



**IP SWITCH**

## **The Network *is* Your Business**

Why the network matters more than ever in today's real-time business environment.

<b>The Changing Networking Landscape</b>	<b>1</b>
<b>New Networking Technologies Take Center Stage</b>	<b>1</b>
Virtualization	1
Web 2.0	2
Wireless networks	2
Converging technologies	2
<b>The Role of the Network Administrator</b>	<b>2</b>
<b>How the Network Can Build Confidence in Your Business</b>	<b>4</b>
<b>Ipswitch WhatsUp Gold</b>	<b>5</b>
<b>About Ipswitch, Inc.</b>	<b>5</b>



# CONTENTS

# THE NETWORK IS YOUR BUSINESS

## The Changing Networking Landscape

From mainframes to thin clients to virtualized environments of servers, VLANs, and network gear, the network has grown both more complex and more important in recent years. What began as small, departmental networks that supported interoffice email and scheduling have grown exponentially to become today's multinational networks spanning companies, countries, and economies. Without the network to connect business processes, doing business as we know it today simply would not be possible. From e-commerce and email to VoIP, video, and collaboration, a strong, healthy, and well-managed network is vital to achieving business success.

Just as the technology and importance of the network have evolved, so too have the responsibilities and roles played by network administrators. Once associated solely with a support function located deep within the IT department, network administrators are now being challenged to play a larger, more visible, and more strategic role — one that leverages the network to support critical business goals and objectives, from increasing sales and customer service, to improving responsiveness and market leadership.

***“Spending on enterprise LAN Switch, Router, WLAN, IP telephony equipment and security appliances grew 17% to reach \$35.4 billion in 2006 spending.”<sup>1</sup>***

## New Networking Technologies Take Center Stage

As significantly as the network has evolved over the past 25 years, new networking technologies such as virtualization, Web 2.0, SOA, and wireless are poised to change the network environment even faster and more profoundly than any changes to date. As these new technologies proliferate and converge, they have the potential to alter the network like never before. Let's take a look at some examples:

***Server virtualization is now considered a mainstream technology among IT buyers. Although only an estimated 8% of deployed servers are virtualized today, most IT professionals surveyed in August 2006 expect to double the penetration of virtualized servers in their organization within 12 months.***

***With the adoption of virtualization, core infrastructure strategies are being turned upside down.<sup>2</sup>***

***Virtualization*** gives businesses the ability to dynamically relocate information assets like servers and PCs without physically touching the hardware. It also solves the long-standing challenge of decoupling hardware and software. Tactical virtualization allows you to move a backup server from Sacramento to Boston to respond to a server crash. Strategically, businesses can use virtualization to reposition servers to respond to business needs. For example, an e-commerce vendor based in the U.S. could move all database backups to Western European locations on Sunday morning and early afternoon in response to heavy sales processing volume from customers in that region. And with virtualization extending to LANs, Web servers, and e-commerce sites, businesses will be able to take advantage of enhanced manageability, speed, and security.

<sup>1</sup> Abner Germanow, IDC Link, Why Is Networking Growing Faster than the Rest of IT? Doc #1cUS20717207, June 04, 2007

<sup>2</sup> IDC Directions 2007, Enterprise Class Virtualization 2.0: Application Mobility, Recovery, and Management, Doc #DR2007\_5MEW, Feb 2007

But along with the benefits of virtualization come increased challenges related to the reliability of the network. By reducing the number of servers and devices, virtualization actually increases the risk factor for keeping each device up and running. The loss of a single physical server running 10 virtualized servers will have a much greater impact on your business. Security risks also come into play here as a single illegal access to your network or virtualized server could compromise a significant amount of computing power. Effective network monitoring is critical to the success of virtualization.

**Web 2.0** promises to transform websites from isolated information silos to rich, collaborative sources of content and functionality. As these new computing platforms enable Web applications, they will have an enormous impact on the growth of IP addressed devices. The increased numbers of mobile and always-on devices, coupled with the rapidly growing number of Internet users has led to projections that the pool of IP version 4 (IPv4) addresses will be exhausted sometime in 2010.<sup>3</sup>

In response, IPv6, with its larger address space of 128 bits versus 32 bits in IPv4, is gradually being adopted. The longer IPv6 addresses will increase the number of addresses available for networked devices, allowing for example, each mobile phone and mobile electronic device to have its own static IP address. But Web 2.0 doesn't stop with traditional computing devices. Imagine PCs built into products like kitchen appliances, cars, and other non-traditional devices. Each will require its own IP address and a way to access the network with reliable 24x7 uptime.

