SNA network management directions

by D. B. Rose
J. E. Munn

Network management is the process of monitoring and controlling the components of a communication-oriented network of information systems in the areas of configuration management, operational control, problem management, change management, and performance and accounting management. This paper discusses the evolution of the SNA network management architecture and products that implement that architecture, and describes their likely future direction.

History and trends

SNA network management architecture is embodied in the management services components of SNA.[1] Management services functions are represented in the architecture by management services components in the control point, in the physical unit (PU),[2] and in the individual layers of SNA. Network management architecture in this paper refers to these SNA management services.

As SNA has evolved since its introduction in 1974,[3,4] network management has played an increasingly important role. At SNA's inception, SNA networks were relatively simple, with a single host and a tree network. Today, SNA networks may contain multiple hosts, tens of thousands of terminals, interconnected but independently administered networks, small-system subnetworks, and Local-Area Networks (LANs). Today's networks also include a diversity of customer-owned and -managed terminal and switching equipment, the potential for multiple carriers' involvement in a single link connection, and new technologies.

Network management architecture has evolved with the connectivity enhancements provided by SNA. The beginnings of SNA network management architecture in 1979 were driven largely by requirements from the IBM service organization, with the introduction of multiple-host SNA networks. Today this network management architecture is increasingly being driven by customer requirements resulting from the increased skill levels and costs involved in managing larger and more complex networks. These customer requirements, along with service-driven requirements, are being closely monitored as the evolution of network management architecture continues.

The network management products of IBM are also evolving at an accelerated pace to meet increasing network management needs. IBM announced a number of network management products in the late 1970s and early 1980s. Network Problem Determination Application, Network Communication Control Facility, and Network Logical Data Manager performed such specialized tasks as problem determination for hardware and logical entities.

By the mid-1980s, the need was recognized to combine the functions of these network management products into one overall network management product strategy. The result was the 1986 announcement of NetView,™ NetView/PC,™[5] and Open Communication Architectures as the basis for satisfying

that need. The NetView product combines and enhances the functions of three network management program products and includes functions from two other program offerings. This combination benefits the customer by providing a consistent operator interface to these functions and by simplifying the installation process, because only a single product need be installed.

As the complexity of network configurations increases, the criticality of maintaining high system availability increases accordingly.

In June of 1987, additional NetView capabilities were announced, including functions for automated and remote operations management, and support for *generic Alerts* that enhance IBM's open network management. Generic Alerts provide generic code points for descriptions of Alerts, probable causes, and recommended actions, thereby making NetView's processing of Alerts independent of the product sending the Alert.[6]

The continued evolution of SNA network management architecture and the products that implement it can be expected to build upon this network management base.

Network management categories

Network management covers many functions that are necessary to manage a communication network. SNA network management comprises the following major categories:

- Problem management—the function of dealing with a problem from its detection through its resolution. The steps of problem management are (1) determination, (2) diagnosis, (3) bypass and recovery, (4) resolution, and (5) tracking and control.
- Change management—the planning, control, and application of changes (additions, deletions, and modifications) to the resources of a network.
- Configuration management—the facilities and processes necessary to plan, develop, operate, and maintain an inventory of information system resources, attributes, and relationships.
- Performance and accounting management—the process of quantifying, measuring, reporting, and controlling the usage, responsiveness, availability, and cost of a network.

Each of the major categories of network management provides operations and security management. Operations management deals with the facilities and processes to support remote operations and automated operations. Security management is the control of access and authority to use network resources. New requirements in each of these network management categories are discussed in the following sections.

Problem management

As the complexity of network configurations increases, the criticality of maintaining high system availability through expedient problem resolution increases accordingly. Problem management is the process through which high system availability is achieved. Problem management involves problem determination, problem diagnosis, problem bypass and recovery, problem resolution, and problem tracking and control. The requirements that are understood for each of these steps are the following:

- *Problem determination* is the detection of the loss or impending loss of availability of a system resource to an end user, and the isolation of the detected problem to the failing hardware, software, or microcode component.
- *Problem diagnosis* is the determination of the specific cause of a problem and the action required to resolve it. Diagnostic data gathered during problem determination provide input to this step. It may be necessary to gather and analyze additional information to complete problem diagnosis.
- *Problem bypass and recovery* is the bypass of a failure, if necessary, until a problem can be resolved. The decision to bypass a failure is determined by the criticality of the lost resource and the cost of providing the bypass capability. If continuous (24-hour) operation is a requirement, recovery from a problem must take place immediately following problem determination and di-

agnosis. Bypass and recovery procedures should be automated whenever possible.

- *Problem resolution* is the action taken to correct a problem. Once a problem is resolved, any steps taken in bypassing it may be undone and the original resources placed back in service.
- *Problem tracking and control* is the tracking of problems from detection until their final resolution. Many different symptoms may result from the same problem, and different problems may be related. The tracking of problems allows the correlation of related symptoms and problems and helps to ensure timely recovery.

The first network management products, introduced in 1979, helped the network operator perform problem determination. Initially, statistics were kept at each node and collected by a host computer. A person with access to the host could analyze the statistics and attempt to diagnose problems in the network.

Each SNA node is responsible for its own error analysis to determine whether a problem exists and whether local recovery action can be performed.

Today, each SNA node is responsible for its own error analysis to determine whether a problem exists and whether local recovery action can be performed. If a problem exists that cannot be resolved locally, the node sends an architected Alert signal to the NetView program to indicate that a component in the network is unavailable and that intervention is required. The architected Alert signal allows immediate notification of problems in the network so as to foster quick and easy problem resolution. Many devices monitor hardware and line interfaces and send Alerts to the NetView product.

