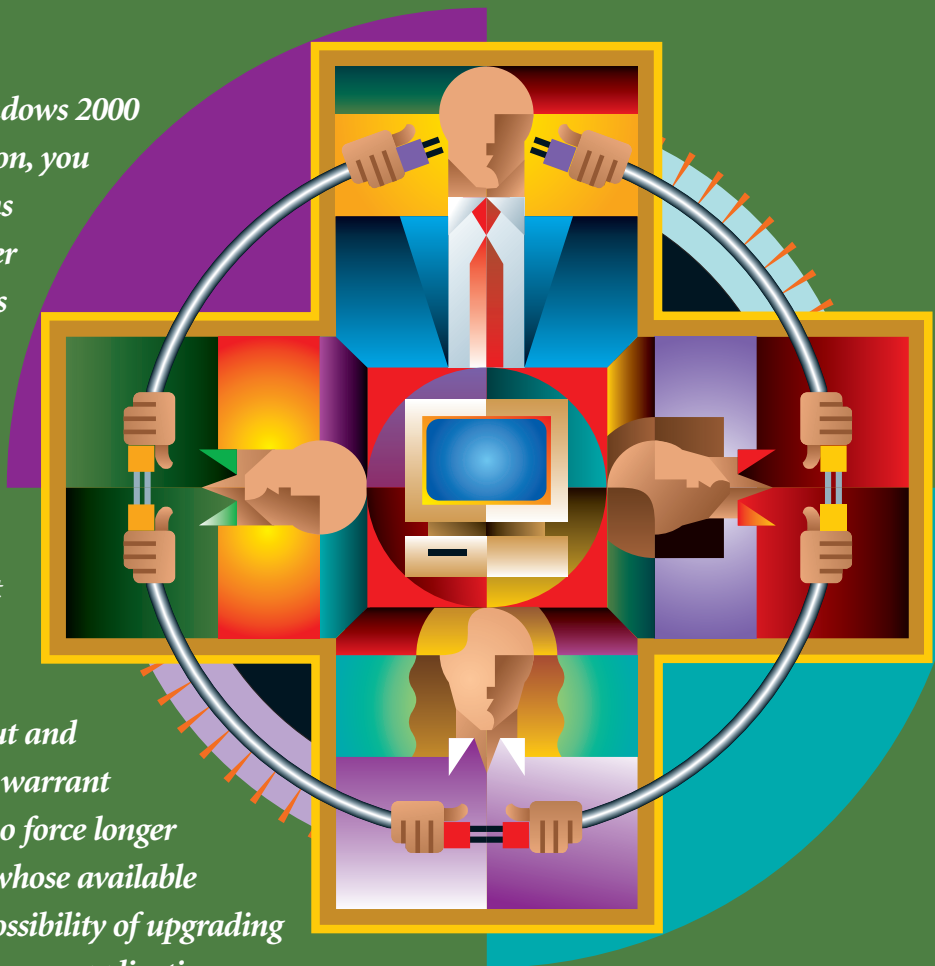


# Systems Administrators: Doing More with Less during Tough Times

By MARTY SCHER

*Unless you have been supporting Windows 2000 and Windows NT networks in isolation, you won't be surprised to hear that systems and network administrators are busier than ever. Corporate belt-tightening is affecting even normally recession-resistant IT groups, many for the first time, and is requiring that IT support more, increasingly complex, systems with fewer resources. The current economy has reduced, but not eliminated, the need to purchase, implement, and manage new technologies. Equipment does wear out and increased capacity requirements may warrant upgrades. Budget trimming might also force longer retention of older computer systems, whose available hardware resources might limit the possibility of upgrading to a more stable OS and easier-to-manage applications.*



**O**n the upside, certain industry trends are providing some much-needed breathing room for busy Win2K and NT administrators. Many companies continue to postpone Win2K server upgrades and the implementation of Active Directory (AD). These delays give IT more time to research AD architecture designs and the possible radical reconfiguration of existing NT networks, including Windows XP clients; and to review Microsoft's .NET strategy and the integration of its vast array of complex products. Also, in the ongoing battle for the network OS (NOS) market, Microsoft still manages to easily hold its ground in the Windows/Linux war. This news alone should let support

teams breathe easier, because it spares them from having to learn different NOS technologies and how to integrate them with existing legacy systems.

Despite this potential breathing room, however, IT undoubtedly will be working this year with fewer people and fewer technical resources. The bottom line is that regardless of the head count, systems still need support and customers still need the highest level of service. This article looks at three areas—network management tools, security, and communication—that continue to concern IT and explores how IT can do more with less.

## Network Management Tools

As more IT departments begin to flatten NT network domain structures and migrate to Win2K and AD, administrators should begin to see a much needed centralizing of user-account security management functions. For companies not yet ready to upgrade to AD, or that are using a mixed-mode environment, many tools are available to assist in centralizing Win2K and NT user-management functions. To expand on the native Win2K and NT user account tools, products such as UserManagementNT (<http://www.tools4ever.com>) offer industrial-strength tools for bulk user account creation and maintenance. If you require central control of user

security settings, take a look at NetPulse 2000 (Labcal Technologies, <http://www.labcal.com>), which provides the ability to define and configure enterprise-wide user security policies from within one software application.

