

# Keys to Practicing Proactive Network Management

By Charles Thompson

**SMART** people coupled with smart tools leads to smart business decisions. However, even very smart people make very bad decisions if they have no information—or worse, incorrect or misleading information. When it comes to successful network management, good information is essential. So what can responsible IT managers do to make sure they are receiving the best information that will help them manage the network successfully?

IT managers often turn to network analysis tools when critical issues strike. However, these same managers may not realize that most crises can be avoided if they use network analysis tools to monitor and test the network continuously. To be able to do this, IT managers need to identify rising problems before they cause expensive downtime and become a user irritation. Many corporate administrators practice crisis management rather than network management because they use ineffective analysis tools, or they use the right tools in the wrong way.

All IT managers will want to keep a few things in mind if they want to manage a network in a preventative, proactive manner rather than merely troubleshooting. Every IT manager needs a good understanding of the corporate network. Understanding the network well enough to manage it in a preventative manner requires setting a baseline to define what is and isn't normal activity on the network. This includes capacity planning and monitoring the network to ensure complaints and downtime are kept to a minimum.

A robust, distributed, and multi-topology protocol analyzer is the most efficient tool to help IT managers have the information that will allow them to have total, proactive control of a network. To practice the most proactive network management, IT managers will want to have a protocol analyzer with long-term logging and traffic generation capabilities as well as configurable alarms.

IT managers of unmanaged or ineffectively managed networks are always reacting to problems as they arise. Users complain about slow servers and unavailable databases. Systems continually go down for unscheduled troubleshooting and upgrades, with “solutions” that often make problems worse. Effectively managing a network means obtaining

accurate, objective and pertinent metrics before any decisions are made, especially decisions to spend money. The only solution that can provide all the metrics needed is a distributed network analyzer coupled with remote probes for complete visibility into all areas of the network.

An investment in a distributed network analyzer is well worth the money. For example, an analyzer can immediately inform IT managers when bandwidth usage spikes unusually, thus threatening the health of the network. A mature analyzer includes the ability to page an administrator when undesirable network conditions are sensed. This allows time to quickly take action and thus avoid numerous user complaints.

For example, consider the following scenario. One company's router usage alarms were triggering all over the network. There had been no negative repercussions yet, but if the trend continued upward at the current rate, the network would be showing intermittent problems within days, and perhaps be totally overwhelmed within a matter of weeks. The IT manager at this company did not know if she should buy faster routers or faster WAN service, or both.

The manager understood that good decisions require applicable and correct information, so she used the analyzer to decode the increased traffic. The manager discovered that the increased bandwidth usage was the result of various file-sharing applications. By looking at long-term trending logs provided by the analyzer, she was even able to determine that the file sharing applications spread from a single department, where the first concentrations of suspicious port/protocol traffic were seen.

Given the detailed information from the analyzer, the administrator configured the firewall to block the ports currently known to carry such traffic. In addition, the manager instructed Human Resources to update the employee handbook to explicitly forbid file sharing applications. Good information, good assumptions, good business decisions.

This scenario demonstrates some benefits of a proactively managed network.

- ▼ Because the bandwidth spike was caught by IT before users noticed any slowdowns, no money was lost in system downtime.


- ▼ No money was wasted on hardware upgrades or other solutions that ultimately would not solve the underlying problem.
- ▼ The solution (enforcing corporate network usage policies) saves the IT department money by making upgrades unnecessary and the entire company saves money through improved staff productivity.
- ▼ The solution helps the company avoid potentially serious legal liability.

When users do alert of a network problem, having a deeper knowledge of the network speeds up resolution, preventing failed solutions and repeated complaints. This knowledge is best obtained through information that only an enterprise-strength analyzer can provide.

Another company, one with an ineffectively managed network, had similar router issues, due to one employee's surreptitious file downloading sessions. The company went ahead and upgraded the router without any information to base the purchase on. As the company was not deploying VoIP or any other bandwidth-sucking technology, this router upgrade was unnecessary, and came only after repeated, unresolved user complaints had taxed the already overworked administrator's time. A company will not survive a competitive market for long if they repeat this pattern in any aspect of the business, especially crucial IT infrastructure. Bad information, bad assumptions, bad business decisions.

To manage a corporate network with the aim of avoiding user complaints and downtime, an analyzer should include some key measurements and testing tools. The most complete, distributed solutions handle wireless, WAN, gigabit, and other topologies with seamlessly interoperable probes and consoles. Long-term logging

capability lets managers analyze networks over time. With the data to understand what are the characteristics of a healthy network—it is easier to spot impending slowdowns or future areas of concern. Triggered notifications let managers set conditions under which they want an automatic heads-up notification. The best conditions include a rule-based filter engine that lets managers program alarms based on flexible criteria. Traffic generation capability will help managers test out hypotheses during troubleshooting and planning when they need to see the effects of certain levels and kinds of traffic on a particular part of the network.

Smart people coupled with smart tools leads to smart business decisions. IT managers that use a distributed network analyzer to monitor their networks continuously will be able to prevent problems before they happen and resolve issues as they arise. That in turn will keep users happy and businesses running smoothly and profitably. By using a comprehensive network analyzer, smart IT managers will have the information that can lead to smart business decisions. 

---

*Charles Thompson, Senior Systems Engineer for Network Instruments, LLC ([www.networkinstruments.com](http://www.networkinstruments.com)), works with the Network Instruments Sales Organization to provide technical expertise and in-depth product information to enterprise accounts. Network Instruments is the industry leading developer of superior, user-friendly and affordable network management, analysis and troubleshooting solutions. Charles can be reached at 952-932-9899 x234 or [charlest@networkinstruments.com](mailto:charlest@networkinstruments.com).*

*Supporting Servers and Desktop Environments*

# SUPPORT™