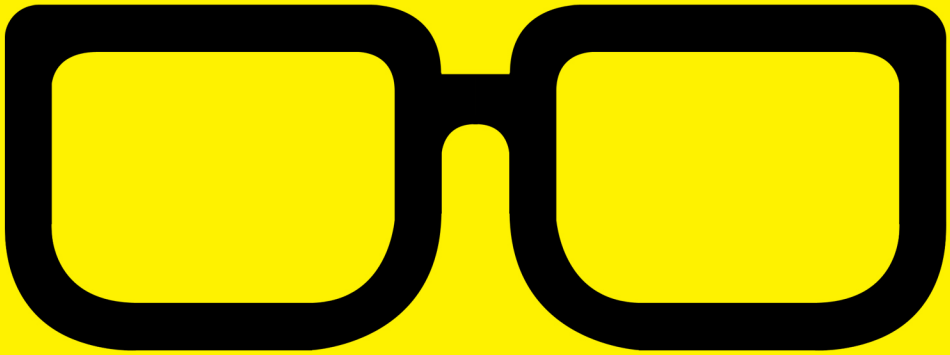
SPONSORED BY

InterMapper

GEEK GUIDE



Enterprise Monitoring Success

LINUX™ JOURNAL

Table of Contents

MIKE DIEHL has been using Linux since the days when Slackware came on 14 5.25" floppy disks and installed kernel version 0.83. He has built and managed several servers configured with either hardware or software RAID storage under Linux, and he has hands-on experience with both the VMware and KVM virtual machine architectures. Mike has written numerous articles for *Linux Journal* on a broad range of subjects, and he has a Bachelor's degree in Mathematics with a minor in Computer Science. He lives in Blythewood, South Carolina, with his wife and four sons.

GEEK GUIDES:
Mission-critical information for the most technical people on the planet.

About the Sponsor

The HelpSystems Solution for Network Monitoring

InterMapper: Comprehensive Network Monitoring, Mapping, and Alerting Software

HelpSystems has more than 30 years of experience creating IT management software that expertly solves business problems with elegant solutions. Part of the HelpSystems family of brands, InterMapper is an easy-to-use network monitoring, mapping, and alerting software that's powerful enough for the enterprise but affordable enough for small-to-medium-sized businesses. InterMapper starts by auto-discovering every IP-enabled device in your network and helps you create maps that display real-time statistics on each one. InterMapper can monitor your devices for everything from response time and bandwidth utilization to temperature and packet loss. If a threshold looks to be exceeded, InterMapper can alert you to this possibility before it may cause larger problems. With InterMapper, you have real-time, in-depth knowledge into the health of your network and the peace of mind that you'll always be one step ahead of costly network outages or slowdowns.

Enterprise Monitoring Success

MIKE DIEHL

Introduction

You've all heard the mantra: "better, faster, and cheaper". It seems that a system administrator can't go to a management meeting without hearing it. Thinner profit margins and higher customer expectations require that IT departments up their game. In this eBook, I discuss how enterprise monitoring can help and how to deploy a quality enterprise monitoring system successfully.

If you were to put a server on the open Internet, it wouldn't be long before someone out there did a port scan on it.

Management teams are barraged by industry pundits constantly telling them about the next best thing to do in order to save money on IT costs. There's outsourcing, public cloud, private cloud, virtualization, and any number of mechanisms designed to save money on IT expenses. Whether they actually save money isn't the point; the point is that saving money is always on your manager's mind.

Plus, customers certainly aren't helping the situation. They've grown accustomed to high-speed, instant access to resources that are available 24 hours a day. Studies have shown that even a one-second delay in loading a Web page reduces that page's effectiveness by 15%. Databases and e-commerce sites are expected to be fast; otherwise, people would just use the much simpler manual alternatives.

