Preface

Our industry has made significant advances in supporting both advanced network topologies and interconnected networks during the past several years. The traditional star networks are rapidly evolving into distributed amalgamations of subnetworks built on different networking technologies and often supplied by multiple vendors. Ownership and management of these networks may span organizational boundaries. A network might include, for example, the autonomous divisions of governmental or corporate organizations, a company, its customers, and the vendors serving the company, or perhaps a group of loosely affiliated educational institutions. The task of effectively managing such networks has become increasingly complex.

Although the evolution from star configurations to single workstations and interconnected networks does bring convenience and economies, this progression eliminates the security afforded by the redundancy of separate networks, and makes the task of network management more critical. Network management is the theme of the first four papers in this issue.

The paper by Rose and Munn reviews the evolution of network management and examines its categories of *problem* management, *change* management, *configuration* management, and *performance* and *accounting* management. The authors discuss the impact of voice and data integration, local-area networks, and multivendor environments on network management requirements.

Central to providing network problem identification, isolation, and resolution are the capture and display of details of network component failures. Using standardized message formats, the SNA Alert mechanism provides products in an SNA network with the means to effectively communicate problem notification to a network operator. The paper by Moore additionally provides a description of the Alert process as well as the composition of the Alert messages and their subsequent display using the NetView™ program.

Capturing network management data for processing by the NetView system can be substantially facilitated by use of the IBM NetView/PC™ program offering. The paper by Ahmadi, Chou, and Gafka describes how an appropriately configured IBM PC can be used to permit non-SNA devices to pass network management data to an SNA host. These data, for example, may be Alert notifications, or perhaps call detail information for a Computerized Branch Exchange. Additionally, in a network without a NetView host, the NetView/PC product can serve as a network focal point by recognizing and displaying Alerts and by further supporting the problem management process.

The last paper of the set on network management describes the NetView program product. This paper, by Kanyuh, describes the evolution of the NetView program and its major components, including a command facility and session, hardware, and monitoring components.

IBM has separately published these network management architectures, along with the application programming interfaces for the NetView program. This facilitates the full participation of non-IBM devices and programs in the network management process. It is apparent that these products will continue to grow and evolve as the requirements of network management develop.

Supporting the needs for information access for a functionally and geographically diverse user base requires thoughtful planning. With an architecture in place, the systems decisions necessary for strategic and tactical actions can be made with more surety and speed. The paper by Devlin and Murphy describes such an architecture developed for the IBM Europe/Middle East/Africa organization. Based on relational database technology, EBIS consists of seven distinct components to store, update, secure, locate, transform, distribute, and present data. Its design allows intelligent workstations to access and present information from multiple sources.

Gary Gershon
Editor