AN INTEGRATED NETWORK MANAGEMENT SYSTEM FOR CABLE TELEVISION

John C. Anderson, P. Eng.
Rogers Engineering

Abstract

The Integrated Network Management System (INMS) uses computer technology to monitor and control all of the equipment in Rogers primary fiber hubs, secondary fiber hubs; and trunk amplifiers and power supplies in the coaxial cable TV system. In the event of a fiber cut, or optical hardware failure, a backup route or redundant hardware automatically switches in to restore service. The INMS system monitors all of this equipment and reports any fault conditions that occur to a central Technical Action Center (TAC). Through different security access levels, all users can monitor the network, but designated technicians have the ability to issue switching or reconfiguration commands. INMS is unique in that it provides a single graphical interface to the outside plant with a consistent representation of several different vendors' equipment laid out in a logical network presentation. Rogers has developed software that integrates the proprietary communications protocols of various vendors into one system of centralized network management. The operator now has a comprehensive view of the entire network status at any time, providing more effective problem isolation and resolution. This system is providing real gains in network operation efficiency and customer service.

Background

The past several years have witnessed dramatic changes in cable television network architectures. These changes have been driven by the need for improved signal quality, better reliability and expanded bandwidth. The local headends that formerly served a community are being replaced by regional headends that serve multiple primary and secondary fiber optic hub sites. These regional headends provide economies of scale for signal reception, processing, routing, and scrambling. However, with the use of digital or FM fiber optic backbone systems, the local fiber hubs are in essence small headends that receive the fiber signal and remodulate onto VSB-AM systems for either coaxial or further fiber distribution. The large tree-and-branch coaxial networks are also evolving rapidly into fiber-rich networks with much smaller serving areas off the fiber feeds. Some architectures are now calling for 500 to 2000 home nodes served by each fiber. Fiber optic receivers are being placed in large numbers throughout the distribution network.

With this network evolution we are also seeing a proliferation of new components in the network, such as fiber secondary hubs and optical bridgers. Future changes as part of the full service network such as DVC, video-on-demand, and high speed data services will only

add to the number and complexity of the installed equipment base.

Fiber optic systems have brought new vendors into the cable TV marketplace and traditional vendors have increased the range of their products. However, it is extremely rare to find a cable TV system built with a single vendor's hardware. In most cases, a network consists of hardware from numerous vendors and of varying vintage. Unlike the telecom environment, many cable TV manufacturers and suppliers have either not addressed network management issues at all, or the solutions that they offer are proprietary and only apply to their particular hardware. These stand-alone systems do not communicate with one another to rationalize alarms, create trouble tickets and outage reports, or interface to other operations support systems. Network management protocol standards and interoperability are virtually nonexistent in the cable TV industry. The result is a mix of various computer systems from different vendors each interfacing with a particular type of hardware. These single-vendor systems focus on technology control, rather than the end-to-end process of delivering signals reliably to the customer. Consequently, the system operator must deal with an array of independent computer systems and an astute operator must interpret the cause of alarm conditions.

With all of the activity in fiber optic and full service network deployment, the ongoing operational implications have received very little attention. Part of Rogers Cable TV fiber optic and customer service strategies was the recognized need for an automated network management system to aid in the operation and maintenance of this growing base of network equipment. Without some form of automation, there would be a severe strain on staff skill levels and overall manpower requirements.

Network Management System Requirements

A Network Management System is a tool to co-ordinate, monitor and control the distributed hardware resources throughout a network. To be fully effective, the network management system requires cohesive interaction between the human operators, the software applications and the network hardware elements.

Rogers had a number of key requirements for an integrated network management system:

1. The system must integrate the various stand-alone systems into one so that an operations technician could view the network on one computer screen as a system, rather than a series of disjointed devices. The graphical presentation of multiple devices at multiple locations to multiple end-user workstations must be in a consistent format.

2. The system must be able to handle various device protocols, no matter how proprietary or standardized, complex or simple they might be.

3. The system must be flexible in configuration to handle multiple users logged on simultaneously, both from a central location and distributed throughout the operating divisions.

4. The system must be very user-friendly, providing automatic updates to operations technicians and allowing them to concentrate on solving problems rather than operating the network management system.

