Analyzer From Afar

Distributed LANalyzer agents gather network stats for centralized management.

Laura Chappell

Distributed analysis is an exciting addition to version 2.0 of Novell's NetWare Management System (NMS). Based on the company's LANalyzer for Windows, Novell's NetWare LANalyzer Agent enables network managers to capture packets and solve problems on an internetwork—without venturing out of their offices.

Typically, nondistributed protocol analyzers only capture and analyze traffic on the locally attached segment; because bridges and routers filter out traffic from the local segment, network analyzers offer only a "local view" of a network's health. However, the NetWare LANalyzer Agents, located throughout the internetwork, automatically detect and report to the centrally located NMS Console such problems as duplicate IP addresses and network overload. NetWare LANalyzer Agents also enhance NMS's auto-discovery feature by adding every device on the monitored segment to the NMS maps, regardless of type or protocols in use.

Distributed Analysis Advantage

Anyone who has used a nondistributed analysis system on a large internetwork is familiar with the limitations imposed by devices that filter out network traffic. To get a snapshot of network health using a nondistributed analysis system, you must move the network analyzer from segment to segment because bridges filter packets based on node addresses and routers filter packets based on network addresses.

In contrast, distributed network analysis systems—such as NMS with the NetWare LANalyzer Agents—place agents on various network segments and report back to a centralized console (the NMS Console). If a network error occurs or an unusual condition arises, the NetWare LANalyzer Agent reports a "rising alarm," indicating that an alarm threshold has been crossed. If, for example, the CRC alarm threshold is set at 5 CRC errors per second, the LANalyzer Agent automatically transmits a rising alarm message to the NMS Console when this threshold has been exceeded.

To capture packets on the network, the console sends a capture request to the NetWare LANalyzer Agents. The agents located at the server capture the desired packet into a predefined buffer area. You can then view the decoded packets at the NMS Console. Available decodes include NetWare 2.x, 3.x, 4.x (including SAP, RIP, IPX, SPX, and NCP), AppleTalk (Phase I and II), TCP/IP (including SNMP), and NFS.

Setting Up the Ideal Distributed Analysis System

The NetWare LANalyzer Agent (NLA) consists of a set of NetWare Loadable Modules (NLMs) strategically loaded on any server running NetWare 3.x, 4.x, or NetWare 3.12 Runtime (included with NLA). You must load NLA on one device on each segment you want to monitor.

The network depicted in Figure 1 consists of three Ethernet segments and two token ring segments separated by repeaters, bridges, and routers. NetWare LANalyzer Agents have been placed on each segment that is separated by a bridge or a router because these devices filter out traffic from the attached segments.

The NetWare LANalyzer Agents must be installed on devices that use promiscuous-mode network interface cards and drivers, which receive and buffer traffic destined for stations other than the local device or a broadcast address. For example, if you want the NetWare LANalyzer Agent on Server FS1 to capture all traffic sent to the NMS Console, the card and driver loaded on FS1 must be in promiscuous mode.

The following promiscuous-mode drivers ship with the NetWare LANalyzer Agents:

- Novell NE1000 8-bit Ethernet board (NE1000);
- Novell NE2000 16-bit Ethernet board (NE2000);
- Novell NE/2 16-bit Micro Channel Ethernet board (NE2.LAN);
- Novell NE/2-32 32-bit Micro Channel Ethernet board (NE2_-32.LAN);
- Novell NE3200 32-bit Bus Master Ethernet board (NE3200P.LAN);
- 3Com Etherlink II Ethernet board (3C503.LAN); and
- MADGE Smart 16/4 Ringnode token ring board (MADGE-ODI.LAN).

You can obtain promiscuous-mode drivers for other types of cards from the card manufacturers, though not all cards support promiscuous mode. (For example, the chip set used by IBM's 4/16 Token Ring cards [TROPIC] prohibits them from using promiscuous mode.)

