Shareware Spotlight Column

Powerful and Free Tools For Network Analysis

By Jim Justen

Last month we took a look at a few of the many excellent tools for network analysis that are available for free in the open-source realm. In response to reader comments that I focus too much on the Windows environment, this month I'm continuing the topic, but looking more closely at Linux applications.

In my defense, I concentrate on Windows because it is a constant in the wide-ranging readership of this magazine. Whether you work in a mainframe or standard client/server environment, odds are you are using some form of Windows client, whether as an admin station or simply for general office documents.

But I also know that many readers are now embracing Linux as their administrative platform, and rightly so. As I mentioned in last month's column, some of the most powerful network tools are only available on Linux (or rather, POSIX-compliant) platforms, or often the Windows version development lags behind that of the Linux.

Ironically, in spite of the ascendance of the open-source software concept, Linux has been weathering attacks on many fronts. The lawsuit by SCO threatens the entirety of Linux, and European software patent hearings loom over many open-source efforts.

In fact, over the time in which I wrote this column, the Web sites of a number of open-source applications have posted "closed until resolution of patent hearing" notices—forcing me to find new, unaffected applications. While perhaps this is merely posturing by developers to bring attention to the severity of the threat, the threat is decidedly real.

In spite of these worries, the concept remains attractive. Indeed, if any one category of software represents the possibilities inherent in the open-source ideal, it is network analysis tools.

This month's selections are remarkably powerful applications for tracking network performance and issues. Most of these programs are so complex and full-featured that it would be easy to devote an entire column to each one. Of course, space prohibits that, so by necessity these are brief overviews of some of the best tools available.

BIG BROTHER 1.9 BY BB4 TECHNOLOGIES

Despite the ominous name, *Big Brother* is your friend. Trust me. Though it may sound vaguely like a hacker tool, in fact *Big Brother* is a powerful network and systems monitor for legitimate enterprise network administration.

Using a client-server architecture, *Big Brother* aggregates system health data from monitored devices (clients) to a central server. The server side is primarily a Linux tool, although there is a version for Windows, and it slightly lags the Linux version in features.

Client devices are polled for status, and results are displayed via a Web interface called BBDisplay. Using a simple grid of color-coded dots following the name of the monitored server, this Web interface is the heart of *Big Brother*. We all know (hopefully) that red means stop and green means go, and *Big Brother* uses this deeply instilled piece of human experience to convey information quickly. For example, you can tell whether you may safely go on a coffee break at a glance, even from across the room, because the background of the entire monitoring page is the color of the most serious event in the network.

Tests are available for a wide range of server health metrics such as: CPU load (a five-minute load average), disk space alarms, DNS response (essentially a simple nslookup), and verification of the SMTP process. You can customize the scripts to verify the presence of any process you choose.

Big Brother can send alerts to devices such as pagers and cell phones. These alerts use a three-digit code to indicate the type of warning, and though this is a bit cryptic at times, it gets the job done. And, proving its enterprise-level-availability chops, *Big Brother* can be run on parallel systems for redundancy.

One touch that I found amusing is that *Big Brother* has a specific port assigned for client-to-server traffic. Can you guess what port number is assigned to *Big Brother*? If you guessed port 1984, George Orwell would be proud of you.

Clients exist for even the most mixed of multi-platform environments and are available for VMS, AS/400, Mac, and Novell among others. In addition, there is an active community for questions and continued development. The dedication of this group is impressive, and they have even developed plug-ins for monitoring National Weather Service alerts!

There are flaws: Although *Big Brother* can monitor Web servers, the process simply confirms a response and checks for the word "error" in the returned page. Also, HTTP server testing will fail on password-protected pages, which often represent the most mission-critical elements of a Web site.

And unfortunately, *Big Brother* is not really freeware. It could be called "might-be-freeware." Loosely, if the system you install on is profit-generating in some form, it requires a license. However government, individuals, charities and even many types of business will not need to buy a license. Even if a license is needed, the cost is reasonable. Paid support options are available for the free licenses, and an impressively enhanced commercial version is available also, and may be well worth the cost for enterprise installations.

