



Managing for Value

**Decoding the Mysteries of
Network and System Management**

by Jacob Stoller

**Sponsored by
End to End Networks Inc.**

Table of Contents

Network and System Management – Where's the Value?	3
Network and System Management Basics.....	4
NSM Tools – How They Work.....	4
Buying NSM as a Service	5
Service Level Agreements	5
NSM Objectives: What Companies Pay For	6
How NSM Provides Value.....	7
Making the Network More Visible	7
Deploying Network Expertise.....	7
Summing Up: An NSM Value Framework	8
Case Example – Company "A"	9
About End to End Networks	11

Network and System Management – Where's the Value?

Nobody likes to spend money when they don't know what they are getting. The information age, however, has put many decision makers in that very position. Network and system management (NSM) is one of those entities that is frequently purchased with very little understanding of what is actually being delivered.

The network has rapidly grown from relative obscurity to become the most critical single vehicle for IT delivery. Today, we function in a virtual work environment, where one file folder could reside on a system in New York, while the one next to it resides in a server in Hong Kong. The system problems that used to be confined to environmentally sealed computer rooms can now occur anywhere in the world. An unmanaged network today is as unthinkable as a mainframe without a console. But delivery is becoming an increasingly complex affair.

The NSM industry talks about the need to manage networks for business value. This is hard to dispute, but what does this really mean? This whitepaper, sponsored by End to End Networks, is intended to answer this question, and to help decision makers understand the basic issues around NSM and the value it provides. It is based on interviews with NSM users, industry experts, an ongoing study of the industry, and detailed discussions with End to End Networks and their clients on how they meet network support challenges.

Network and System Management Basics

Network and System Management can be defined as **the collection and processing of information from a number of devices to verify that they are operating within specified parameters, and the use of that information to prevent and minimize system disruptions.** The concept is simple, but the realization is not. The following trends have made this an increasingly complex task:

- Devices are provided by multiple vendors, and on a variety of operating systems.
- Devices may be dispersed all over the globe, and managed over the internet, data lines, or high speed internet.
- Many managed devices, such as laptops and PDA's, are not stationary.
- The growing need for security has spawned many new issues, such as firewall management, intrusion detection, and viruses.

NSM Tools – How They Work

The explosion of the network in the last 15 years was fuelled by the wide acceptance by the industry of a common language or protocol known as TCP/IP (Acronym for Transmission Control Protocol / Internet Protocol). The IP network, as it is commonly called, became the lifeblood of local and wide area networks, and, more recently, of the internet. The collection of information used to manage systems and networks has a lot to do with TCP/IP; this is still the common language for "talking to" a wide range of devices. It is also the basis for much of the "techno talk" that is commonly heard when engineers are troubleshooting a network problem!

NSM uses automated software-based tools to collect and process management information. NSM software is a multi-billion dollar industry, dominated by large companies such as IBM/Tivoli, Computer Associates, and HP Openview. The "big names" focus on large environments, while more recent offerings by Microsoft, NetIQ, and Aprisma focus on PC-based distributed environments.

The marketing hype around these tools is considerable; they claim to leverage infrastructure for strategic advantage, apply business intelligence to IT, and a host of other metaphors. Essentially, however, what these tools do can be simplified as follows:

- Collect and store information from a wide range of networked devices.
- Consolidate, "slice and dice", and display information in a useful format.
- Notify individuals when attention is required.
- Initiate automated procedures based on information received.

NSM is not rocket science, but it does involve mountains of information that is useless unless managed properly. **So the challenge for NSM is not in only managing devices; it is also in managing the information that gets collected.**

This is where expertise comes in. If you hook up an NSM tool to your IP network, you will get a long series of alerts of various sorts, in a format that is not useful. The vast majority of these will be either redundant or superfluous. The art of NSM is in knowing what requires attention and what doesn't. The caveat here is that if you're going to programme the system to ignore certain information, you'd better know what you're doing!

But what gets seen and what doesn't get seen is only the beginning. An automated procedure might make a decision to attempt a server re-boot before paging a technician. Or it might make a decision to delete a number of archived files in order to prevent a disk crash. Needless to say, the policies that govern these decisions need to be designed by experts.