**Wireless networks** have exploded in recent years, with their convenience and accessibility quickly making them a must-have for users and businesses alike. WiFi and WiMAX are changing the way users think about their expectations for connectivity. The increased bandwidth and reach of WiMAX are enabling last mile connectivity for high data rates and providing a diverse source of Internet connectivity as part of a business continuity plan.

But wireless networks only work when they are supported by a strong wired network infrastructure. A wireless network with inconsistent performance will fail to support business processes and can lead to a lack of user confidence in the technology. As wireless grows in acceptance and becomes the preferred method of business communication, the need for a strong network backbone will only increase in importance.

**Converging technologies** like VoIP, video, and collaboration are poised to expand the network further, as users embrace new methods of communicating and sharing information. Just as email and instant messaging quickly became "killer applications" for businesses, these new technologies hold the promise of transforming the way businesses operate, but with even higher stakes. If the network fails during VoIP and collaboration communications, not only will those communications fail, but the business objectives tied to them may fail as well. Particularly with VoIP, video, and collaboration technologies, the network needs to have enough pipe to push all of this data back and forth consistently and reliably.

The user experience plays a huge role here as well. As boundaries have dissolved between the home and the office, and between countries and regions, users have come to depend upon the technology that allows them to speak real-time with customers, partners, and coworkers all over the world, just as if they were sitting next to one another. With this functionality now a natural part of modern communications, users won't be willing to give it up.

## The Role of the Network Administrator

Along with changes to the network, the role of the network administrator has evolved. As networks work harder to deliver the functionality that businesses require, expectations for network administrators have increased, with users and business line managers seeking greater accountability and responsiveness. Many network administrators have their salaries and bonuses tied to performance benchmarks. The challenges for network administrators in meeting these expectations include:

<sup>3</sup> IPv4 Address report. <http://www.potaroo.net/tools/piv4/index.html>

- Prioritizing the must-do list to focus on the critical tasks that impact the network and the business most directly, to increase revenue and profitability as well as customer and partner satisfaction. It is very likely that in the near future network administrators will have portions of their pay calculated on the profitability (P&L) of the business they work with.
- Lacking effective tools to monitor and manage the network, network administrators are often the last to know when a networked device goes down. The notification instead comes from customers or employees – obviously not an ideal situation.
- Service level agreements (SLAs) are becoming standard practice, with IT agreeing to deliver a specified level of service to users within the organization.
- Network administrators are typically responsible for an environment that has evolved gradually over several years, with devices and servers added to and removed from the network with little or no advance planning or notice. Effectively monitoring this kind of ad hoc networking environment is an enormous challenge and can often take a back seat to the important day-to-day challenge of keeping the network up and running.

To address these challenges network administrators must stop simply reacting to the network and start taking a more proactive approach to maintaining network health and anticipating downstream usage concerns. The first step in achieving this proactive approach is to establish a complete understanding of the network through a discovery process. If network administrators don't fully understand the network's scope, it won't be possible to manage it effectively – you can't manage what you don't see.

Discovery involves identifying all of the devices on the network: routers, switches, servers, printers, and all other networked devices. Discovered assets are then mapped to identify connectivity points and locate devices. Once network devices are discovered and mapped network administrators will have a better understanding of exactly what devices are on the network, the services enabled or not on the devices, device locations, and how they interact with other devices as part of business workflow processes.

With this information in hand, network administrators can turn their attention to monitoring the health, performance, and availability of the network. Anytime, anywhere network monitoring provides notification when problems occur on the network, and over time gathers network information that can be used for reporting, planning, and budgeting.

Reporting plays an increasingly important role in network management. As more business operations are tied to the network, business line managers must work closely with the network administrator to ensure that their customers and users have fast, uninterrupted access to the network. Business line managers require regular communications on the status and performance of the network and as a result they are building strategic new partnerships with network administrators to ensure they reach their business objectives.