5. The system must be justified financially in operating efficiency improvements and better customer service.

6. The system must use off-the-shelf components, with low cost points-of-presence and have a linear growth cost.

7. The system must have several levels of security that could be partitioned either geographically or by equipment type, to prevent unauthorized access to the system.

Rogers Integrated Network Management System

A network management project team from Rogers spent over a year researching various systems that were in the marketplace. Almost all of these proved inadequate for the requirements identified. Most operated on high-end expensive workstations, and, with software, a total solution was in the order of several hundred thousand dollars. Most of these solutions only supported telecom and LAN/WAN protocol standards. Very few systems could handle simple monitoring such as voltages or contact closures, and many had limits as to the number of devices they could handle. A number of systems were simply "managers of managers" that brought proprietary vendors' systems together on one screen but didn't really integrate the alarm and database functions.

Consequently, Rogers assembled a team of software developers and began to develop an Integrated Network Management System. "Off-the-shelf" components were sourced which included both hardware and software tool kits. All workstations and hub site communication servers (c-servers) were to be 386 or 486 type PCs with standard interface cards installed. Hewlett-Packard's Openview software adapted best to Rogers' applications. Although originally designed for WAN/LAN monitoring, this software tool kit allowed for user customization. The various workstations and c-servers would communicate via a Novell LAN interconnection, since this technology was already in place for Rogers office LAN systems.

Technical Overview

INMS is a highly distributed system; it uses 386 and 486 type PCs interconnected using any standard Local Area Network (LAN) technology for both hub site servers and local workstations. The distribution of processes allows for system modularity, and flexibility while the adherence to existing standards offers a solid base for future growth.

A number of INMS system software modules, or processes, cooperate to manage the wide variety of information packets present in the system at any one time. These processes include message routing, database access, security,

status management, and system testing. Security is active on all users, network devices, c-servers, message packets and LAN activity. INMS information is not accessible to a given user without approval from the security process. The status management process is responsible for maintaining a current snap-shot of the network that rapidly issues updated alarms to work stations using INMS. Without this process, it would take an inordinately long time to log onto the network and get updated on the status of all devices. The distribution of processing provides INMS with a linear growth path, with no practical upper limit concerning number of users, locations or devices.

Each hub site has a communication server (c-server) connected to the INMS backbone using a variety of async, sync, X.25 or T1 bridge hardware. An INMS workstation can be collocated with the c-server at a hub site for local monitoring and control of devices by field staff. Each c-server typically supports up to thirty-two physical ports, with each port supporting an individual vendor's protocol (both proprietary and non-proprietary). The c-server acts like a network management multiplexer and translator, combining a number of proprietary sources into a single INMS communication port. Under typical operation, the c-server either polls devices cyclically for a change of state, or is interrupted by one of the managed devices when a change of state occurs. This initiates an event within the c-server that takes the proprietary source and converts it to a standardized INMS message. Once converted, the c-server packages the event message within an envelope and issues a datagram to the status manager for alarm filtering. The status manager compares the datagram to see if its contents result in a change-of-state of the current network image. If a change of state has occurred, the status manager issues an event to all workstations registered (via security) to access this information.

The INMS user workstation uses both graphics and text to represent the current state of the managed network or devices within its access. The system design ensures that monitoring and control procedures are similar for a wide range of devices, even though the underlying protocols or technologies are vastly different. This ability allows even junior TAC staff to function as seasoned professionals. The end user workstations of INMS are typically 80486 based computers, equipped with super-VGA, high resolution monitors, a mouse and 4 MB of RAM. A company LAN connection is the only requirement for a workstation location. INMS is accessible (with security limitations) to everyone within the company from technicians, to supervisors, to executives. The workstation presents the user with a simple graphical (Windows-based) representation of all networks and facilities, plus access to the textual database, trouble ticket, e-mail and login screens.