Additionally, because the Internet isn't the perfect utopia it once was, all of your IT operations need to be better, faster, cheaper, and more *secure*. If you were to put a server on the open Internet, it wouldn't be long before someone out there did a port scan on it. And as you know, this is just a precursor to an outright attack on that machine. Attacks happen all the time, and the big question is how to know

when they are happening and when they've been successful.

These are exciting times to be working in IT, but with all of the advances in the industry, things haven't gotten easier. If anything, it has become a tougher industry to work in that requires a broader range of skills.

For the rest of this guide, I discuss how enterprise monitoring can accomplish management's goal of "better, faster, cheaper, and secure", without adding too much to IT's level of effort.

Note: it's understood that many companies don't have specialized networking, server, or database groups. In many companies, this all falls under the umbrella of "IT". These terms will be used in this guide fairly loosely and may describe functions that overlap each other in a particular company, much like the job description of the typical IT worker. Although this guide is geared toward larger environments, the main points are applicable to organizations of almost any size, with or without specialization within its IT department.

Three Steps to Enterprise Monitoring Success

The path I outline in this eBook is a three-step process to enterprise monitoring success, but it's probably not an intuitively obvious path. The three steps are as follows:

1. Centralize control.

2. Delegate responsibility.

3. Distribute awareness.

If something like this happens, you may find yourself in a management meeting justifying your server availability and network performance claims against metrics that you didn't even know were being gathered!

Centralize Control

The first step to enterprise monitoring success is to get rid of everyone else's pet monitoring projects and establish a centralized monitoring system. For example, you don't want the business development group using free software or services to monitor servers in order to ensure that their business intelligence or CMS systems are working. If something like this happens, you may find yourself in a management meeting justifying your server availability and network performance claims against metrics that you didn't even know were being gathered! And there's no guarantee that these metrics are being gathered correctly. In addition to being potentially awkward, this type of redundancy is expensive and doesn't do anything to further the goal of "better, faster, cheaper, and secure". It amounts to being a stick that one department uses to beat up on the other (IT) department.

Of course, you can't just say, "Thou shalt not monitor." Such edicts rarely work. The most effective way to centralize control over the enterprise monitoring operation is to establish a solid, working system that reliably and accurately provides the information that all of the stakeholders need.

Once a compelling alternative is in place, those private monitoring fiefdoms tend to die of abandonment.

Delegate Responsibility

What often happens early on in an enterprise monitoring project is that the server manager will build a monitoring system to watch the servers and to keep from being caught by surprise by users and higher-level managers. Then the server manager decides to monitor parts of the network as well. This attracts the attention of the networking group members, who immediately get on the bandwagon because they understand the value of being proactive when it comes to managing a network. This all sounds pretty good except that most of the work and responsibility for managing the new enterprise monitoring system is concentrated within a small number of fairly senior members of the IT staff. These senior staff members already have enough (or more) to do without having to manage a monitoring system as well. This is where delegation of responsibility comes into play.

Day-to-Day Maintenance: The senior IT staff should grow the enterprise monitoring system to maturity and then shed the responsibility for its day-to-day maintenance as quickly as possible. Because of the specialized skills that the server and network administrators have, it's important that they maintain some degree of involvement in the long-term management of the monitoring system, but they don't need to be involved in the day-to-day operations.

Enterprise monitoring isn't technically challenging and probably isn't even interesting to senior IT staff members. Let's face it, lack of interest will kill a project almost as quickly as lack of

funding. But, some people truly thrive on this type of work. They enjoy being the "first responders" when a server goes down. These people want to be center of the action, and they enjoy looking for potential problems that no one else has found or has had time to investigate. These people tend to be good at communicating, and they tend to be good with customers and users. They also typically appreciate standardized and repeatable operating procedures. These people are who you want watching your enterprise. They may not be able to decode a sniffer trace or repair a RAID, but they will watch your enterprise like a hawk. You just have to give them the appropriate tools and training.