The NetWare LANalyzer Agents fully implement all nine groups of the Ethernet RMON (Remote Monitoring) standard and support SNMP on TCP/IP, IPX, and AppleTalk protocols, enabling network managers to query the NetWare LANalyzer Agents with any network management console that supports the standard RMON agents. The advantage offered by the NMS Console, however, stems from its easy-to-use interface structured on Novell's LANalyzer for Windows (see Figure 2).

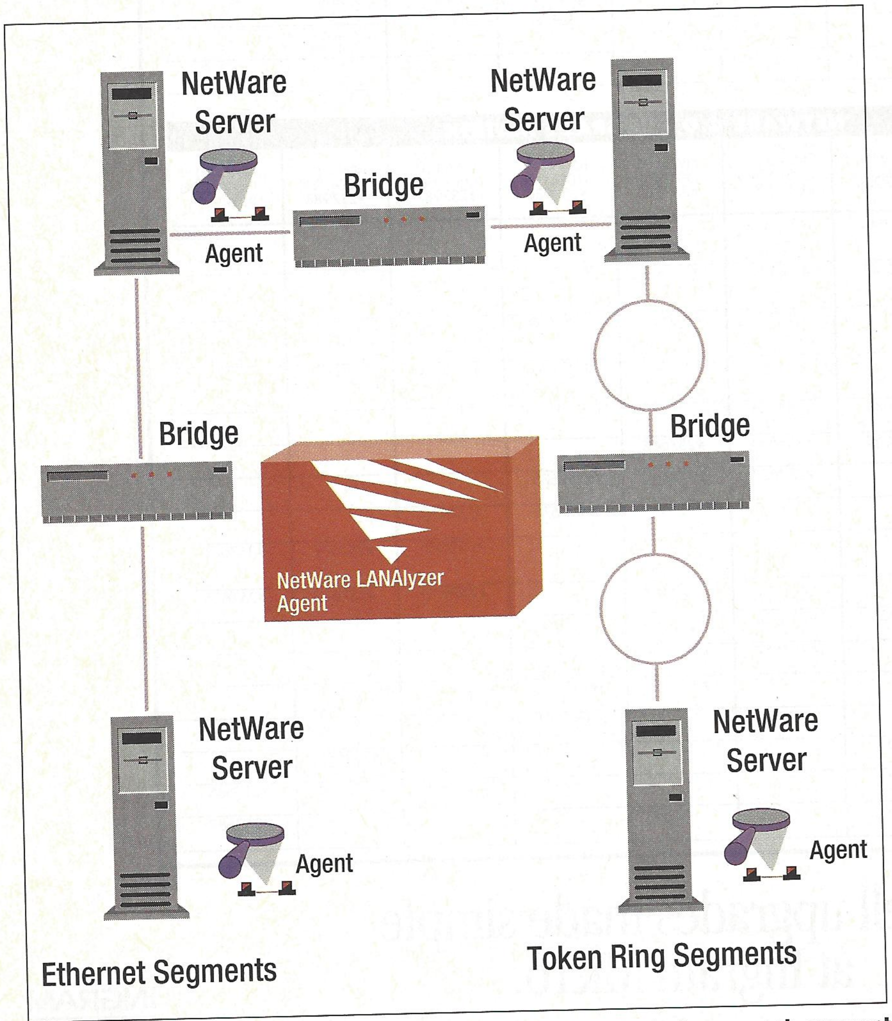


Figure 1. NetWare LANalyzer Agents must be loaded on one device on each segment that is to be monitored.

Network Checkup

NetWare LANalyzer Agents track and report the most common Ethernet and token ring network performance errors. A comprehensive tutorial system, NetWare Expert Tutorial, is included with the product to provide training in centralized network management and troubleshooting. The system defines the major errors that occur on Ethernet and token ring networks, and (regardless of error type) posts an alarm icon next to the problem segment whenever an unusual event occurs.

Events detected by NetWare LANalyzer Agents include the following:

- **Utilization (Ethernet and token ring).** This alarm indicates that usage on an Ethernet or token ring segment has exceeded the maximum threshold. A gradual increase in utilization usually indicates normal network growth, but a sudden increase generally means that an unauthorized data transfer has taken place, or that noise or jabber on the cabling system has increased.

