Survey of Network Monitoring and Visualization Tools

Below are screenshots, short descriptions, and URLs of various network monitoring and visualization tools. This is not a comprehensive list of tools, but rather a representative sample. A larger list of network monitoring software is available at http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html.

The majority of network monitoring and visualization tools are intended for systems administrators in enterprise computing settings. The tools often have poor user interfaces, and require users to understand far more about networking than can be expected of a novice.

Most of the network monitoring and visualization tools come in the following varieties:
- Line graphs of network performance
- Device-centric views of network infrastructure (usually implemented as a graph in which nodes are devices, edges are traffic)
- Tools to view and dissect individual packets
- Command-line tools

Since we’re focusing on network visualization, I’ve left command-line tools out of this survey.
HP OpenView

HP OpenView is one of the most common enterprise network management suites. A list of all OpenView products is available at http://www.openview.hp.com/solutions/a-z.html.
Other OpenView-based products

Several companies other than HP have developed applications using OpenView. Nastel Technologies is an HP partner that has developed monitoring tools for IBM WebSphere.

Network Magic

Network magic is the only visualization tool I’ve found that is aimed toward home users. It shows a topology of all machines on a home network. It claims to ease network troubleshooting by automatically finding problems, but from my experience using it, the help it provided was little more than a Microsoft Windows help library. I did like that it allowed users to flag and monitor suspicious machines on the network, however, I was expecting more from this program based on the hype at its website:

http://www.networkmagic.com
Etherboy

NDG software, creator of Etherboy, was recently purchased by another company and this product is no longer available. However, you can read an apt review of the software (and its sister products) at [http://www.pcmag.com/article2/0,1759,90440,00.asp](http://www.pcmag.com/article2/0,1759,90440,00.asp).
NetVizor

NetVizor elegantly visualizes large computer networks. I don’t think we’ll see any home networks this large.

http://www.cc.gatech.edu/gvu/ii/netviz
Etherpeg/Etherwatch

Etherpeg (for Mac) and Etherwatch (for Windows) are two pieces of software that grabs images out of a network traffic stream and creates a collage. Etherwatch also allows users to watch Google search terms being used on the network. Both pieces of software raise privacy issues, but they seem like they would be at least mildly interesting to home network users.

Etherwatch (Windows version) - http://www.etherwatch.com
Friendly Pinger

Friendly Pinger is a freeware program that shows a topology of network devices. You can use the program to monitor file sharing and available services on the network, as well as audit software and hardware on any network machine. After trying this software, I wasn’t terribly impressed. The user interface was clunky, and I couldn’t think of any reason I would actually use this software in a real-life situation.

http://www.kilievich.com/fpinger/preview.htm
Adrem Netcrunch

Adrem Netcrunch is yet another network visualization and monitoring tool (available for the low price of $1195 a license. Obviously I didn’t try it out!). The user interface looks like a Windows XP-skinned version of HP OpenView.

Network Performance Charts

Here’s an example of a network performance chart. Most network performance graphs look similar to this one.

I grabbed this particular chart from [http://www.infotoday.com/cilmag/sep01/schuyler.htm](http://www.infotoday.com/cilmag/sep01/schuyler.htm)
NimSoft Traffic Analyzer

NimSoft Traffic Analyzer picks apart Ethernet packets to give performance information. It looks remarkably like the Network and Performance monitors in Windows Task Manager.

http://www.nimsoft.com/environments/traffic-analyzer.shtml
A (Literal) Network Map

Here is a campus map with networking infrastructure information overlaid on it. The map tells little to an outsider, but a person familiar with the Drake University campus can find information about locations of networking infrastructure based on the picture below.
GT Network simulation

Here is a simulation of a campus network created by Professor Richard Fujimoto’s research group. I don’t really understand the details of this visualization, but I think it’s pretty.

