Focusing On IBM Host-Based Enterprise-Wide Computing
ENTERPRISE SYSTEMS
JOURNAL

The Keys to Network Management: Know Your Business, Know Your Business Needs

by Imran Anwar

Companies are judged by how well their systems, both internal and external, function or malfunction. This is true, regardless of an organization’s size or the complexity of its operations. In the past, only Fortune 500 companies were "computerized." Now companies with fewer than ten employees support and maintain their own LANs, linking their workstations and doing business via the Internet. E-commerce allows a company’s "vital statistics" to remain completely unobserved and, in fact, they are rendered irrelevant.

It makes little difference where you are or how big you are if your Web site is offline or your internal communication is interrupted. If your customers can’t communicate with you, or if your internal systems won’t allow your customer service representatives access to the information they need, you cannot communicate with your customers. Thus, in order to succeed, a company must manage its network – every node, every server, every connection. The business goals the network is meant to serve and the functions it is intended to perform must be clearly identified.

What Are You Trying to Manage?

Managing a network begins with knowing the critical business processes of your organization. You know why you’re in business, what your product or service is, and what you’re trying to accomplish. The next step is to determine which of those processes must be completed, which pieces of the network impact those processes and the order of priority for any necessary repairs. It sounds simple, but the importance of this exercise cannot be overemphasized. It is true that, ideally, everything works perfectly all the time. But since that is impossible, you must determine which systems you must have working in order to conduct business – in other words, determine the basics for your business to survive. As in the case of your car, the radio and the clock and even the air conditioner are certainly important. But, the ignition, carburetor and brakes are vital to the safe and effective operation of the vehicle. Determining what processes are "mission-critical," and their order of priority in the event of failure, require careful analysis and planning.

Any Failure Is Public

The major impact of the Internet on network management is that any system failure is made all the more public. E-mail, online order entry and research via search engines expose every person or enterprise with a Web site to failure that can be witnessed by anyone who has Internet access. To say that word travels fast has become a gross understatement. Is there anyone who watches the news who didn’t hear about some e-commerce company’s inability to make promised Christmas deliveries? Those were internal business failures of planning, choice of vendors, etc., but they were very public customer relations disasters.

Security

Concerns about security are valid, but they are not at the heart of a network management program. "Network security" is not really a separate function. Rather, it is one more aspect of an organization’s overall security effort. Network management includes security concerns, but is a much larger endeavor. Security is, in fact, a freestanding discipline that addresses all aspects of the organization’s operation, including the network, the physical plant, records retention, personnel clearances and business continuity. The same threats to property and personnel exist, and the same data is vulnerable to theft or corruption. The means by which this destruction can occur have expanded, but the basic business risks an operation faces are the same. Damage may be more devastating or more widespread, and it can certainly be accomplished much more quickly, but attacks can be just as direct or just as random.

"Increasing bandwidth leaves networks wide open to both hackers and to government intrusion," says Dan Drooger, an independent Project Manager. "Firewalls, secure machines and anti-virus protocols have evolved in response to advancing technology and must certainly all be in place. But they really serve the same purpose as padlocks, vaults and ID cards. The principles of responsible and effective corporate security have not changed."

Key Components of a Network Management System

Network management should function as a cohesive whole, just as the network itself functions as a single entity, even though it may be made up of many parts. A single tool should manage all of those parts. No matter how many nodes, sites or freestanding systems are in place, a single network management tool can provide seamless and invisible oversight, interaction and response. The challenge, then, is selecting the right network management tool for your operation.

In order to truly manage your network, you need a tool that can analyze historical performance data and create a unique "system personality profile." This will allow for advanced warning of critical situations affecting your most crucial systems. Obviously, predicting system failures before they occur helps to maintain and even increase revenue-generating activities while minimizing the costs associated with system downtime. No one wants to replicate the experience of eBay, which lost 3 to 5 million dollars in one outage, as well as a huge chunk of its stock market value.

Nor are those costs strictly external. At Siemens, the data necessary to make salary payments could not be transferred because a router burned down. Even an immediate repair is not enough to restore the damage done to employee morale and confidence in this type of situation. A policy-based network management tool could have been implemented to predict and prevent this catastrophe.