### **Compliance**

The growth of regulatory compliance requirements has added another layer of complexity to the task of managing the network. A wide variety of industries now find themselves facing governmental regulations that require auditing capabilities. Integrating network management into a compliance strategy helps businesses comply with regulations like HIPAA, Basel II,

***“Savvy IT shops are driving the shift toward strategic and proactive network management practices. Factors such as video and voice over IP will force enterprises to understand their network capacity better than they do now prior to deployment. Proof of compliance will require enterprises to deploy tools that will provide reports that show what devices are in and out of compliance.”<sup>4</sup>***

<sup>4</sup> Tracy Corbo, IDC, “Worldwide Network Availability 2007-2011 Forecast and Analysis”, IDC, Doc #207662, July 2007.

and Gramm-Leach-Bliley, with user activity authenticated and archived safely on the network or distributed to a safe archiving depot. Businesses and network administrators must have processes in place to archive communications like email and instant messages and identify network access to records containing private individual information. Proactively managing compliance can help businesses avoid costly, time-consuming audits and remain focused on achieving business goals.

### **Security**

Security is vital to the health and performance of the network with threats coming from denial of service attacks, phishing, worms, viruses, and Trojan horses, just to name a few. It's critical that both the security devices at the perimeter of the network and on the interior are performing as expected. To aid in this process, security devices are increasingly manageable by SNMP standards that provide remote monitoring and configuration capabilities and help ensure the availability of authentication servers and firewalls.

### **How the Network Can Build Confidence in Your Business**

A fully and proactively managed network does more than allow you to operate your business – it builds confidence in your organization among customers and users. Email, IM, VoIP, and video are central to the way business communication occurs today, and the network is the mechanism that allows those communications to happen – naturally, easily, and perhaps most importantly, uninterrupted.

High expectations have become a marketplace reality. Compare network performance expectations to those of cellular phone users. Just a few years ago, dropped calls were tolerated because consumers had the expectation that they would happen. Today, consumers have little tolerance for dropped calls and leading cellular operators are making uninterrupted performance the principal component of their brands. The same is true for networks and the administrators who manage them – the tolerance for less than high performance simply doesn't exist. Network administrators interested in long-term employment are embracing the high expectations mission tightly.

The health of the network depends on effective performance monitoring, security, and compliance that allows business line managers to turn network data into actionable business information. These managers are directly accountable for the performance of the network and need to know how the network is performing today and how it will likely perform in the future. Is network traffic and capacity increasing? Is it time to budget for new hardware? Does partitioning the network make sense?

As network administrators transition from a strictly tactical role in the company toward a more strategic contribution, the importance of network performance is becoming a leading concern for executives throughout the organization. Effective network monitoring capabilities will continue to play an important part in the health and success of business. Network administrators and business line managers must create a new partnership that aligns network performance with business objectives. This collaboration between network administrators and business line managers will be an essential component of business success.

## Ipswitch WhatsUp Gold

Ipswitch WhatsUp® Gold delivers comprehensive and easy-to-use application and network monitoring that allows you to turn network data into actionable business information. By proactively monitoring all critical network devices and services, WhatsUp Gold reduces costly and frustrating downtime that can impact business. With an all-new Web-based interface, WhatsUp Gold lets you take control of your network infrastructure and applications for the important strategic work that drives results. In a marketplace overwhelmed with complexity, WhatsUp Gold provides simple deployment, robust scalability, groundbreaking usability and fast return on investment.

WhatsUp Gold isolates network problems and provides awareness and understanding of network performance and availability. WhatsUp Gold:

- Discovers and maps all your network devices
- Notifies you when problems happen on the network
- Gathers network information over time and generates reports
- Provides anytime, anywhere network monitoring

In addition, WhatsUp Gold delivers all the tools you need to monitor and manage your network, including dynamic network discovery and mapping, fast problem resolution, and comprehensive SNMP and WMI network monitoring and reporting.

For system and hardware requirements, or to learn more about WhatsUp Gold, visit [whatsupgold.com](http://whatsupgold.com).

## About Ipswitch, Inc.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to monitor their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading Ipswitch WS\_FTP® Professional client and Ipswitch WS\_FTP Server and communicate via Ipswitch IMail Server. To view the Daily Network Monitor blog, visit [dailynetworkmonitor.com](http://dailynetworkmonitor.com). For product and sales information, visit [ipswitch.com](http://ipswitch.com).