Ethereal

Ethereal is a packet capture and sniffing program. It’s handy for collecting network traffic traces, and getting a sense of how many packets are flying across a network. Ethereal is a tool that would be very overwhelming to someone who knows little to nothing about networks.

http://www.ethereal.com
Etherape

Etherape looks suspiciously like Etherboy, except that the size of lines between computers changes along with the amount of network traffic.

http://etherape.sourceforge.net
Host Grapher

Host Grapher collects statistics about individual machines, rather than networks. Machine statistics are shown as graphs on a website. Host Grapher isn’t very exciting or pretty, but maybe it’s useful to someone.

http://software.foxlink.org/hostgrapher2/
Netdisco

Netdisco is a web-based network management tool for networks larger than what you might see in someone's home. It, too, is not very exciting or pretty.

http://netdisco.org
**VISUAL** (Visual Information Security Utility for Administration Live)

VISUAL is a network security visualization tool that allows users to see communication patterns between home networks and outside hosts. The internal network is represented as a grid, and outside hosts are represented as yellow squares. The tool is aimed to sysadmins who need better tools during crisis situations.

This tool came from the paper: Robert Ball, Glenn A. Fink, and Chris North. “Home-centric visualization of network traffic for security administration.” Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security.

![VISUAL tool](image)

*Figure 2: VISUAL displaying 80 hours of network data on a home network of 1020 hosts.*
**TNV: Time-based Network Traffic Visualizer**

This software is a visualization system for intrusion detection, and is very much geared toward people who work as intrusion detection specialists. This software can help people understand what normal (and abnormal) network traffic looks like, and examine packet details in order to investigate security incidents or troubleshoot network problems. The details provided by this software are far too advanced for use on a home network. You have to know quite a bit about networking in order to derive any useful conclusions from what you see in the visualization (i.e. you would need to know that a consistent flow of packets may likely be an ssh session, while as bursty heavy traffic might be associated with a web server).

More Information about TNV is available at:
http://userpages.umbc.edu/~jgood/research/tnv/


![Figure 1. TNV visualization: host A is under a prolonged SNMP attack from host B. The lower part of the figure shows the details of the attack, including the packet payload.](image-url)
CyberSeer

The authors of this paper propose (but have not yet developed) an immersive system for network management and security called CyberSeer. Administrators view network information via a combination of visualizations and sounds. I like this idea! A depiction of what the system might look like is below.

Other Useful Tidbits

Security Visualization Software
Greg Conti, a PhD student at Georgia Tech, has compiled an extensive survey of network security visualization tools. This survey is available at:

http://www.rumint.org/gregconti/publications/20040731-visual_security_survey.ppt

Greg’s website also has multiple papers and slides from talks about security visualization. http://www.rumint.org/gregconti/index.html

Top 75 Network Security Tools
Insecure.org, home of nmap, has an extensive list of network traffic capture and various security tools. Check this list out! It’s good!

http://www.insecure.org/tools.html

jpcap
jpcap is a Java API for developing packet capture software in Java. It also includes quite a bit of pre-packed code examples showing how to capture and create basic traffic visualizations. The examples included with jpcap are slightly awkward to use in Windows, especially if you have more than one network card. Overall, though, this API looks promising.

http://jpcap.sourceforge.net

SNMP
SNMP is probably overkill for this project, but it might be worth looking at again this fall if we get a chance. Jonathan Sevy at Drexel University has an open-source implementation of the protocol in Java.

http://edge.mcs.drexel.edu/GICL/people/sevy/snmp/snmp.html

Piccolo
Piccolo is a zoomable user interface toolkit for Java and .NET. It’s neat!

http://www.cs.umd.edu/hcil/piccolo

Home Network Security FAQ
CERT provides information about security risks to home networks. This can be a useful reference as we complete the home network visualization project.

http://www.cert.org/tech_tips/home_networks.html
**PinPoint**
Emre Kicimin, the author of PinPoint, does research on using data mining to detect faults in network services. He has written a toolkit called PinPoint can be used to detect application failures. The software is available for public use (and is being used by some students at UC Berkeley and in a few other places). We might want to consider using PinPoint in conjunction with the network visualization project:

[http://www.stanford.edu/~emrek](http://www.stanford.edu/~emrek)


**Chronus**
Chronus uses “time travel” to troubleshoot computer problems. That is, it saves historical information about a computer’s configuration so that when troubles occur, users can refer to a previous working configuration of the machine to find out what broke. It would be useful to make a version of this software that stores historical information about network infrastructure rather than just individual computers.

See “Using Time Travel to Diagnose Computer problems”

**Pebbles**
The Pebbles project at CMU investigates the use of handheld remotes to control networked devices in the home.

[http://www.pebbles.hcii.cmu.edu/](http://www.pebbles.hcii.cmu.edu/)