One of the side effects of having a dedicated monitoring team watching the enterprise is that the members of the team will become familiar with the enterprise. They'll learn which network links tend to be busy. They'll discern patterns in traffic levels and server availability. And most important, they'll recognize when things "just don't look right".

You could spend a lot of time and effort profiling your enterprise and establishing and re-tuning alarm thresholds and still not approach the effectiveness of a live human being watching a monitoring display.

Many network monitoring tools allow users to see what types of traffic are on a particular network link. This requires that agents be installed either in the networking equipment or the servers. However, if this infrastructure is in place, the network monitoring team is in a prime position to be able to discover active attacks on the network and servers proactively. Large spikes in raw network traffic or SMTP traffic coming from a server that doesn't normally send e-mail are both example indications that something may have gone horribly

wrong. The network monitoring team may be able to detect a situation like this and have the network management team resolve it before it becomes a customer-facing issue.

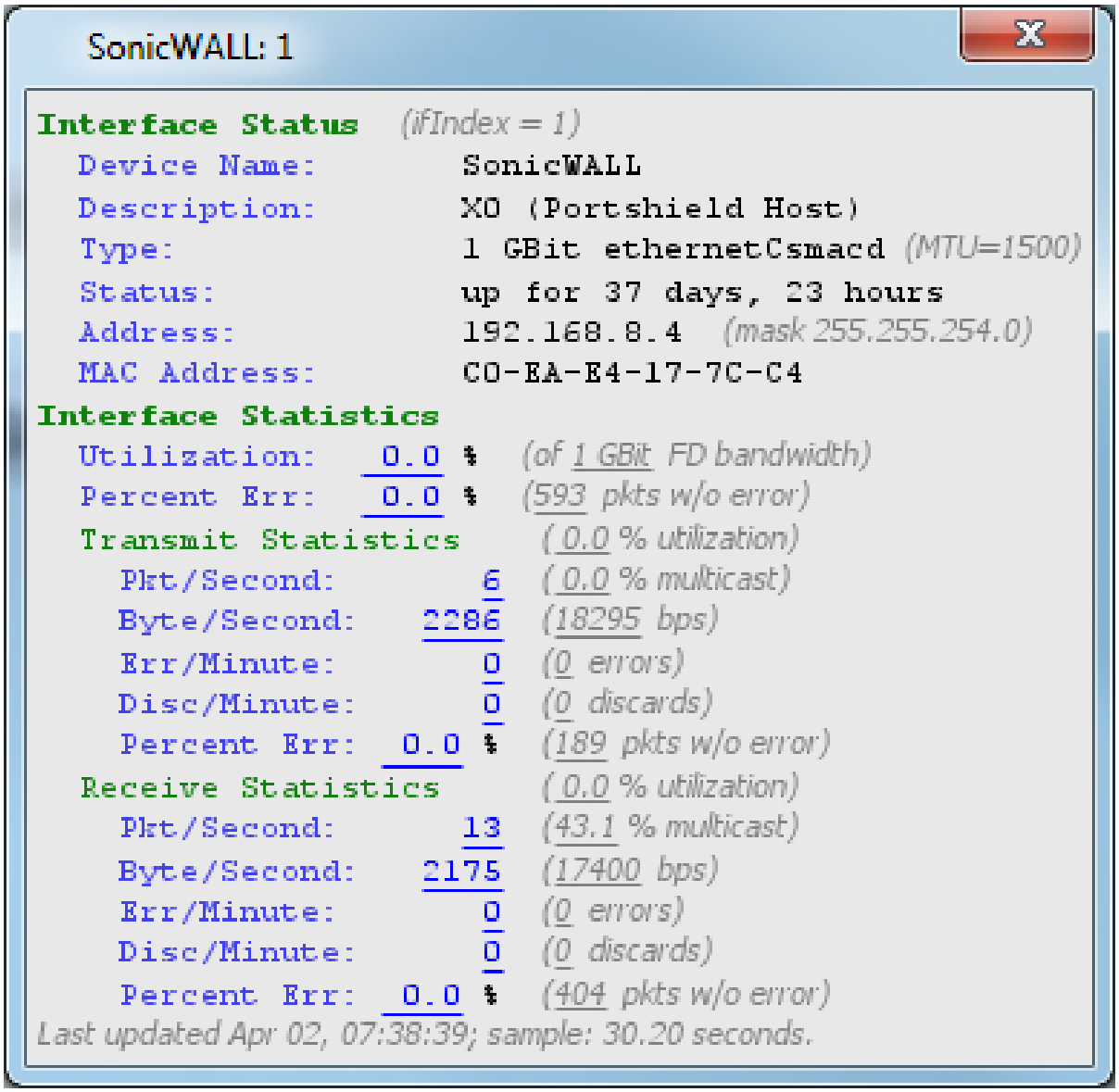


FIGURE 1. Some network monitoring systems, Like InterMapper by HelpSystems, can use SNMP queries to display detailed information about devices on the network.

So, delegate the day-to-day monitoring of the enterprise to people with traits well suited to that type of effort. It's important that the enterprise monitoring team members be given the broadest investigative boundaries as possible, even if they don't actually have any ability to resolve a specific situation. Given the proper environment, they will discover things going on in the enterprise that nobody else has time to discover until it's too late. Ask yourself if you'd rather say the following to a user, customer, or manager: "I wasn't aware that this was going on, but I'll be happy to look into it further." Or this: "Yes, our monitoring team discovered that issue a few days ago, and we are working on getting it resolved."