It's no surprise, therefore, that the successful deployment and administration of NSM tools requires significant resources. Large organizations, such as major banks, have teams of people dedicated to NSM. The trend for smaller organizations who can't afford this kind of staffing is to outsource the service to a managed service provider such as End to End.

Buying NSM as a Service

The key to getting NSM to work as a service is ensuring that the set up and use of NSM tools is appropriate to the technical and business environment. Because of the complexity of the multi-vendor networked world, no two companies are alike when it comes to their networks. Types and location of equipment, hours of operation, wide area carriers, and remote access all have to be taken into account when setting up NSM tools.

The uniqueness of an environment, however, extends beyond the technical; the relevance of that information could be very specific to a company's business. For example, an NSM tool can detect when a system is using up disk space faster than a specified parameter dictates. Does this justify a costly automated after-hours call to a service engineer? If you're an accounting firm and it's tax season, the answer is probably "yes". But if you're a retailer during the post-Christmas slump, and it's Monday, the answer might be "no". Setting up a proper NSM environment can involve hundreds of decisions like this.

For these reasons, outsourcing NSM involves a close working relationship, and it involves customization. Many people have been led to believe otherwise; that NSM is a commodity that can be provided in "cookie cutter" fashion. This viewpoint has been perpetuated in particular by telecommunications providers, who seek to apply the mass market approach they have successfully used in their core business.

Service Level Agreements

Many people would argue that the way to provide the above is with a clearly defined Service Level Agreement, or SLA, that includes a series of metrics. This is partly true. When parties come together in a business agreement, it is important that the relationship be clearly defined in writing. However, it is a mistake to believe that something as

complex as NSM can be defined for once and for all through a series of terms and conditions. Most experts believe that over-reliance on SLA metrics results in an adversarial relationship where the parties don't work well together.

A simple example is the use of an uptime commitment. The static metrics used in many SLA's fall far short of guaranteeing a satisfactory level of service. Even a metric as basic as availability is not as straightforward as it seems. A commitment of 99.99% uptime (called "four nines") means that your vendor can "afford" to leave you down for 30 minutes per year. This could mean 6 outages of 5 minutes each. It could also mean one 30 minute outage. Under certain circumstances, either could have dier consequences for a business. But availability is simple compared to metrics that govern a help desk, where human factors come into play. In that case, management by metrics can quickly become a tedious exercise that often fails to get to the root of issues that users are concerned about.

What makes much more sense is for both parties to be "pulling in the same direction" towards the fulfillment of business goals. This means that both sides need to understand the value that is provided by the service, and to work together towards achieving that value.

NSM Objectives: What Companies Pay For

End to End Networks has long held the above-stated view, and has worked towards long term agreements based on a strong mutual understanding of the customer's objectives. End to End's customers, therefore, were able to provide clear and useful insights into the establishment and attainment of suitable goals.

While every company has unique considerations in terms of its network, the following are consistently sought after as organizations strive to manage their networks better:

- **Prevention and resolution** of system disruptions. NSM provides a warning system by detecting anomalies at an early stage, and also provides useful information to speed the troubleshooting process. This results in fewer system failures, quicker problem resolution, and better service levels. NSM also helps to prevent human error, which is a primary cause of IT downtime.
- **Governance.** NSM helps organizations account for what they have, and verify that proper measures are in place to prevent viruses, data theft, network disruptions that could harm the business, and a host of other threats.
- **User Confidence.** A well-managed network is a trusted network. This allows employees to work more efficiently, and keeps customers using the system and not going to a competitor.

How NSM Provides Value

Making the Network More Visible

One of the keys to realizing the objectives of network management is knowing the location and condition of a large number of devices. With the help of automated tools, NSM provides the following:

- **Alarms.** This includes visual alarms on a screen, audio alarms, or automated phone calls, emails or pages.
- **Filtering.** Network management tools can be programmed to remove redundant information so the viewer is not overwhelmed.
- **Reports.** By reviewing specific reports on a regular basis, management can keep track of issues affecting the network.
- **Asset management.** Having a clear and accurate picture of the network includes having up to date information on what has been deployed, moved, or changed.
- **Portals.** Portals provide convenient access to network information regardless of location.

