Back to Basics

Finally, an easily installed and configured network monitoring application that delivers.

BY IAN BROWN

good
- ■ Easy to install and configure
- ■ Backup server functionality that's easy to implement
- ■ Good user and device audit-logging capabilities

bad
- ■ No regular synchronization of live and backup servers
- ■ No user-group support
- ■ No Web-based front end

Network-management applications range from simple monitors to root-cause analysis machines that do everything but tell you who made the coffee. Castle Rock Computing's SNMPc exemplifies what a simple monitor should deliver.

Castle Rock has been making network monitoring and management products since 1987, and SNMPc was one of the first SNMP managers for Windows. Version 7.0 comes in two flavors: Workgroup and Enterprise. New to this version are disaster-recovery support over a redundant backup server (an unusually advanced feature for an inexpensive product); simple user security features, including accounting and auditing; customized TCP service polling; and map-edit tracking. Version 7.0 also has improved management of event-action filters and event-viewing criteria.

I installed the Enterprise version on a Windows 2000 server with 600-MHz dual processors and 512 MB of RAM at our Syracuse University Real-World Labs®. After logging on to the management console, I ran discoveries of two network subnets with 200 devices to populate the network map. SNMPc took a little time to discover all the devices—including a variety of Cisco Systems, Hewlett-Packard, SMC and 3Com machines—but this is understandable, considering the size of the network.

Back Up, Jack
To test the redundant backup server, I installed the software on a server similar to my primary server. The setup was easy—I input the IP addresses of both servers as a configuration option, enabled the backup service option and disabled active polling on the backup server.

I then took my primary server offline. Using the default configuration settings, my backup server sensed that the primary server was down and took over polling operations in less than two minutes. All of my settings were intact, including user information, device settings and configuration options. Remote polling agents that were connected to the primary
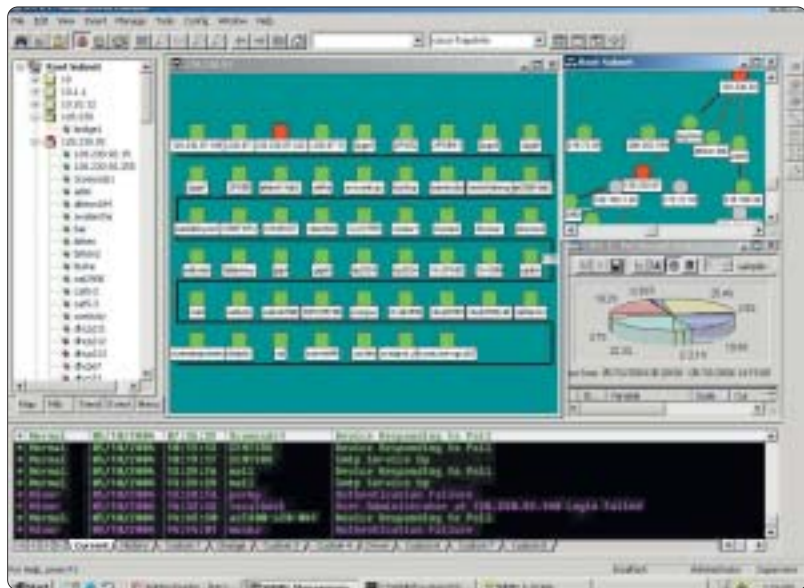
Administration features in SNMPc's Explorer-like interface include a variety of views. Among these are map, MIB, trend, event and menu.

server hooked up with the backup server automatically, so I didn't lose any polling statistics or uptime data.

The only negative: The backup and export of the database files from the primary server occur automatically only once a day, and you can't configure it for more frequent intervals. Therefore, you have to back up the server manually whenever you make major changes to the system configuration.

The View From There

SNMPc uses an Explorer like interface to display its operations. In the default view, the console window is split into three panels, which show all operations. The left panel contains five tabs: map, MIB, trend, event and menu. The map tab lists the discovered devices, sorted by

> **Just need a simple network monitor? Castle Rock Computing's newest SNMPc sets the standard.**

subnet. The MIB tab displays a MIB browser that lets you view information for a selected device and shows private MIBs from device manufacturers.

From the trend tab, you can design trending reports that collect data from devices over time. You build reports by selecting common variables from a drop-down menu, such as interface usage (in bits per second) and interface utilization (expressed as percentages). I built several reports with just a few mouse clicks and, after waiting a short period for data collection, viewed my reports on-screen.

The event tab lets you set alarms and specify how admins should be alerted. To test the alarm, I put one of my Web servers on Port 8080, rather than the standard port, and

created a customized TCP port service for polling the server using SNMPc. I configured an event condition to notify me with an on-screen alarm and a WAV sound if the monitored port on the server went down. I then stopped the Web service manually. SNMPc used its customized port polling to notify me that the service was down.

The lower section of the console window is the event log-alarm panel. From here you can configure up to eight custom log views that filter for specific objects and/or their status. The logs display all the alarms and polling log messages generated by the application, including tab views for current and historical events. I created a filter for all devices that had a critical-red alarm and saw all the devices in that status. I also created a filter for my mail server, which let me view historical data on the server—both the server status and the status of the SMTP service being monitored.

The main panel in the center of the console window shows the graphical device maps and generated reports, graphs and charts. Clicking on a subnet icon brings up a new window, which displays all the discovered devices, each color-coded by status, and a small indicator showing if the device was discovered using SNMP or ICMP polling—regular features associated with any good network-monitoring system.

Access Control

Adding and configuring users in SNMPc is a breeze. There are three user security levels: supervisor, observer and operator. Supervisors have full control over all software functions; operators and observers can be restricted to viewing or editing specific subnets and reports. I set up several users and defined access to a specific subnet and group of reports for each user. Unfortunately, you can't group users—you must set

up permissions for each individually.

New to this release of SNMPc is a password-expiration feature.

> **Clicking on a subnet icon brings up a new window that displays all the discovered devices.**

However, you can't set a specific expiration date for each user—there is only a global setting for all users.

The software doesn't have a Web-based front end, though Castle Rock says this feature will be released later this year. I accessed SNMPc remotely through a console application and a Java console. Both were easy to install and configure, but by default only one session is allowed with the remote console. For multiple remote-console sessions or to use the Java console, you need a remote-access extension license.

The user configuration can disable the remote administrator login as a security measure. This worked fine when using the remote console, but access was allowed from the Java console, which can only be restricted by IP address. This isn't a major problem, because only the remote console has the full functionality of the local console—the Java console has only read access.

SNMPc is on the right track, adding useful features for monitoring and trending networks. And the price is attractive for organizations with small IT budgets.

■ **SNMPc 7.0,** $995 to $5,645. Castle Rock Computing, (408) 366-6540. *www.castlerock.com*

Ian Brown is a network consultant at Syracuse University. He has worked in network and systems administration. Write to him at ibrown@nwc.com.