Both of these are completely acceptable responses to a trouble report. One of them, however, conveys the fact that the IT department is managing the enterprise in a proactive and customer-focused fashion. Sure, there will be times when the monitoring group members come up with issues that really aren't of any consequence, and that's fine. They will learn and become better at finding issues that really do matter. In the mean time, the senior IT staff members will have time to do the things that they need to do and that interest them more. If the monitoring group merges with the help-desk group, they can become the "face of IT" for the enterprise and deflect a lot of effort away from the more senior members of the department.

Delegating responsibility results in tasks being performed by those staff members most likely to get the job done.

FIGURE 2. Netflow sensors allow the network monitoring staff to examine the amount and type of traffic flowing on the network.

Distribute Awareness

The final evolutionary step in enterprise monitoring success is to distribute access to the monitoring system to other departments and organizations within the company. Of course, this may seem contradictory, given that the first step was to centralize. The difference is that you have centralized control, so now you want to distribute access.

This goes beyond the "we're all on the same team" cliché. The goal is to find a synergy between the various

client departments and teams. For example, the more technically sophisticated teams like WebOps or the DBAs will know their systems well enough to be able to discover problems by themselves and hopefully resolve them by themselves. Other less technically sophisticated teams, like sales, typically will find a member of their staff to be the "go-to" person for any IT issues. If this person has access to the monitoring system, he or she will field many questions like "Is the database down?" without having to involve IT at all.