INMS uses a series of "layered" screen displays to graphically illustrate the network topology and status. Each layer presents a set of icons that provide access to different successive layers containing more detail. The color of the icon indicates the status of the underlying devices: red indicates an alarm, yellow a warning, green is OK, blue indicates the device is out of service, purple indicates a disabled

alarm. Using a mouse, a user can "drill down" through several layers of detail to isolate the cause of an alarm or to check the status of a particular device. After the appropriate log-in procedure, the opening screen is that shown in Figure 1, the Ontario Inter-city Fiber Optic Network. A mouse click on Toronto, for example, takes the user to the local Toronto fiber network, Figure 2, which shows the primary fiber hubs. A mouse click on the Sheppard hub takes the user to the display of the fiber detail screen, Figure 3. The user can then drill-down further to the equipment detail on each fiber. Figure 4 shows the optical equipment on fiber block A. At the equipment level screen, the user can interrogate each device and retrieve real-time status of all measurable parameters. For example, Figure 5 shows the secondary optical receiver status for Block A. Remote video monitoring via a tunable demodulator and signal restoration controls are available using the screen in Figure 6. Similar navigational steps take the user down into secondary hubs and out into the coaxial trunk network, Figure 7. Figure 8 illustrates the interrogation of individual trunk amplifier parameters. Standby power supplies are monitored and controlled in a similar fashion. The entire layered display system is analogous to an inverted tree that allows the user to navigate across and into the network through thousands of possible paths easily and logically.

Every physical component of INMS is off-the-shelf, multi-vendor, multi-source equipment. Manufacturer independence allows the implementation of INMS at the lowest competitive price, and provides multiple sources for backup or emergency purchase.

On high priority links, INMS typically operates as an "out-of-band" management system. Out-of-band means that the network management information data traffic is transported external to the network being monitored. On links with lower priority, the carriage of INMS data traffic is on the network, with dial-up redundancy available in case of total network failure. Small fiber repeater sites, that do not warrant a full c-server installation, communicate via automatic dial-in and dial-out access.

Operational Results

Rogers has implemented INMS in all of its operating divisions interconnected with fiber. INMS has few limitations on what devices can be monitored or controlled. It is being used for Rogers Cablesystems fiber distribution network including digital, AM, and FM fiber links. In each primary fiber hub INMS provides control of agile modulators and demodulators; and video and RF switches. Using INMS, redundancy equipment and procedures are in place to deal with entire fiber cable cuts, loss of individual fibers or associated equipment, or the loss of an individual output channel. In any of these events, signal restoration occurs in seconds rather than hours. INMS is expanding to secondary fiber hubs as they are installed, to provide monitoring of optical transmitter and receiver status, and control of redundant path switching. Approximately 4000, or one third, of the company's trunk amplifiers are now on-line with INMS, with the remainder scheduled for the balance of the year.

