Automated Status Notification System

NASA Lewis Research Center's Automated Status Notification System (ASNS) was born out of need. To prevent "hacker attacks," Lewis' telephone system needed to monitor communications activities 24 hr a day, 7 days a week. With decreasing staff resources, this continuous monitoring had to be automated. By utilizing existing communications hardware, a UNIX workstation, and NAWK (a pattern scanning and processing language), we implemented a continuous monitoring system. The system is based on statistical analysis of our telephone call records (about 18 months worth), comprising mean call levels (traffic patterns) based on calls per time of day, calls per day of the week, and type of calls--Federal Telephone Service (FTS), Direct Out Dial, and Direct Inward Dialed calls. From these statistics, we programmed thresholds for alert levels into the system software.

Now that this ad hoc tool monitors our telephone activity, if telephone traffic in the Fujitsu 9600 exceeds the call traffic threshold set in the monitoring program, pocket pagers are called and special codes are sent that indicate the type of traffic and the number of calls exceeding the threshold. If the person who receives the page deems it necessary, they have a response team investigate the anomaly, and if warranted, they shut down the calling path.

ASNS runs 24 hr a day, 7 days a week, and it reports every hour that the threshold for the previous hour is exceeded. Thus, we know, in real time, what our telephones systems are doing, and we can react as necessary.

We have extended the same concept to our data networks. We currently monitor 15 critical network devices on a 24-hr, 7-day basis. Every 5 min, each device is queried; if less than 90 percent of the packets are transmitted, a pager notification is sent and logged. Since we developed this process, other devices that do similar types of monitoring have become commercially available.

Resources Needed for ASNS

- Access to a Unix workstation attached to the network
- Minimal programming and statistical knowledge of normal operations
- Dial-out capabilities (pagers and modems)
- Pocket pager (can be local or nationwide)

Applications of ASNS

- Continuous monitoring of voice and data networks
- Alerting during nonworking hours of significant events pertaining to the health of networks

- Automated repair calls during nonworking hours
- Greater visibility of high-profile resources
- Continuous monitoring of subsystems attached to networks
- High-profile monitoring of network devices undergoing upgrades and repairs
- SNMP (Simple Network Management Protocol) E-mail alerts of significant network connectivity events or loss of connectivity
- 24-hr, 7-day notification of hacker attempts on voice mail and telephone systems
- Facility and environmental monitoring (using some additional PC cards)
- Intrusion alerting and security for network communications rooms.