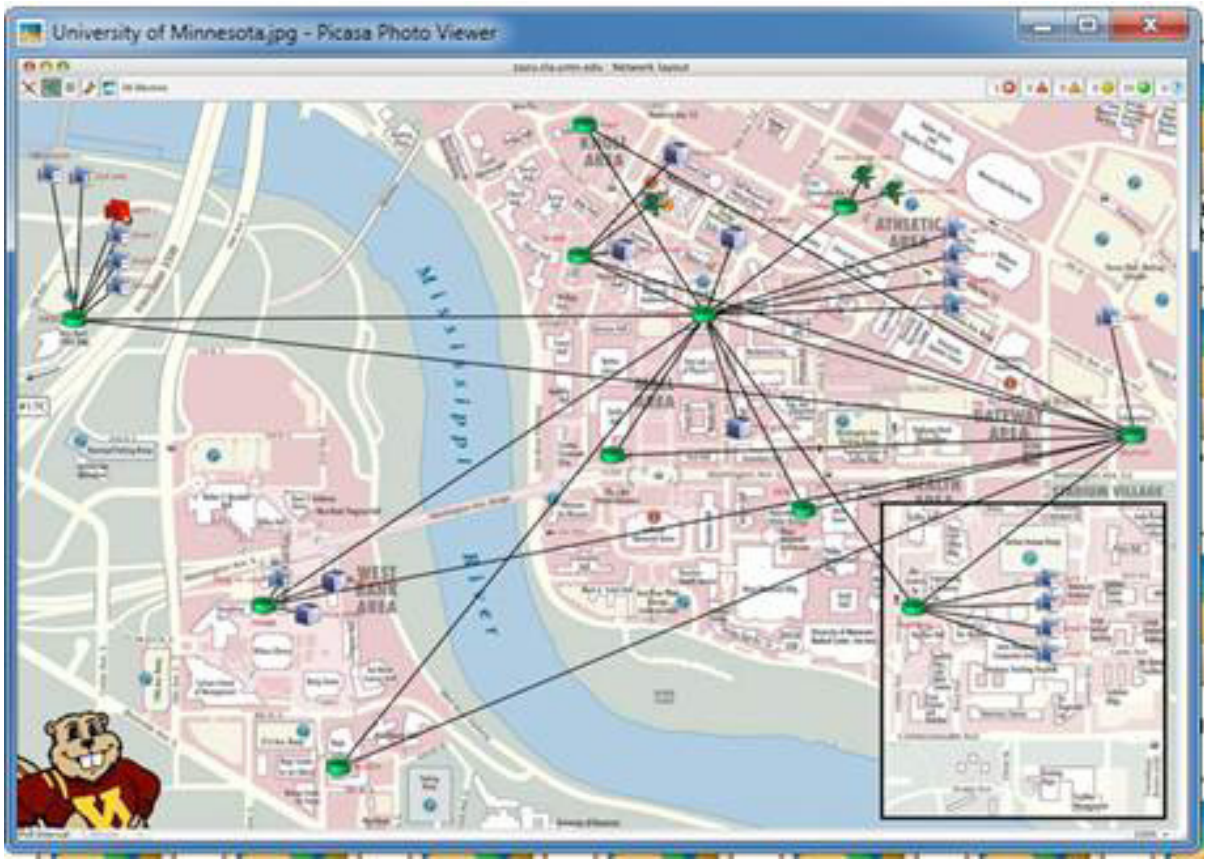


FIGURE 3. Network maps should be tailored to display the information that a particular user needs.

Access: One of the keys to distributing access to the enterprise monitoring system successfully is to ensure that the various stakeholders have the access they need to be helpful, and *only* that access. Nobody wants this to devolve into 15 different IT shops all under one roof. But you do want to develop contributing partnerships with the other organizations within the company. It doesn't make any sense for the DBAs to be monitoring the Web servers, but it might make sense to let them have some knowledge about the state of the core network insofar as it affects the availability of their database servers. By the same token, management probably doesn't need a detailed map of the enterprise, just one that contains the major core servers and the customer-facing servers.

It's important that all of the stakeholders who have access to the monitoring system understand that there is a communications path that must be followed in the event that an issue is discovered. You don't want the other departments responding to an IT issue by contacting the system administrators directly. This places an undue burden on the system administrators and negates the whole point of having a centralized help desk and monitoring system. You want to have all trouble reports and general questions channeled through the help desk (or the monitoring group in the absence of an actual help desk). This allows the help desk to become a clearinghouse for information regarding the general health of the enterprise and the status of various trouble reports.