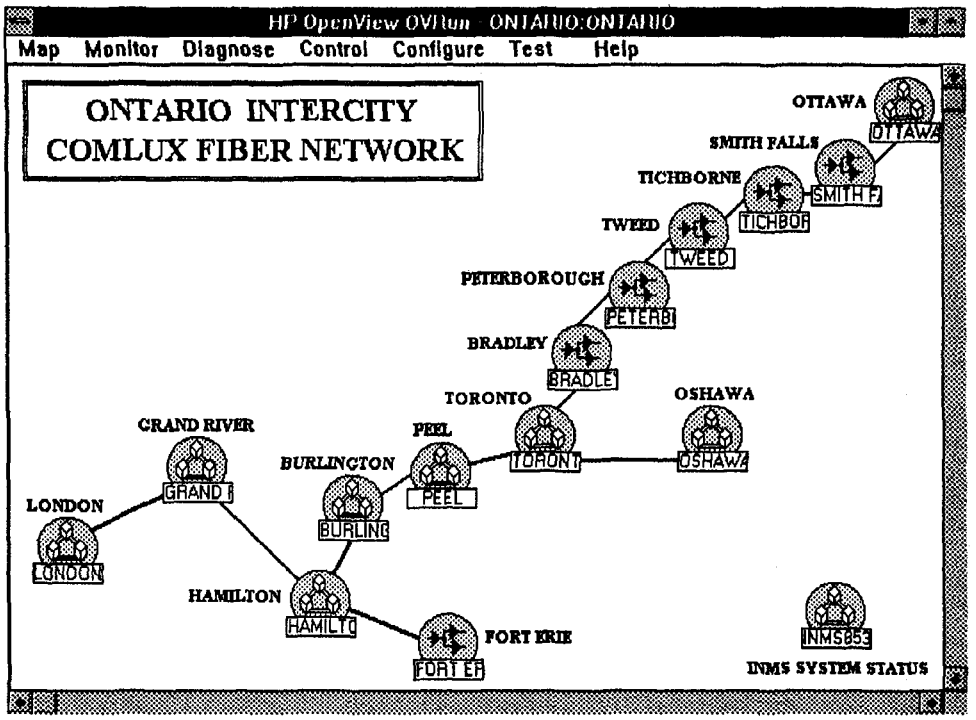

Figure 1
Ontario Inter-city Fiber Optic Network

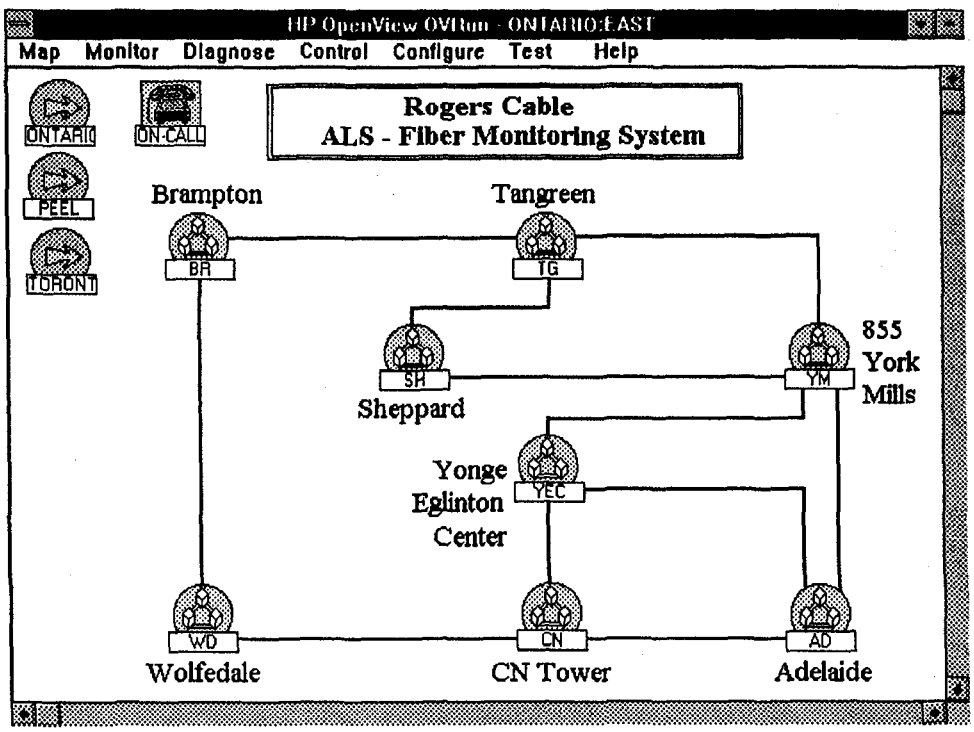

Figure 2
Toronto Primary Hubs

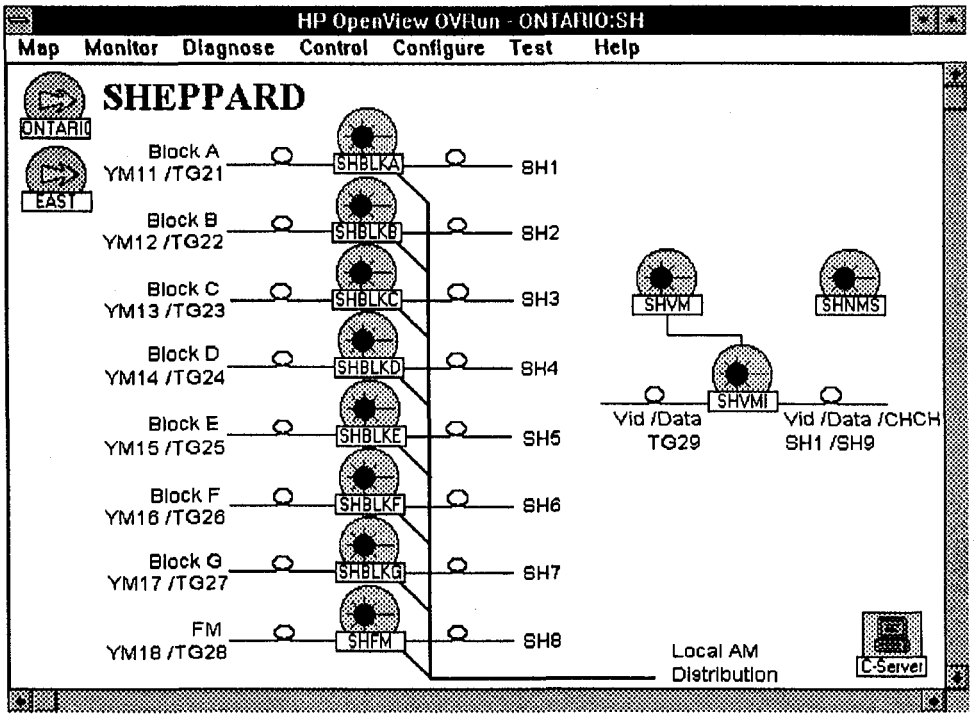

Figure 3
Sheppard Hub Fiber Detail

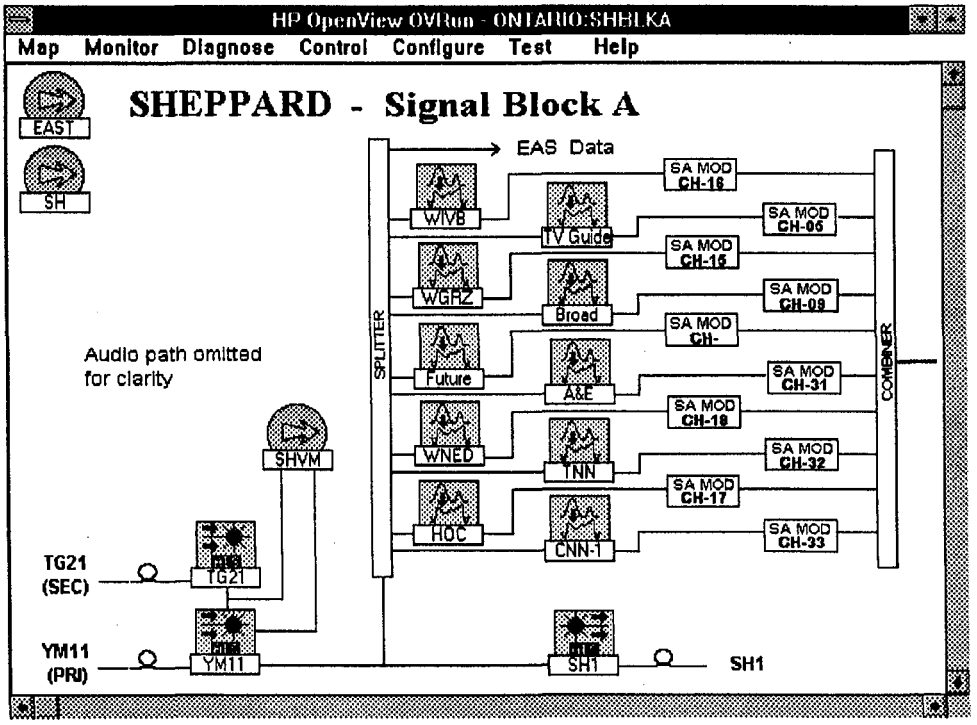

Figure 4
Fiber Block Equipment Detail

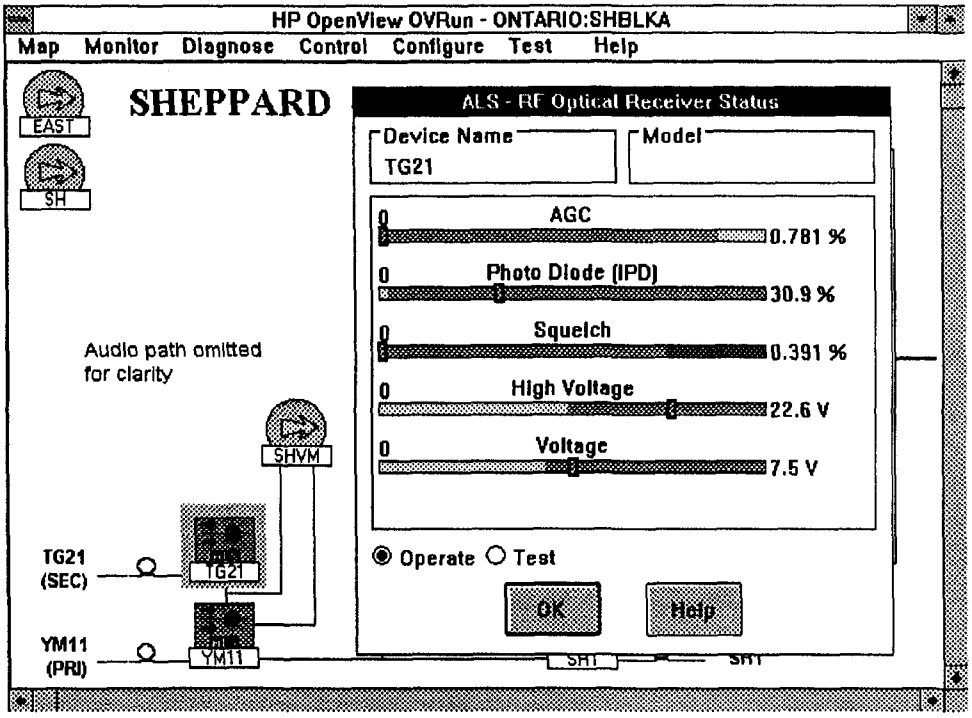

Figure 5
Optical Receiver Status

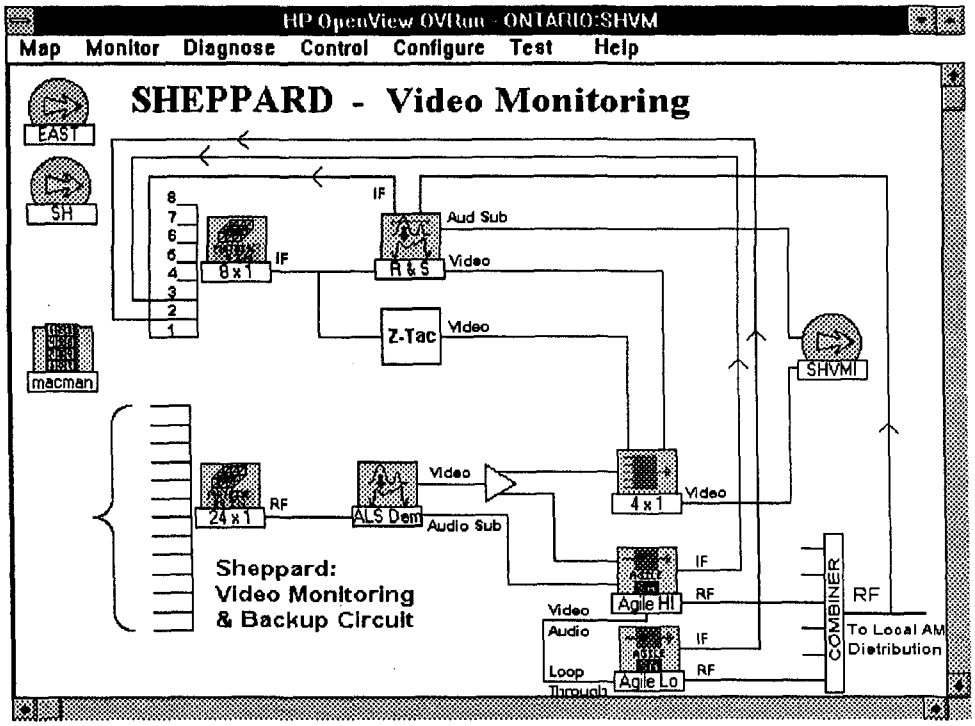

Figure 6
Video Monitoring and Backup Switching

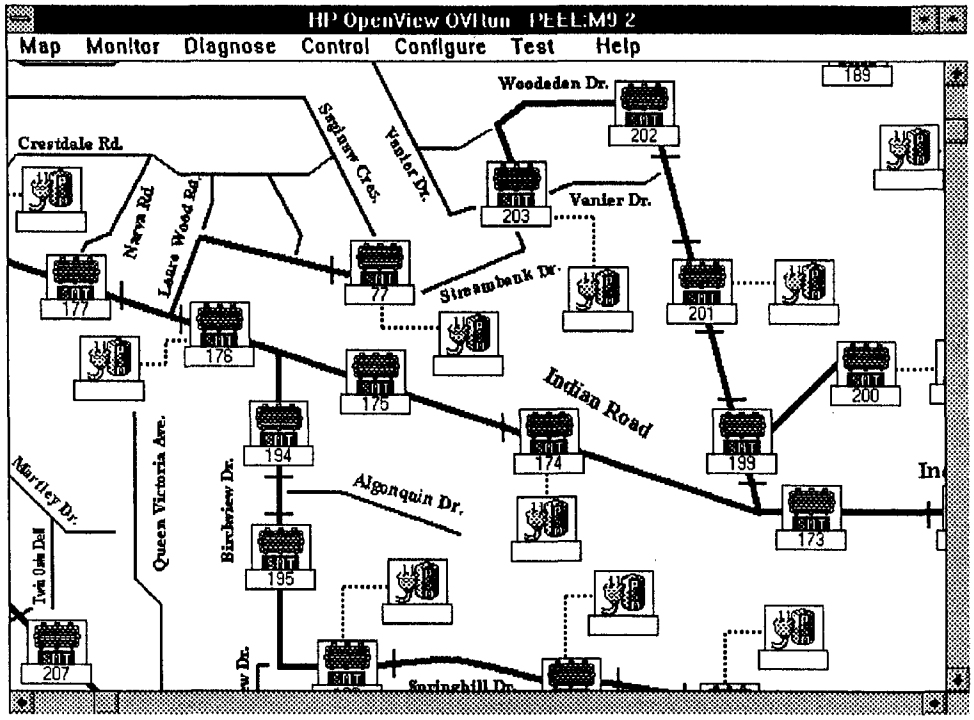

Figure 7
Typical Coaxial Plant Screen

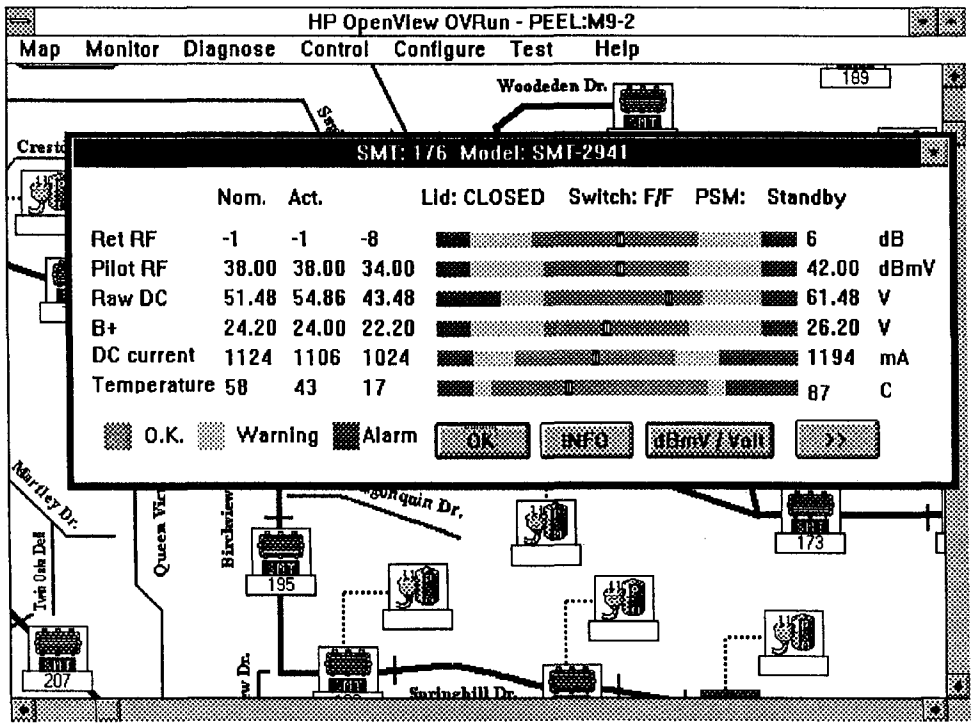

Figure 8
Amplifier Status Window

Using INMS, a technician, manager, or executive can graphically review the status of the network, its components and relationships. The network status can be viewed either globally, by city, by hub site or by equipment type. Real-time alarm conditions can be reacted to remotely without the sometimes unnecessary dispatch of technical staff. Should the Technical Access Center (TAC) operator feel that a problem requires hands-on attention, a technician can be dispatched using the INMS Trouble Ticket System. Color-coded icons represent all components in the overall network within a geographical display. All