- **Broadcasts per second (Ethernet and token ring).** This alarm indicates an increase in the number of packets addressed to all devices on a network segment. Typically, the number of broadcast packets should represent a low percentage of network traffic. A sudden increase in their number may indicate that a routing problem is causing a broadcast storm.

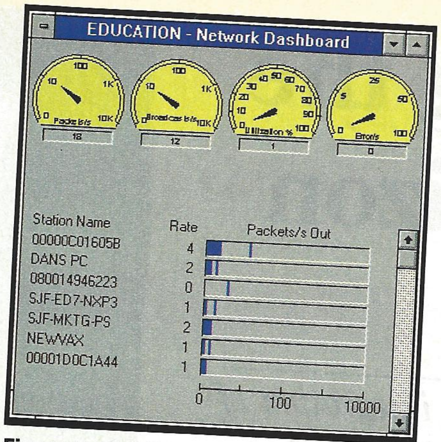
- **CRC errors per second. (Ethernet).** A CRC error indicates that a packet has been corrupted either by a faulty network interface card or a faulty cabling system. Many CRC errors per second attributed to a single station indicate a faulty network interface card. CRC errors attributed to numerous stations on the network signal a cabling problem.

■ **Fragments (Ethernet).** Although fragments are normal Ethernet events, their sudden increase can indicate a problem with a network component. A good rule of thumb for fragments is to examine them in conjunction with utilization. A simultaneous jump in usage and fragments indicates an increase in network cabling system utilization. If fragments increase while utilization remains steady, it's likely you have a faulty network component.

■ **Undersized and oversized errors (Ethernet).** An undersized packet does not meet Ethernet's minimum 64-byte packet size requirement; an oversized packet exceeds Ethernet's largest allowable packet size (1,518 bytes). Undersized and oversized packets indicate that a faulty or corrupted LAN driver is being used on the network.

■ **Beacons (token ring).** Beacons on a token ring network indicate a disabling hardware error. When the token ring network is beaconing, the ring is not functional. You can locate the fault domain (and thus the cause of the beacon situation) by examining the NetWare LANalyzer Agent's Ring Information Table.

■ **Congestion errors (token ring).** Congestion errors indicate that a token ring station has insufficient buffer space to copy a frame that is addressed to it. If a packet is sent to the file server and the server cannot buffer the frame, the server card is considered to be congested. You may need to reconfigure the adapter to allocate additional incoming packet buffers.



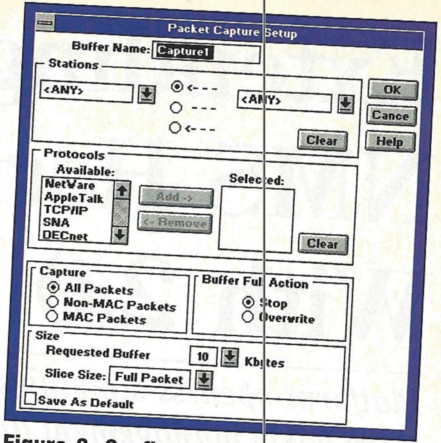
Station Name	Rate
00000C01605B	4
DANS PC	2
080014946223	0
SJF-ED7-NXP3	1
SJF-MKTG-PS	2
NEWVAX	1
00001D0C1A44	1

Figure 2. The NMS Console interface for distributed analysis is based on Novell's LANalyzer for Windows.

Even if an alarm has not been generated, you can query the NetWare LANalyzer Agents to quickly determine network utilization, packets per second, error rates, traffic patterns, and so on. For example, if a user complains that he or she is unable to attach to the local server ("File Server Not Found"), the network manager can begin capturing packets on the segment to determine whether or not the station is transmitting and the server responding. The network manager can capture all packets from the station and server to determine if different frame types are in use as well.

As Figure 3 shows, configuring the NetWare LANalyzer Agent to capture specific packets (as defined in the example above) is an intuitive process: You simply enter the station name or node address of the device from which packets should be captured. You can perform a more complex capture by defining the protocol type of the desired packets. For example, if a NetWare File System (NFS) server is not responding to an IPX client, all NetWare (IPX) traffic can be filtered from the server.