All told, *Big Brother* boasts powerful features, and an interesting melding of commerce and altruism. It would be a good choice for any organization seeking better monitoring of its networked resources.

MULTI-ROUTER TRAFFIC GRAPHER (MRTG) 2.1.0 BY TOBIAS OETIKER

The foundation of any stable network is a solid baseline for normal network activity and behavior. *Multi-Router Traffic Grapher (MRTG)* is truly a best-of-breed tool for this purpose. One of the "greatest hits" of the open-source world,

MRTG has become a must-have tool for serious network administrators.

Briefly stated, *MRTG* generates graph images for a visual representation of the traffic counter results pulled from any SNMP-enabled device, such as a router or switch. These graphs are embedded into Web pages and viewable in any Web browser.

However, this explanation doesn't begin to describe the full range of *MRTG's* possibilities. This is a highly complex tool with a vast range of features and possibilities.

MRTG is written in Perl and is available in both Windows and Linux versions. It is not especially easy to install on Linux, and Windows is more challenging yet. However, provided you have a current version of Perl installed, it is a more tedious than difficult process.

Once you jump the install hurdles, *MRTG* is stable and reliable and not difficult to configure for basic deployment. And as is the case in so many open-source projects, there is an active and helpful user community and a wealth of information on the Web dedicated to clever implementations of *MRTG*. Chances are somebody has already tried what you would like to do and shared their experiences.

I was especially impressed by *MRTG's* logging implementation. It maintains a constant-size log file, and yet provides extensive graph views of activity in daily, weekly, five-week, and yearly formats. Unlike some comparable commercial programs, you will never lose crucial historical data due to excessive log size. Moreover, certain very long-term patterns and trends of network trouble only become apparent in graph form. When looking for clues to elusive connectivity issues, this can be a lifesaver.

MRTG can monitor any SNMP variable on a network, the basics being items such as disk activity, server requests, or CPU activity. If you use external programs, *MRTG* is mostly limited by your imagination. There is even an implementation of *MRTG* being used to measure ocean levels. In fact, *MRTG* is being used to measure everything from temperatures to keyboard and mouse activity. In short, if you can measure it, *MRTG* can likely graph it.

Although challenging to implement fully, the rewards of MRTG are well worth the effort.

NEWTRAFFIC 0.1.3.1 BY ROBERT SANDILANDS

Tools like *MRTG* and *Big Brother* answer the question: *what is happening on my network?*, but sometimes the question becomes *what **would** happen on my network if…*

NewTraffic supplies an answer.

NewTraffic generates large amounts of UDP/TCP traffic from clients (single or multiple) to servers (also single or multiple) for the purpose of stress-testing firewalls, routers, VPNs and other infrastructure between the two points.

NewTraffic does not provide metrics or measurements of any kind. It simply simulates traffic to answer hypothetical questions such as whether it is possible to configure a router during a given number of user sessions, or how much of a certain type of traffic would overwhelm a network link.

Clients are available for Linux and Windows, and configuration is very easy.

The interface is just a single window with fields for time intervals, number of connections per client, target address, port, and payload. Significantly, you can have packets randomize or increment in size for realistic results.

That is the extent of the interface, there is no results panel. Rather, the results of this tool only come from your observation of network behavior, or through metrics from tools like *MRTG* or *Big Brother*. Despite the minimalism of the interface, the insights you can gain from the *NewTraffic* are invaluable.

Programs like *NewTraffic* showcase the best of the open source/freeware concept, a simple and effective solution for network administrators who need to know the limits of their network.

CONCLUSION

As always, this month's applications are available in NaSPA's download libraries, and your comments are welcome: jimj@naspa.com.

Jim Justen is the NaSPA VP of Shareware.

BigBrother: http://www.bb4.com
BigBrother add-ons: http://www.deadcat.net
MRTG: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/index-2.html
NewTraffic: http://robert.rsa3.com/traffic.html
More about the threat of European software patents to open-source software: http://swpat.ffii.org/index.en.html