control functions use a consistent style across all vendor's equipment. Full auditing and security levels ensure that only authorized users are able to control devices specifically assigned to them.

On-call technicians have access to INMS from home using dial-up facilities and a laptop PC. In many situations, they can take corrective action even before leaving home. During the day, certain field technicians can access INMS from their vehicles using cellular dial-up facilities.

INMS monitors a number of hub site environment conditions such as temperature, primary AC power, standby generator power, fire and smoke alarms, etc. This provides an early warning of potentially major problems.

Each hub site has a current "on-call" technician list icon attached to it listing various phone numbers . The TAC center operator can quickly establish who to call and how best to reach them depending upon the nature of the problem.

Each alarm is time stamped and logged in the INMS database. Report writer software facilitates ad-hoc and regular reports that sort and provide statistics on alarms by site, by type of equipment, by date, etc. This functionality provides management with the tools to analyze the effectiveness of network operations.

Future Directions

Rogers Cable TV currently operates with three main operations support systems: the customer database and billing system (Supersystem), the Integrated Network Management System, and the automated mapping and facilities management (AM/FM) system. These three "islands" of technology currently cannot be linked electronically but yet they support three independent databases with overlapping functionality. The long-range goal of Rogers Cable TV is to provide an integrated customer service system that would link these three systems together into a comprehensive operations support system. For example, it would be desirable to relate an equipment alarm on INMS to the affected addresses on the AM/FM system, and then relate these addresses to subscriber accounts on Supersystem. A technical service representative (or perhaps even a voice response unit (VRU)) would have up-to-the-minute information on the technical status of each subscriber when they phone in. The municipal base map on the AM/FM system would contain information such as demographics of subscribers, property information, zoning information and building types. The AM /FM system would be able to sort and correlate information that is now either not available or which must be assembled manually, such as address