Deploying Network Expertise

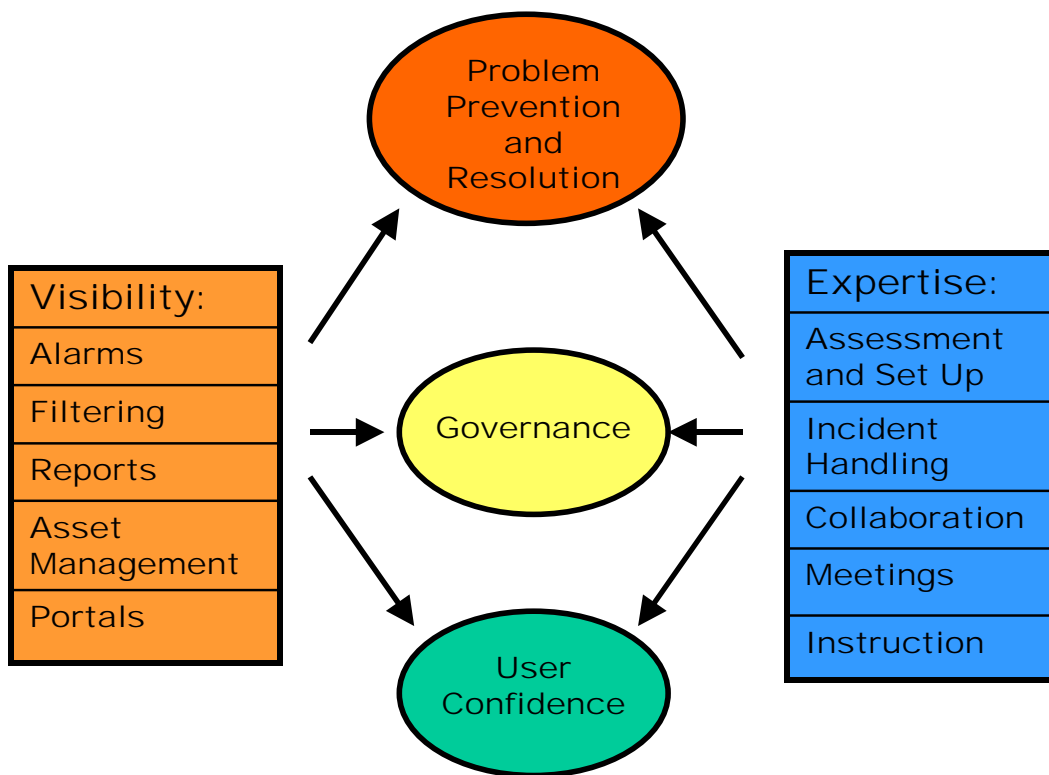
Vendors frequently talk about the number of experts they have on staff. This is important, but the bottom line is how this expertise is deployed. As a buyer of expertise, the client needs to understand the principle areas there "the rubber meets the road" regarding the delivery of expertise.

- **Assessment and Set Up.** Getting the tools to monitor and manage the right parameters is key to the success of NSM.
- **Incident Handling.** How a service organization responds to and resolves calls, and how customer personnel are treated, are key factors.
- **Collaboration.** Close collaboration with other vendors and the client's technical staff, as opposed to adversarial relationships, are key to efficient event handling.
- **Regular Meetings.** Meetings at regular intervals ensure that communication is good, roles are understood, and systems are monitoring and reporting the right information.
- **Instruction.** The ability to instruct people at the right level is an essential component of deploying expertise.

Summing Up: An NSM Value Framework

The diagram below sums up how NSM value is derived from a wide range of managed tasks and features. There is no magic bullet; the components are highly interdependent, and complement each other. Asset management, for example, provides valuable information for governance purposes, but it also reduces downtime by reducing human error. A portal not only allows better response to problems, but makes users more confident because they know are aware of what's going on. And so on.

NSM Value Contributors



The most prevalent result in all of this, however, is obscurity; the well-managed network simply fades into the background. This means that people who need to know get clear and timely information about network issues. Those who don't rely on the network because they know it is properly looked after. This attitude is in line with what long standing End to End customers are reporting.