Once packets on the network have been captured, the Packet Display window shows the NetWare, TCP/IP, or AppleTalk packets decoded in plain English. For example, if a token ring station is beaconing, the Packet Display shows the source of the beacons. In the full decode screen, the upstream neighbor's address is displayed, providing an easy way to locate the token ring fault domain.



Buffer Name: Capture1

Stations
<ANY> ● <--- ○ --- ○ <--- <ANY>

Protocols
Available: NetWare, AppleTalk, TCP/IP, SNA, DECnet
Selected:

Capture
● All Packets
○ Non-MAC Packets
○ MAC Packets

Buffer Full Action
● Stop
○ Overwrite

Size
Requested Buffer 10 Kbytes
Slice Size: Full Packet

□ Save As Default

Figure 3. Configuring the NetWare LANalyzer Agent capture filter is a fairly intuitive process.

NetWare LANalyzer Agent Bonus

NMS 1.1 created internet and segment maps that were not complete: If the NMS discovery server (NetExplorer server) could not detect a device, that device would not appear on the map. NetWare LANalyzer Agents, by comparison, add every device on their monitored segments to the maps, regardless of the device type or the protocol they use.

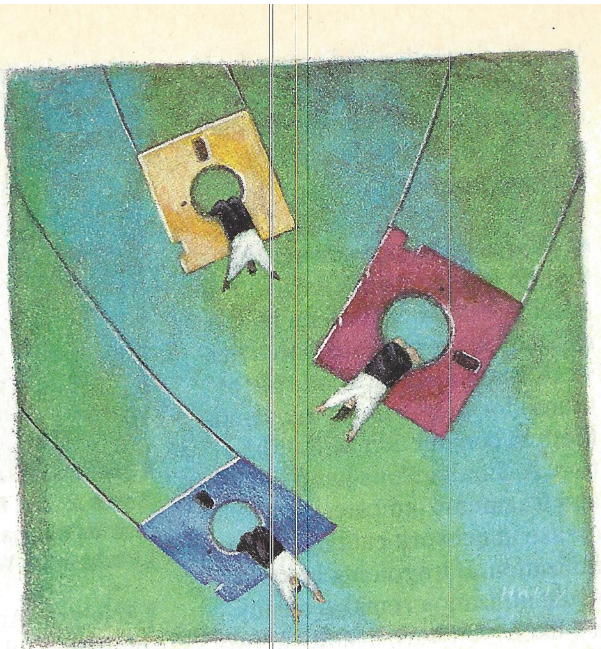
The NetWare LANalyzer Agents add a device (for example, a DECnet router on the local network segment) to the local map as soon as they determine that it is communicating on the local segment—a must for companies that want a comprehensive view of all network devices.

Thanks to NetWare LANalyzer Agents, NMS has come a long way since Version 1.0. Being able to analyze network performance from a single location improves troubleshooting response time and reduces the cost of travel time—not to mention wear and tear on your shoes. □

Laura Chappell is a senior partner with the Technology Consortium, a San Jose, California-based company that creates interactive multimedia training products for the high-tech industry.

Extending the NMS Horizon With 2.0

Platform openess simplifies integration of third-party management applications.



Roger Spicer

Novell's NetWare Management System (NMS) has left behind most of the immaturity inherent in a Version 1 software product and entered its Version 2 years as a more stable and full-featured product. NMS 2.0 is clearly worthy of serious consideration, but it shouldn't be judged solely on what falls out of the environmentally correct Red Box. As this article shows, extending management capabilities with third-party agents can make NMS a real competitor as a complete enterprise management platform.

With management services for NetWare servers, routers, and HMI (Hub Management Interface)-compliant hubs now included in the console (see Figure 1), NMS 2.0 has certainly improved. The platform's openness as well as the multitude of vendors that are developing NMS-compatible agents are making comprehensive management of NetWare networks much easier.

Most HMI-compliant hubs come bundled with the NetWare Hub Services agent, and though it's impossible to really manage a NetWare server without an agent, there may now be a viable alternative to using Novell-developed agents, which represent only the tip of the iceberg when putting the full power of a management platform to use.

