrate to Green IT

"Green IT" refers both to using IT to conserve energy and to using computing resources efficiently. It also refers to the reduction of carbon emissions and the appropriate handling of hazardous waste. Green initiatives not only benefit the environment, but they significantly reduce operating costs. Additionally, companies are increasingly under pressure from their customers to do business with other "Green Companies."

IT organizations can implement green solutions in any part of the IT infrastructure. Many IT organizations start in the data center and focus on conservation and efficiency in network equipment, power systems, servers, storage, cooling systems, etc. However, significant efficiencies can also be found in branch offices, such as the integration of multiple network elements into small branch office routers resulting in lower power consumption.

There are many aspects of a network design that lend themselves to energy efficiency. For example, having a network that can support collaboration and hence reduce the carbon emissions associated with travel is one example. Other examples include implementing a network design that has a reduced number of network devices and implementing devices that are themselves highly energy efficient.

Failure to design the network to support green initiatives will not have an immediate dramatic impact. It will, however, have a big impact over the long term. In particular, IT organizations that do not implement green IT will:

- Continue to cause unnecessary harm to the environment
- Incur higher operating costs
- Cause their company to lose revenue

Implement IP Storage

The demand for storage is increasing, and is expected to grow for the foreseeable future. There are many factors driving the increasing need for storage. For example, the network is being used to store engineering and scientific data, including things like medical imaging, as well as to host videos, which are increasingly used for distance learning. Regulatory requirements are driving the need for increased storage. As a case-in-point, the Securities and Exchange Commission requires that all stock brokers keep complete records of all communications with clients. This necessitates that all phone calls are recorded and all email is archived.

While the estimates of the rate of growth in the demand for storage vary, the general consensus is that storage is growing at least forty to fifty percent per year. At this rate of growth, the demand for storage doubles roughly every eighteen to twenty-four months. One of the ways that some IT organizations are managing the cost of storage is by implementing a storage area network (SAN). A SAN enables a company to share storage among systems and hence increases storage utilization.

A SAN was traditionally built using Fibre Channel, which is an expensive and complex technology. To overcome the limitation of Fibre Channel, many IT organizations are beginning to use IP in the SAN instead of using Fibre Channel. The benefits of this approach have been well documented[5]. For example, redesigning the network to support IP storage:

- Reduces complexity based on leveraging common network hardware
- Reduces cost based on the price/performance of IP vs. Fibre Channel
- Enables interconnecting SANs

[5] Who's using IP Storage, and why? http://www.infostor.com

NOW is the Time for Action

In a time of moderate economic uncertainty, the tendency for many companies is to take an "ostrich approach" with their networking and to try to wait for the next boom before they upgrade their networks. But the successful company will look at this as a time to be proactive and to make a bold step to upgrade the networks in order to provide superior services at a lower total cost.

Business demands will not get simpler, and competition will not decrease. The best way to establish and maintain a competitive edge is with a bold initiative to upgrade your network design so you'll be ready for the next decade and its challenges.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com