A holistic outlook is essential for effective enterprise management. Any organization can reap the benefits derived from integrating management of all IT resources by overlaying a common object-oriented infrastructure across multiple lines of business. The goal is to be able to manage all of your IT resources from anywhere in your operation at any time. It should be easy for administrators or, ideally, non-technical management personnel to behave as if they are on a single large computer, or to focus only on those resources that are relevant to their specific jobs. This envisions a truly heterogeneous system that really does allow the management of anything from anywhere.

The core set of management functions needed for network and systems management includes security, scheduling and workload, storage, performance, output, resource accounting and charge-back, problem management and complete event control. Your network management tool should provide all of these, as well as virus scan capabilities to ensure the safety of the environment. It must track, filter, correlate and forward events, as well as take automated action in response to those events. Any response should also be contained at the lowest possible level.

Invisibility is a much-desired attribute in any network management tool. The people using your system – customers or employees – should be unaware of the activity going on "behind the screen." Literally hundreds of thousand of signals can be hurtling along system lines. Millions of connections can be made, interrupted and restored. Data can be sent, diverted and retrieved. And all of this should go on while your customers and employees conduct business as usual. Having identified the most critical functions and predicted the most probable locations and types of failures, your network management system will have been built to respond with as little human intervention as possible. It will notify your systems personnel when it is in need of their assistance. It will only warn higher levels of management on an as-needed basis. There is no need for the CIO to be called in for every incident. Reports of system failures and repairs will keep management apprised of what the system is doing and where upgrades or adjustments may be necessary. The system itself will evaluate events and interact with as few or as many of your staff as are necessary to take the appropriate actions. The level of response will fit the situation.

Choosing a Network Management System

Network management tools exist that will do all of the things a company needs and more. But in order to find the best tool for your particular application, you have to shop. Thankfully, you do not have to do this on your own.

Whether you decide to pursue this project in-house will depend upon your own company's resources. Generally, though, outsourcing is the method of choice – particularly for wiring and the other aspects of hardware installation. Outsourcing network management is a new and growing field. Your service agreement will define the managing entity's level of response. You may require members of your service provider's staff to be assigned to your facility at all times, or you may be one of many clients connected to a "help desk" at the provider's location. In the case of a system failure, they may dispatch service personnel to work on your equipment or simply notify you or your designee of an event in progress. You will have to determine what's best for your situation.

This is not a short-term solution. As your business grows and expands, so must your network. End users must have access to increasing numbers of applications, and this increased data exchange will put pressure on bandwidth. You will need both a common user interface and advanced traffic-flow/bandwidth management. You want to work with someone knowledgeable and experienced in designing long-term network management strategies.

The successful development, installation and use of a network management system begins, however, with you. Only your intimate knowledge of your industry and your own organization’s purpose and place within it can lead you to the proper choices. When those decisions are left to others or to chance, chaos is the result. Chris Carabajal, a Systems Administration Supervisor for a California Workers’ Compensation Insurance carrier says, "Keeping the computer running is not the greatest challenge in managing a network. It’s dealing with the politics of who and what projects get priority. The clearer those lines are, the better the whole system works."

The marketplace is becoming increasingly "networked," with e-business becoming the rule, rather than the exception. Not only those organizations on the worldwide Web are impacted, either. Internal systems management is as critical as anything external. Neither the CIO nor the end user cares whether the problem is with an interface card, a router, a frame relay link or an ATM backbone. The system’s just "broke." They look at and use the network as a cohesive whole, delivering applications and services to end users who have specific business-related tasks to perform. For this reason, you cannot have 23 different tools for 23 different pieces of your system. There must be a single, "universal" management tool in place that monitors your system and keeps it running with a minimum of interruption to your critical processes or inconvenience to your internal and external customers. Now *that* is network management.

About the Author:

Imran Anwar is Director of Product Strategy for Computer Associates’ network management solutions, and CEO of EverTrack Inc., a Computer Associates and UMC Group joint venture, delivering GPS-based products and services to "geography-enable" the management of organizations’ resources in realtime. He can be reached at imran.anwar@cai.com.

To Table of Contents

to ESJ Home Page