All management platforms derive their true power from the variety of services that can operate on them and their adaptibility to users' environments. Companies using standardized platforms or specialized hardware, or those that already employ a variety of software management tools and utilities, may be able to enhance the NMS console to suit most or all of their management needs (see Figure 2).

Managing Superservers

An alternative to a Novell agent can be found in the area of server monitoring. At first glance, Novell's NetWare Management Agent (NMA) seems to provide all of the configuration information and statistics a network administrator could possibly desire. However, if you use the Compaq SystemPro, you can go a step further with that company's Insight Manager Agent. (See "Server Management: A Critical Control Is Added to Network Management," page 24.)

Managing 10BaseT Hubs

Although many hub manufacturers supply HMI agents with their hubs, a tool such as SynOptics Optivity for NMS offers more in-depth analysis. Using Simple Network Management Protocol (SNMP) over IP or IPX, Optivity for NMS manages the network as a single cohesive entity rather than a diverse collection of elements. Optivity's integration with NMS provides a consistent interface for managing hubs, servers, or any number of devices that don't require managers to learn separate tools for each of the components.

Cabletron's Spectrum for Novell NMS provides an alternative high-end approach to hub and cable management. Supporting Cabletron's Ethernet, token ring, and FDDI management modules, Spectrum uploads and downloads device configurations and provides statistical analysis by packet size and protocols used. Manageable hub products are also available from Standard Microsystems and Intel.

Network Utilities

Many familiar utilities are being integrated into the NMS platform. For example, popular utilities from Brightwork Development, Microcom, and Frye Computer Systems can now be launched from within the NMS Console.

With its LAN Server Watch, Brightwork Development offers server management utilities that monitor 30 key system parameters related to performance, security, capacity, and configurations and that use NMS alarms to alert network managers of abnormal behavior. LAN Server Watch automatically determines normal performance levels for the network and warns of abnormal behavior through console messages, e-mail notes, or a telephone pager.

Brightwork Development's popular NETremote+ provides the NMS Console with the same real-time support and monitoring found in the stand-alone versions. NETremote+ also facilitates network traffic analysis by providing PC configuration details, network information, and LAN statistics. If a user is having problems loading an application, for example, NETremote+ can examine the user's node configuration and memory information as well as test connections by sending packets to a workstation and noting the success or failure.

The company's LAN Automatic Inventory creates a database of information that includes user names and configuration details, software versions, hardware equipment (hard drives, floppy drives, processor, monitor), details about memory, and network and file-server information. The product detects and reports any changes in configuration, tracking when new applications or workstations attach to the LAN—even at remote sites.

Finally, SiteMeter, Brightwork Development's software metering and virus protection software, has also been ported to the NMS platform. (Microcom and Frye Computer Systems offer similar node configuration and troubleshooting products.)

Packet Analysis

One of NMS 2.0's hottest new features is its ability to monitor and analyze remote segments from a centralized console. (See preceding article.) A Software Developers Kit (SDK) for the NetWare LANalyzer Agent enables developers to create additional protocol decodes for the NMS system. For example, Triticom is now offering DecodesPlus for NMS, providing decoding for DECnet Phase IV and DEC LAT, Banyan Vines, and NETBUI/NETBIOS protocols. Networks running Windows for Workgroups, LAN Manager/LAN Server, VMS, OS/2, and Vines in addition to NetWare and Unix servers need this product.

Router Management

Novell offers NetWare router management as part of the NMS console. The NetWare MultiProtocol Router includes agents and can be monitored and managed by the NMS Console from the moment it comes out of the package.

