PROCESSOR.

Tech & Trends   🖶 Click To Print

General Information
June 11, 2004 • Vol.26 Issue 24
Page(s) 3 in print issue

It Works Better When You Plug It In
Testing Tools Help Isolate Network Problems

One of the most common headaches for a corporate IT admin is the Monday morning phone call complaining that a network connection is down. It was working OK on Friday. Did someone kick out the cable? Did a port fail on a switch? Is the configuration fouled up on the PC itself? It could be a simple fix, or it could be an all-day nightmare.

Frequently, the only tools a small business may have to diagnose the problem are a notebook PC and the experience of the admin. But an alternative exists: a whole family of network-testing tools from a variety of manufacturers. These tools provide the traditional "ping" checking that is the mainstay diagnostic test of networking, as well as more physical analysis such as cable continuity and wiring validation.

Network-testing tools break into a couple of broad categories. One distinction is between tools that test the physical networking layer (to determine, for example, if a Category 5 cable has been correctly wired) and those that test the data that moves across the wire. Another distinction is between tools intended for diagnostic testing of problems and those that monitor and gather statistics on network health.

At the high end of the product universe are network management tools such as HP's Open-View suite, which provides monitoring and control capabilities, as well as trouble-reporting and escalation. For most small and medium-sized enterprises, however, these advanced tools are both financially prohibitive and beyond the functional requirements of their admins.

■ Good Networks Are No Fluke

One manufacturer known for its handheld test equipment is Fluke Networks. Fluke's product set for the SME market is centered on diagnosing common connectivity and configuration problems. At the low end of the product line's price range, the LinkRunner is a handheld tester that can identify physical faults in an Ethernet drop, as well as run a ping to a known IP address. The unit can acquire its IP address via DHCP, or the IP address can be manually entered. The advantage of this $350 unit is that it can test the network drop independent of the workstation, reducing the number of variables.

The $1,500 NetTool is the next step up the ladder for Fluke. In addition to having all the capabilities of the LinkRunner, the NetTool can be placed between an end-user device (such as a workstation) and the rest of the network, where it can be used to monitor activity. Using the NetTool, admins can diagnose packet errors and monitor activity on the local segment for problems such as unauthorized protocols on the network.

At the top of the SME product line for Fluke is the OneTouch Series II, priced at approximately $3,500. The OneTouch uses SNMP requests to map out the switched topology of your LAN; it can

then report on the condition of ports and link status. In addition, the OneTouch can analyze network performance and utilization on the segment it is connected to. Using a Web server embedded in the unit, an admin can even remotely monitor and control the tests performed.

■ Watching The Packets Flow By

In comparison, Agilent Technologies' product line is aimed at monitoring and analyzing both network faults and overall network performance. Its entry-level products are software-only and run on off-the-shelf PCs. The $3,500 Network Analyzer lets an admin monitor and analyze traffic on a local segment; it can also remotely monitor segments using capture software that runs on a PC attached to that segment (licenses for the remote capture software start at $700 per node; quantity discounts are available).

Depending on the NIC card used in the PCs, some physical-layer faults can be detected. Although it is possible to use this configuration with Gigabit Ethernet, it may not be possible to capture all of the packet traffic on a highly utilized network. If this becomes an issue, Agilent recommends the use of one of its dedicated products that use proprietary hardware, although the five-figure price tags for these units may cause sticker shock for the typical SME.

Network Associates offers capabilities similar to Agilent's with its Sniffer product line. Like Agilent's Network Analyzer, the Netasyst Network Analyzer is a software-only solution intended to run on an existing PC. This $2,000 product can decode packets for many common protocols, analyze traffic, and uncover problems such as dropped packets and frame errors. In addition, Netasyst provides early detection of viruses by comparing network traffic against Network Associates' constantly updated database of virus signatures. The $5,000 Expert Edition adds advanced analysis tools to help manage and predict future problems with the network, as well as diagnose current ones. Like Agilent's product line, the Sniffer line is also available in high-performance (and pricey) dedicated hardware solutions.

Both the Agilent and Network Associates products can also integrate into a broader network management infrastructure, using solutions such as HP OpenView. This allows for greater flexibility in terms of alert and notification. For example, an admin can be paged if unusual traffic patterns are observed on a critical network segment.

Why should an SME consider using these products? That will depend a great deal on how critical network efficiency and reliability is to the company's success. If the network environment is relatively stable and its current performance seems acceptable, the existing tools in use by the IT department are probably sufficient to the task. But if workstations are constantly being moved, if traffic seems to get congested for no good reason, or if the admins need a good look at the packets going between their Web server and their database engine, a network analyzer may be just the ticket. ■

by James Turner

View the chart that accompanies this article.
(*NOTE: These pages are PDF (Portable Document Format) files. You will need Adobe Acrobat to view these pages. **Download Adobe Acrobat Reader***)