On the hardware front, although Win2K and NT server hardware is more reliable and powerful than ever, equipment degradation and failure does occur. But like nearly every other corporate function, system downtime is no longer an option. Unless the support team has a crystal ball, monitoring the event logs of dozens, and maybe hundreds, of Win2K and NT servers can be nearly impossible. Fortunately, most enterprise server vendors integrate system monitoring and alerting capabilities into their server products. These tightly integrated hardware and software tools constantly monitor the health of servers, standing guard to quickly alert support personnel in the event of even a minor problem that could affect server operation. Compaq's Insight Manager (<http://www.compaq.com>) is a leader in server status reporting. This free software tool is included with Compaq servers and offers extensive fault, configuration, and performance management and alerting.

Resources also are available to help you address and correct OS security and stability issues. No OS is perfect; every version of Win2K and NT has had its share of problems. An important consideration when dealing with Microsoft or other vendors is how quickly they publish a fix when problems occur. Microsoft, usually no lumbering giant when it comes to moving quickly, is smart enough to realize that major problems, especially major security problems, make for very bad PR, so the company is swift to own up to a problem, release a fix, and disseminate needed information. The wise Win2K and NT administrator subscribes to the Microsoft security notification email service (<http://www.microsoft.com/technet/security>). This free service can save the day in the event of a major security issue, giving you the edge to correct a problem before it gets out of hand. One potential benefit from working with Microsoft products is that if you encounter

a problem, you are probably not the first to do so; you can pursue many avenues to resolve the problem. Paid Microsoft support is one way to go, but other methods are also useful and sometimes more expedient. Many Web sites supporting one or more Microsoft products include support tips or user forums that can help you resolve unusual problems. Fans of Microsoft Technet, which provides monthly driver updates and technical information about virtually every Microsoft product, gladly renew their annual subscriptions. The ability to quickly search an extensive knowledge base might help you resolve a tough problem within minutes. Although the same knowledge base information is available free from Microsoft's Web site, Marty's law states that your Web link will crash at approximately the same time as your NT server; having the information on-site could be a big plus.

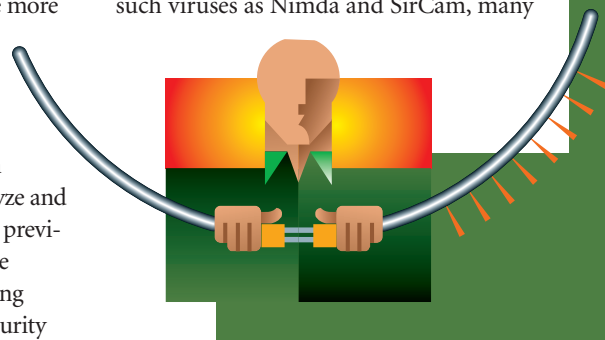
Having the right tools can also help you avoid or quickly resolve network traffic problems. With the large increases in video, voice, and data traffic, bottlenecks might develop in corporate networks. Tools designed to monitor and track traffic levels and troubleshoot problem areas will become increasingly important. Some Microsoft server products include a version of the Network Monitor application, which captures network traffic for display and analysis and lets you perform tasks such as analyzing previously captured network data packets using user-defined methods, extracting data from defined protocol parsers, and analyzing real-time traffic on your network. Third-party vendors offer more advanced software tools to monitor LAN traffic. For example, Observer, from Network Instruments (<http://www.networkinstruments.com>), includes the ability to use agents for monitoring remote networks and trend analysis. One of the more useful functions of these valuable tools is their ability to perform trend analysis, gathering and comparing traffic levels over a period of time. If your network appears to run slower on certain days, you can analyze and compare traffic levels captured from previous periods. Then you can determine whether any trends in network loading might cause problems. Also, data security

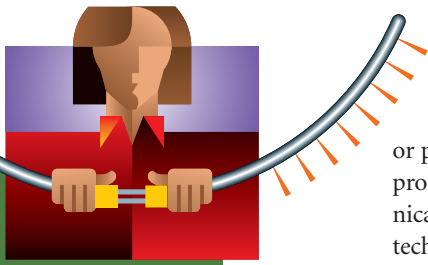
teams might use network-monitoring tools to check individual packets for possible security problems.

### Dealing with Security Problems

If any good has come from the terrorist events of 2001, it is that they served as a wake-up call for everyone involved in technology, underscoring the need to increase data security and the importance of developing, documenting, and testing a Business Resumption Plan (BRP). The speed with which a company can resume operation after a partial or total business disruption is crucial to its survival and continued success. Something as seemingly innocuous as a broken water pipe could destroy a business, especially if the only backup tape of the company's valuable data is floating in a puddle of water. Developing a BRP lets companies review their vulnerabilities, determine replacement resources, and create a plan of action in the event of a business outage. You can develop a simple BRP inhouse; for larger requirements, including compliance with government regulations, you can consult specialty vendors such as North American Emergency Management (NAEM) (<http://www.naem.com>), which can assist in developing and implementing a BRP.