Companies that have invested in high-end routers from Cisco or Wellfleet may want to evaluate the router management software developed by StonyBrook Services of Bohemia, New York. While the routers will be discovered and placed on NMS segments and the internetwork map just like all IPX and IP routers, the icon for Wellfleet or Cisco will appear. Double-clicking

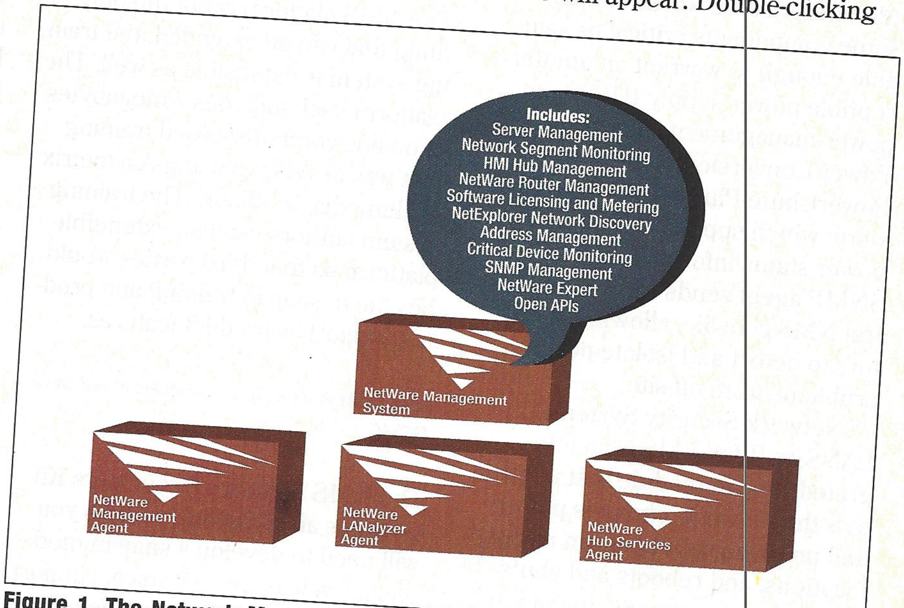

Includes:
Server Management
Network Segment Monitoring
HMI Hub Management
NetWare Router Management
Software Licensing and Metering
NetExplorer Network Discovery
Address Management
Critical Device Monitoring
SNMP Management
NetWare Expert
Open APIs
NetWare Management System
NetWare Management Agent
NetWare LANalyzer Agent
NetWare Hub Services Agent

Figure 1. The Network Management System Console includes services to manage servers, routers, and hubs.

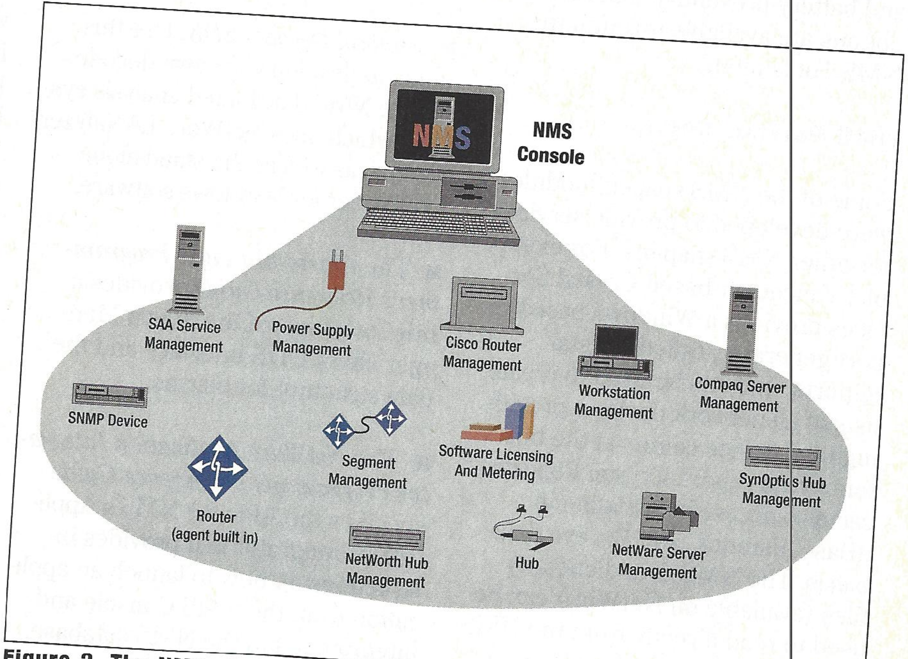


Figure 2. The NMS platform can be extended to fulfill a comprehensive set of management needs.

the appropriate icon will launch the router manager, initiating fault, alarm, threshold, and configuration management. A key configuration management feature offered by this software is its ability to upload or download router information.