Case Example – Company "A"

The following example, based on a real customer, illustrates how value can be delivered through NSM. Company "A" is a long standing End to End client. Their situation typifies the challenges that Canadian organizations face when supporting their networks.

Profile:

Company "A" is the Canadian branch of a multinational corporation, consisting of a Canadian head office and a network of approximately 50 dealers. The network is connected by a carrier network whose operation is critical on a 365/24/7 basis. End-to-End's sphere of responsibility covers:

- Management of the Wide Area Network, including carrier-owned segments.
- Router and Firewall for each of 50 dealer sites
- Router and Firewall for head office
- Wide area link between Canadian head office and corporate head office.
- 6 mission-critical servers

The customer uses a different service supplier to support approximately 60 additional servers, and the organization's desktop environment. The customer also employs an IT staff of 6, several of whom have a basic understanding of network issues.

Company "A" has been an End to End client for almost a decade, and the value of the service has been clearly established and verified. The company reported to us that:

- Service level commitments, which are set by Company "A" 's corporate head office, are consistently exceeded on the Canadian network. Network-related service problems are considered a non-issue.
- As a European-owned corporation, Company "A" complies with global governance standards, and relies on End to End to provide due diligence with regard to protection against threats to the business such as viruses, hackers, router and firewall software bugs, and human error.
- End to End has a potentially tough customer in a national dealer network that is known for frequently complaining. However, Company "A"'s CIO reports, "I have yet to hear a dealer even mention the network." This is due not only to service levels, but to the fact that dealers are properly informed about any network issues.

Here is how End to End achieves these results.

Providing Visibility

With the help of the e-View portal, End to End provides the client with a comprehensive visibility of the network. Some of the highlights are:

- A comprehensive display of events and alarms.

- Role-based access to asset and configuration information, which is maintained by End to End.
- Aggregate information on incidents, network traffic, intrusion attempts, are available.
- Periodic customized reports are used by the CIO to oversee network matters, and report to head office.

Deploying Expertise

The manner in which the expertise is delivered is, according to Company "A"'s CIO, the determining factor. Some of the highlights are:

- Incidents are handled without screeners, and this is true on a 24/7 basis. This gives Company "A"'s staff a quick jump on critical problems.
- Proactive conference calls are held on a bi-weekly basis to ensure that long term issues are being addressed, and that communication is optimized.
- End to End participates in incidents that may not be End to End's responsibility. This acceptance of overlap helps to ensure that optimum service levels, as well as customer confidence, are maintained.
- End to End has a strong reputation for WAN expertise in the carrier community, and in fact provides OEM services to Bell, Sprint, and other carriers. This allows End to End to provide a strong advocacy role when Company "A" feels the carrier may not be performing.
- End to End employees have been cited by the customer as excellent teachers.
- There has been extremely low employee turnover at End to End, resulting in long and solid personal relationships with client personnel.

Conclusion:

What counts here is not that a specific number of checklist items have been fulfilled, but that End to End is providing exactly what the customer requires. What the customer sees is value. Even the CIO thinks little about networks because, as puts it, "I've got End to End looking after that."

About End to End Networks

End to End Networks was founded in 1992 by a team of senior IT professionals. Their early focus was on high end, hard-to-find skill sets in the Wide Area Networking field. One result of this approach was that they became, and have continued to be, a service supplier to the large carriers for real-time monitoring, problem resolution, and reporting. This has made End to End unique in their ability to work with carriers on behalf of end users.

Building on their solid reputation for WAN expertise, End to End has grown to become a fully integrated provider of IT infrastructure solutions including WAN, LAN, Systems Integration, Cabling & Wireless services. End to End provides support from their National Support Centre situated in Markham, Ontario. From the Centre, End to End offers customers a complete IT infrastructure management strategy with a focus on end-user support for multi-carrier, multi-platform and multi-protocol networks. End to End maintains access to all of the major carrier networks.

End to End has recently re-designed it's eView portal, giving clients a wide range of monitoring and collaboration capabilities. As a common management platform, e-View is helping End to End customers stay on top of ongoing network issues, and cope with the rising complexity of their networks.