

# PC Networks – A Growing Challenge for Management

With the exponential growth of PC networks over the past ten years, IT management and users have faced a myriad of challenges. And, while users themselves have created many of these challenges, they expect IT support to provide the solutions. The problem lies in the evolution of desktop usage. Independent workstations initially served PC users for their own requirements.

As PCs became linked, there were no guidelines as far as control or standards. Users wanted the benefits of greater processing power, data sharing and storage as well as intra-enterprise communications. At the same time, they wanted the freedom of customizing their PCs.

To compound their problems, desktop users have added a multitude of applications and tools to their desktops and laptops for both work and recreation. And, more recently, the Internet has become the unbreakable link between PCs and the world at large. Besides email, users are downloading applications, games and just about

anything that catches their interest. Very little regard is given to the impact on their PC performance—including conflicting applications, viruses, security breaches and the exponential growth of other online maladies.

Within any given enterprise, machines that started out with identical configurations have been modified beyond recognition. And, as networks have grown exponentially, so has the workload for LAN administrators and technical support staffs. The proliferation of software, the stream of continuous upgrades, application conflicts, viruses and a multitude of additional challenges have made the life of a network administrator more like a fire chief in a town of pyromaniacs.

Today, people do more and expect more from their PCs, while they are adding complexity to the desktop environment on a daily basis. Chasing an ever-accelerating target, support staffs are expected to keep up with the current state of the network along with every application on every machine.

Unfortunately, demands on the LAN administrator require so much “hands on” activity that little time is left for planning. IT staffs spend an inordinate amount of time on mundane tasks such as manually installing software and chasing down problems relating to conflicting applications.

## The Hidden Costs of Supporting a PC Network are Staggering

Where the primary focus on hardware and software is typically on the purchase price, the Total Cost of Ownership (TCO) is invariably many times that number. According to the Gartner Group, businesses spend up to a thousand dollars a month or more to support each PC on a given network. Even more staggering is the loss of productivity from predictable and preventable conflicts—but IT staff is unable to plan ahead, test or predict outcomes. Technical personnel are typically too busy responding to urgent needs. And PC users stand idly, waiting for machines to be repaired. Help desks are inundated



NCMX<sup>SM</sup>

“Making your PC investment work”<sup>SM</sup>

with calls relating to (preventable) improper installations or conflicting software.

At the executive level, CIOs are expected to manage information technologies within the enterprise using existing resources. They are unable to spend adequate time thinking about or planning for the impact of change on the desktop or the network. They are pressured by productivity expectations from new applications, escalating costs and the functionality requirements of their systems. What's more, their staffs are expected to absorb the impact of growth without additional headcount.

Key problems faced by businesses as a whole:

- A continually growing PC base dependent on a finite support resource (fewer people maintaining more machines)
- The vast majority of networked PCs perform below potential (users experience downtime, lowering productivity)
- LAN support staff typically spends the majority of its time on manual, automatable tasks, leaving other work undone
- An inability to monitor individual machines consistently; PCs are unaccounted for; applications frequently conflict with each other
- Individual PCs often run different versions of the same application, creating challenges in sharing data or collaborating

- Software license compliance exposure is significant
- Software viruses are a major threat
- Security breaches can wreak havoc throughout an enterprise

Key problems faced by IT management include:

- Requirement of labor intensive, often repetitive work to maintain PCs
- Inability to monitor or control user changes to individual PCs
- The nature of work is reactive rather than proactive
- Reliance on expensive outside contractors to install applications
- IT manager unable to accurately know which apps are on individual PCs
- Chronically inaccurate and incomplete data about networked PCs
- Growing demands on IT personnel with no corresponding budget for staff
- High turnover, escalating labor costs and inability to recruit and retain qualified personnel

Skilled technical support personnel have become an increasingly scarce and costly part of IT enterprise overhead. The problem is compounded by a high turnover rate as much as 25% or more industry wide, and budgets that do not allow companies to retain their best talent or keep up with the pace of network growth.

For LAN administrators, much of the work is linear in nature. Technicians must physically service each machine in the network. This unpleasant reality is rampant in enterprises ranging from hundreds to thousands of machines. As members of the IT "volunteer fire department," staff is expected to drop whatever they're doing whenever a call comes in and deal with the urgency of the moment.

Basic planning and preventative maintenance take a back seat and are typically neglected when faced with priority projects. Throughout business, industry and government, these unsung technical heroes are buried in work that, by its nature, is never completed. Some readily admit it, others try to hide it. Small to mid-size enterprises universally lack the resources or discipline to get the job done properly. So systems hobble along. Until the next crisis. Or the next change.

### Solving Automation Problems with Automation

Instead of adding more people to fix the problem (infeasible because of costs and lack of qualified technical labor pool), the answer is to automate the LAN tasks that are 70-80% labor intensive. This will enable technical staff to focus proactively on what they do best—plan, test, trouble-shoot and provide support for truly unique problems rather than react to routine, predictable, time-intensive tasks.

Applying technology will bring order to an area where little currently exists. By automating routine, linear tasks and functions currently handled by overworked LAN administrators, PC networks will enjoy an otherwise unattainable level of system integrity on a daily basis.

There are four key areas that would benefit from such an approach:

- **Asset Management**—Addressing the current state of hardware and software in a given enterprise
- **Asset Assurance**—Proactively handling issues relating to anti-virus updates, space recovery, security updates, license compliance, business due diligence and asset disposal
- **Software Change Management**—Dealing with the ongoing process of adding, upgrading and deleting applications
- **Quality Assurance**—Multi-level testing in a controlled environment with quality checkpoints

The impact of automation would provide many benefits to a PC network, including:

- Hardware and software asset management and configuration control
- Accurate and timely PC hardware and software discovery
- Space recovery-maintenance of hard drive integrity

- Automatic installation of new software, changes and upgrades
- Off-hour PC maintenance and monitoring for uninterrupted productivity
- Regular, reliable inventory with full reports on PC components in network
- Multi-level machine testing before implementing network wide changes
- Faster problem identification and resolution
- Elimination of software license exposure—avoiding costly penalties and negative publicity
- Automated virus protection and the latest security updates on each machine with exception reporting

Using an automated approach, enterprises with a few hundred to several thousand PCs could benefit from the same advanced processes and disciplines that only larger enterprises currently enjoy. And, analyzed on a per-PC cost basis, automation is a compelling alternative when labor, lost productivity from downtime and other factors are taken into consideration.

Most of all, such an approach would finally provide management with the answers that are sorely lacking in their enterprises: What is the current state of each PC on the network? Are we utilizing our resources effectively and efficiently? Exactly where are the real and potential trouble spots? What will the

impact of change be? Are we in compliance with our software? How can we be sure we are protected from viruses?

With the ongoing proliferation of networks, now is the time to create accountability, professionalism and disciplined processes in the management of networked PCs. An automated approach can eliminate middle-of-the-night headaches and create a proactive, well-planned and disciplined model. Ultimately, it will bring about better management, greater efficiencies and a higher level of performance to our enterprise.