UPS Management

All enterprise networks contain some components critical or valuable enough to warrant an uninterruptible power supply (UPS) and power management. American Power Conversion offers the APC PowerChute Plus SNMP agent software, which supplies UPS and line power status information. The SNMP agent sends traps to the central NMS console, allowing operators to detect and isolate power problems from off site.

Network Security Systems' LANSafe II for NMS is an integrated snap-in module that monitors the network, changes power and program settings from remote locations, and reboots and shuts down servers using its line of intelligent UPSs. Network-wide hardware and battery preventive maintenance options are available through the NMS Tools menu.

NMS Partner Services

Some of the NMS snap-in modules were developed to provide services for other NMS snap-ins. For example, Vancouver-based Crystal Services provides a Windows-based report generator, called Crystal Reports, that can be used to create lists of all network devices, providing total device counts at the bottom of the report. Crystal Reports can also access information in dBase, Paradox, and Btrieve databases. The NMS data dictionary files (available on NetWire) can be used to read directly from the NMS database files.

ServicePoint provides a technical support "help desk" snap-in module that opens calls, issues dispatches, and processes other sequences based on a script language. For example, on receiving an alarm from the power management snap-in module, ServicePoint automatically opens a call, dispatches a technician, and displays information on the hardware history, configuration, and even product warranty of the faulty component.

But Wait...There's More

The NMS platform is not the only thing that can be extended; the training system is extensible as well. The platform itself includes 7 megabytes of on-line computer-based training that was developed using Asymetrix Multimedia Toolbook. The training system authors used an extendible platform so that third parties would be able to snap in training and product support as product features.

One Great Idea Deserves an SDK

The NMS Software Developers Kit provides all of the information you will need to develop a snap-in module, as well as free technical support. The SDK includes about a dozen books, including the following:

- *Protocol Decodes SDK.* Use this guide to develop your own decodes for the NMS distributed analysis system, which uses NetWare LANalyzer Agents, as well as the stand-alone LANalyzer for Windows software.

- The *Alarm Manager Programmer's Reference Guide* provides a brief overview of the Alarm Manager client DDE interface and the data structure for alarms.

- The *NetWare Application Integrator Programmer's Reference Guide* specifies the APIs for NMS's Application Integrator and provides instructions on how to launch an application from the NMS Console and integrate it into the NMS database.

- The *NMS Database Schema and Application Programming Interface* provides information on the structure and functionality of the NMS database and the way it implements a model of the network's components and their relationships.

- The *NetWare GUI Tools Programmer's Reference Guide* describes the NMS GUI tools that are used to create buttons, gauges, graphs, legends, and so on. The *NetWare Graphical User Interface Style Guide* shows developers how to ensure that an application interface is consistent with the NMS interface's look and feel.

- *The SNMP Data Server Programmer's Reference Guide* provides information about the SNMP Data Server, which is a background Windows application that uses DDE to provide services.

Beyond the Horizon

Developers are still testing the limits of the NMS platform. Being able to port virtually any SNMP application to this management platform extends its potential far beyond the traditional network device domain. One of the most unique NMS snap-ins to date is Lancert Technologies' Lancert Facilities Manager: If you want your console to notify the facilities manager that the air conditioning has gone out in Building 4, or beep the head of your security staff the next time a security door or storage cabinet is opened, this is the product for you. As you extend the capabilities of the NMS platform, you may find that you can monitor not only a vast array of data communications equipment but the computer room's air conditioning and access as well.

Anyone want to develop a snap-in to manage my Internet Toaster? □

Roger Spicer is a senior partner with Technology Consortium, and he cowrote the Novell NMS NetWare Expert Tutorial *and* LANalyzer for Windows NetWare Expert.