Although certainly less deadly, but still damaging to businesses, is the continuing threat of techno-terrorist acts, including the costly spread of email viruses and Denial of Service (DoS) attacks. Computer viruses, which were originally code based and were usually spread by jumping from floppy disk to floppy disk, have reached the big leagues by running as network-capable macros that have the capability to infect millions of PCs within hours. With the widespread outbreaks of such viruses as Nimda and SirCam, many





companies have felt the pain (and expense) of crashed email servers and lost user productivity. Many IT departments literally found themselves scrambling for control as these viruses spread through their networks.

One of the best ways to control these mass infections is to implement a virus-scanning solution that monitors and protects all email points of entry. Trend Micro (<http://www.trendmicro.com>) offers an Exchange add-on product that monitors all email messages, both inbound and outbound, in real time. When selecting a product, keep in mind that response time is of the essence when dealing with this new breed of viruses. One of the most important features to consider when selecting a virus-protection product is the vendor's ability to address a new virus threat quickly and then automatically update the virus pattern file to your email servers.

On another front, Web-based DoS and other server attacks are becoming more common and can have a disastrous effect on both Internet and intranet Web sites. A DoS attack happens when a virus or other rogue process causes multiple Web servers to unknowingly send network packet floods to a targeted Web site, overloading its server, router, and other network resources, which in turn might slow or completely disable the site. To protect your Web server infrastructure, consider implementing a Web security solution such as Network Associates' (<http://www.pgp.com>) risk-assessment product, CyberCop Scanner, which is designed to continuously run on your network, monitoring and testing Web site vulnerabilities.

### **Increasing Productivity through Communication**

In today's light-speed business environment, communication, both internal and with customers, is as important to the success of a company as any data system

or productivity application. Increasing productivity through enhanced communication between corporate personnel, technical support team members, and customers has never been more important. Using tools that enhance communication will help you in problem resolution, project implementation, and customer service.

Win2K and NT administrators, who may already be using tools to track project-related tasks, need additional tools to manage and communicate daily maintenance and troubleshooting issues related to system and network functions. If the support teams are large or work split shifts, tracking and documenting task progress becomes even more difficult. An answer to this problem might be one of the more exciting tools to come from Redmond in some time: the Microsoft SharePoint Portal Server. Microsoft designed SharePoint to be a central starting point for storing and accessing departmental information. SharePoint is easy to configure and update, offering a solution that facilitates finding, creating, and sharing all data, which could include daily log and statistic files and team notes.

In addition to Web-enabled communication tools, VPNs have proved beneficial for IT personnel who are often required to provide support during off-hours. With the increased availability of broadband Internet access, using a VPN has become a viable method for connecting to a corporate network remotely, giving technical support personnel the flexibility to address system problems and perform maintenance while away from the office. Many times, the speed of a properly configured VPN will rival that provided by the connection back at the office. One remote solution is Intel's NetStructure VPN Gateway (<http://www.intel.com>), which can provide a complete, secure, end-to-end VPN to connect employees and customers.

With more workers connecting from home, managers and team members have less "face time" with each other, which is not in the best interest of effective team collaboration. Conference phone calls can help, but a more effective communication

tool, especially if a higher bandwidth network connection is available, is to implement desktop video conferencing. Thanks to high-quality, low-priced PC sound and camera hardware, coupled with the free Microsoft NetMeeting application, desktop video conferencing, including sharing desktops, is now possible at minimal cost. Video conferencing can help enhance communications between users at different locations.

### **Preparing for Complexity**

The terrorist acts of 2001 have changed all forms of security forever, so accept this fact and vow to make your workplace more secure. By implementing well-designed security policies and using robust security tools, you can create and maintain a secure, efficient, and effective computing environment for your company. Subscribing to automated security email alerts could make you the hero of the day.

If you take the time to research and locate the best technical resources from the vast array that is available, you might find that you can resolve even the most complex system issues quickly. If you find yourself being dragged down by repetitive or complex Win2K and NT administrative tasks, a tool might be available to assist you, and cost justification for the tool's purchase could be in order. Today's business climate is challenging, and the need to communicate and share progress, problems, and visions has never been stronger. Businesses flourish when communication is good, and your department, as well as your career, will benefit if you use tools and other methods to enhance communications. ■

### **About the Author**

**Marty Scher**  
([martyscher@earthlink.net](mailto:martyscher@earthlink.net)), an IT manager for Fleet Credit Card Services, has more than 15 years of computer and network experience. He is also a freelance technology writer and product reviewer, covering Microsoft technologies and digital photography.