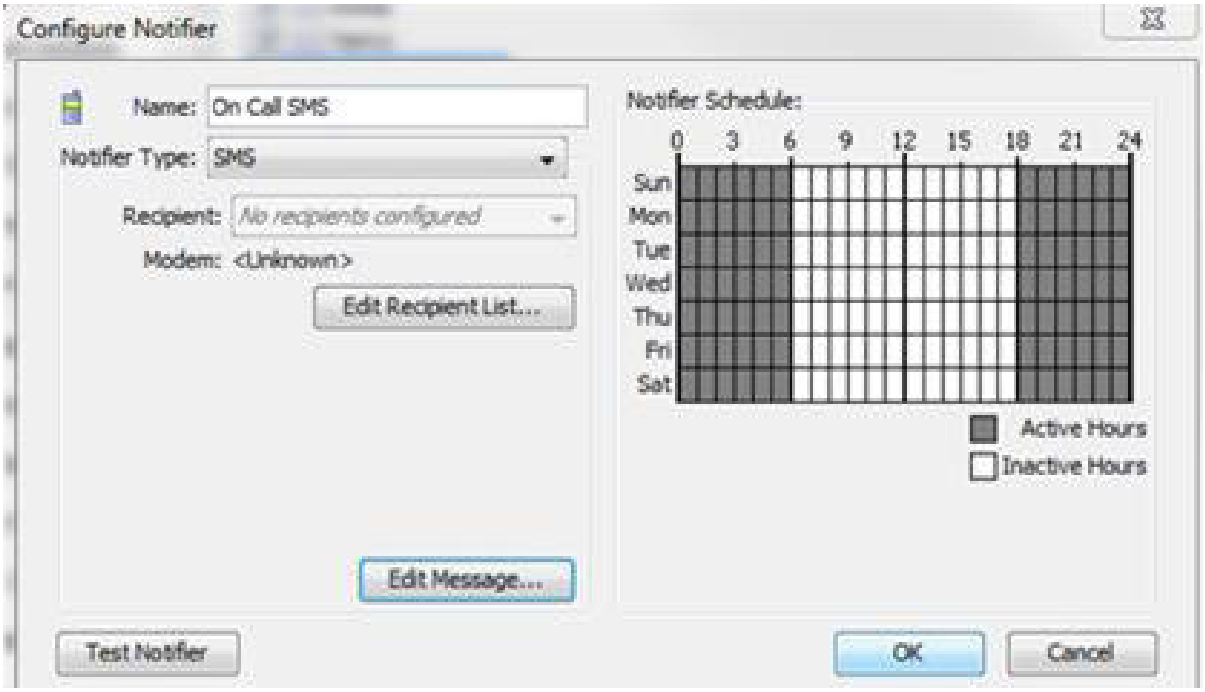


FIGURE 4. Event notification should be flexible and effective.

Let's face it: you're not granting access to the monitoring system because you're nice or because you're lazy. There are three main benefits of giving access to the monitoring system to outside organizations:

- First, you want the other organizations to "join the team" and help improve the enterprise. They can help by finding and reporting issues to the help desk. From there, issues can be tracked and resolved before they stagnate in the minds of the other department's staff. It's much more effective, and pleasant, to hear about an IT problem from the users it affects, than it is to hear about it from their manager. Remember, users will notify whomever they feel will get the problem resolved the quickest; make sure your users perceive that the

If you've been in this business any length of time, you understand that the only time IT becomes visible to management is when something is broken, and that's not good visibility.

help desk is the most efficient way to get problems solved.

- Second, most enterprises are more good than bad. That is, most servers, network links, and services are available much more often than not. Outages are relatively rare. By providing outside organizations with access to the total state of the enterprise, by way of the monitoring system, you are engaging in a subtle effort to modify those organizations' perception of the quality and reliability of the enterprise. Most of the time, they will see "green lights" and eventually will learn to associate the enterprise with those green lights. They also will get a taste for the size and scope of the IT effort. When outages do occur, they will be perceived as anomalies, not the status quo, or "here we go again".