lists of subscribers fed from specific hubs or equipment, inventories and repair histories of installed equipment, subscriber bandwidths, support structure rental detail for billing reconciliation, etc. After linkage, these three core systems would then feed off into computer-aided dispatch systems, GPS systems for vehicle tracking and radiation patrol, and automated work management systems.

Recommendations

Cable television operators are facing numerous challenges with the deployment of new technologies and network architectures, the introduction of new services, new and vigorous competition in the video marketplace, along with pressures from both customers and regulators for better service and reduced costs. It is imperative that operating efficiencies be applied in order to meet these challenges. Network management is one of these efficiencies.

However, the CATV industry is also facing a number of obstacles to the implementation of integrated network management. A lack of industry standards and a proliferation of proprietary vendor solutions has made the task of integrating network management solutions very difficult. The CATV industry must come together and agree on standard protocols or application programming interfaces in order to make integrated network management easier to implement. Vendors seem to be reluctant to offer software solutions either because they add cost to their product, or they are not willing to invest in software development.

Much of the CATV plant hardware in place today is not equipped for network management. The industry needs to start addressing the need for more intelligent devices in the network. Higher levels of functionality are feasible through the use of imbedded microprocessor technology. Some estimates claim that less than 10% of the CATV coaxial plant in the U.S. is active two-way. Most recently, coaxial rebuilds and fiber optic plant are being built two-way active. These are prime areas for immediate deployment of network management technology. New video-on-demand and high speed data services, and network technologies such as SONET fiber rings and ATM will change the single "physical" network connection to the customer to a "logical" connection with "virtual" channels. Network management will be an essential tool in managing these more complex networks in the future.

Acknowledgments

I would like to pay tribute to the talented software developers at Rogers Engineering who have done the "impossible" with INMS.