- The third benefit to granting access to the monitoring system is directly related to budgeting. If you've been in this business any length of time, you understand that the only time IT becomes visible to management is when something is broken, and that's not good visibility. The IT department is in an awkward position. Whereas the sales

department can point to a given number of dollars that it brought into the company, the IT department can't point to any income that it brought to the table. Many managers perceive IT as just a cost of doing business. But without IT, there probably wouldn't be any sales, or accounts payable, or accounts receivable. By providing access to the monitoring system, the IT department is making itself visible in a positive fashion as a service provider and a business

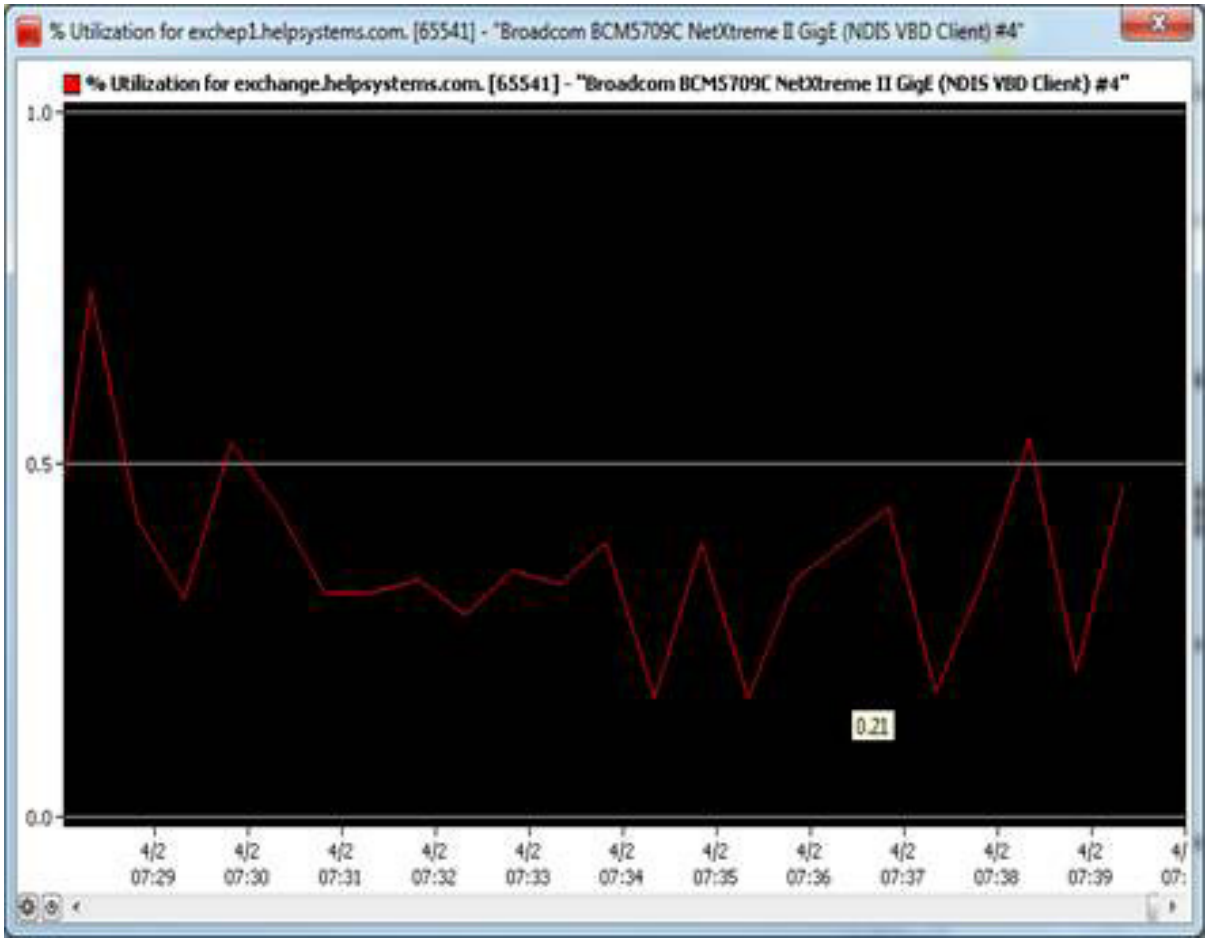


FIGURE 5. Network utilization metrics are a key troubleshooting tool.

Individual issues that may not warrant a response by themselves may be symptoms of an underlying trend that does indicate a problem worth investigating and fixing.

enhancement. The savvy IT manager will leverage this effort when it comes time for IT budget review.

For this last step to be successful, management needs to understand that not every issue that gets "discovered" by these outside organizations will get fixed. For example, the staff members at a remote branch office may report that their network link to the main accounting servers is often congested. That's a real problem, and both IT and management need to be aware of it. However, depending on what upgrading that link would cost, it may not be cost effective to resolve the issue. Also, the IT staff may not feel that it's necessary to react every time a port scan is performed on a given server.

The IT staff members are the subject matter experts (SMEs), and they need to have the freedom to exercise their best judgment as to the scope and scale of their response to a trouble report. But, by having all of this communication channeled through the monitoring group, the monitoring group is in a position to spot trends. Individual issues that may not warrant a response by themselves may be symptoms of an underlying trend that does indicate a problem worth investigating and fixing. Your help desk will

be in a unique position to spot these trends and bring them to the attention of senior staff.

Enterprise Monitoring Tools

Building, managing, and evolving an enterprise monitoring system is hard work. Using the right software tools will make it easier, but you'll find that no one tool will do it all for you. So, you may find yourself deploying a suite of more specialized tools. The trick to deploying a suite of tools is to maximize the breadth of functionality while minimizing overlap. It doesn't make any sense to have three monitoring tools because one tool does a particularly good job of monitoring UNIX servers, while another was recommended by the networking equipment vendor, while the third one....It just doesn't make any sense. The ideal tool does its job very well and doesn't try to do anything else. If you find a network monitoring tool that also does configuration backups, for example, you probably are looking at a tool that is trying to do everything, and it probably won't do it very well.

Also, keep in mind that the goal of the monitoring project is to push the day-to-day monitoring operation down to a group of less-senior staff members and eventually to (perhaps) non-technical staff members in other departments. So the tool that you provide to these groups needs to be powerful enough to do what they expect, but not so advanced that it becomes a training burden for the more-advanced IT staff.

An ideal enterprise monitoring tool will have various roles that can be assigned to users that determine what each user is able to see and what changes they can make. Also, look

for alarming and alerting features that allow staff members to become aware of issues in a timely fashion. Eventually, every IT department will be questioned on the reliability and performance of various elements of the enterprise, so long-term data collection and reporting is a must in any monitoring system. Finally, being able to import and query data from various server agents and network flow sensors will be invaluable when it comes to profiling (either formally or informally) the enterprise.

InterMapper: InterMapper by HelpSystems may be an appropriate part of your IT department's enterprise monitoring system's software suite. With this tool, your IT staff can create network and server maps that are appropriate for each department and stakeholder. Since these maps are based on automatically discovered topology, they are always accurate. InterMapper can perform the usual ICMP and TCP monitoring functions. It also uses agents installed on the servers to gather more detailed indications as to the health of each server. There are InterMapper agents for Windows, Linux, and various other flavors of UNIX. If your network supports Netflow, InterMapper can use that data to allow the monitoring group to see how much (and what kind of) traffic is flowing over various parts of the network.

Although it is advanced enough to have the features that senior network managers want, InterMapper is also easy enough to use that it could be pushed out to the help desk and various other non-technical personnel without becoming a training burden. You can find more information about InterMapper at http://www.helpsystems.com/intermapper.