Today, many devices also provide diagnostic capability, and a number of features are currently available in SNA to provide bypass and recovery. These include the pause and retry logic in Synchronous Data Link Control (SDLC), which allows SDLC links to remain operational across periods of transient error on the links, and the ability to configure multiple predefined routes, so that if the route serving a session fails, that session can be re-established over an alternate route.

In June of 1987, generic Alerts were announced as an enhancement to the SNA Network Management Architecture and to the NetView product offering. By defining generic code points for the Alert description, probable causes, and recommended actions, the generic Alert architecture provides for the consistent definition, reporting, and presentation of problems. NetView's processing of Alerts can now be independent of the product sending the Alert. Generic Alerts facilitate the integration of non-SNA products into IBM's open network management and provide a well-structured format that lends itself readily to automated processing. In addition to the hardware and communications errors currently being reported, recognized requirements for the generic Alert architecture include the definition of generic code points for the reporting of software and microcode errors.

Additionally, problem management includes the following recognized requirements:

- Extension of functions to small-system networks and to a wider range of devices
- Provision for problem correlation when Alerts are received from both endpoints of a peer-to-peer connection or when multiple points in the network report related problems
- Enhancement of bypass and recovery facilities to perform route switching, without disrupting the sessions, should a route fail
- Extension of problem-reporting mechanisms to include notifications to enhance problem-tracking capabilities, such as notification of repair actions started and notification of resources back in service

We are working toward providing network management architecture and product enhancements to address emerging requirements such as these and to continue to extend the support of problem management functions across all environments to provide full end-to-end network management.

Change management

Changes are constantly occurring in today's complex networks. Such changes are driven by many events, including network configuration changes resulting from changes or additions to network components or communication facilities, or new releases of programming systems, new applications, fixes resulting from problem management actions, or perhaps other unforeseen events. The change process itself can introduce new problems to the network, and must be managed carefully to minimize the risk of network disruption.

A need for more sophisticated change management strategies has emerged as networks have increased in size and complexity. Increasingly there is a need for change management strategies that incorporate such requirements as electronic change distribution, unattended change installation, and nondisruptive change installation. The diversity of networks (applications, sizes, geographical dispersion, complexity, etc.) dictates that a number of change management strategies be available to network owners. Change management strategies must be supported that allow change management from a central site, distributed sites, or at each physical site. The level of allowable network disruption for changes also varies according to the network application, and change management strategies must support the required level of availability. Whatever change management strategy is adopted, well-defined management of the change process is imperative if a reliable network is to be maintained.

The change process involves *planning, distributing, installing*, and *tracking* of changes as follows:

- *Planning* results in a plan that defines the steps in the change installation process. This plan should be executable so as to automatically distribute, remotely install, and track the installation of the changes. The change planning process also requires information regarding the current levels of hardware (including microcode) and software for network components, which is best met with a common repository for network configuration data. This subject is discussed further in the section on configuration management and is an example of the overlap between some of the network management categories. The building and testing of changes is included in the change planning step. To do this requires the capability to build and test changes at a central site for later distribution to remote network components.
- *Distributing* involves the electronic distribution of changes via the network using SNA Distribution Services (SNADS). SNADS provides both fanout and store-and-forward functions that are needed for change distribution.
- *Installing* is a requirement for the unattended installation of changes. Change installation should be remotely scheduled for a particular date and time of day. There must also be a backout capability for regression to the previous level when a problem occurs with an installed change. Security is also involved in the installation step, in that it must be possible to verify that a change request is from a valid source.
- *Tracking* is the requirement for feedback information on the status of change installation to the change management central site.

The evolution of the change management functions provided for the IBM 3274 Subsystem Control Unit and its successor, the IBM 3174 Subsystem Control Unit, both parts of the IBM 3270 Information Display System,[7] illustrates the IBM change management strategy to meet emerging requirements. The IBM 3274 Subsystem Control customization[8] process requires a technician to perform the customization while physically at the control unit. As networks have grown in size, this has become an increasingly expensive method of implementing modifications required by configuration changes.

Configuration management is concerned with knowledge.

In 1986, the IBM 3174 Subsystem Control Unit was announced with a central-site customizing function. This function provides the ability to create and maintain at a central site a library that contains control unit parameters for all the IBM 3174s in a network and to generate customized diskettes for them. These diskettes can then be mailed to the individual control unit sites for installation by nontechnical personnel.

In June of 1987, the 3174 capability was announced for participation in electronic distribution of customization diskettes. In October of 1987, the NetView Distribution Manager (NetView DM) program was announced to support this electronic distribution capability. NetView DM is the follow-on product to Distributed Systems Executive (DSX)[9] and is IBM's strategic product for the change distribution function of change management.

The NetView DM capability for electronic distribution of 3174 customization data is based on SNADS and change management protocols that are part of the SNA network management architecture. These protocols provide the capability for NetView DM to retrieve customization data from a central-site 3174, distribute the customization data to one or more 3174s in the network (as shown in Figure 1), and to remotely install or regress the customization data on the basis of criteria that are part of the change plan.

Another example of the direction for change management functions in IBM products is the June 1987 announcement of the IBM PC Distributed Systems Node Executive (PC/DSNX). PC/DSNX allows the IBM Personal Computer AT, XT, and Personal System/2, when attached to a network via an IBM System/36, to make use of the NetView DM change distribution capabilities. (See Figure 2.)

Enhancements to the SNA change management architecture will continue to support the evolution of change management function in network products.

Configuration management

The configuration management category, as defined in SNA network management, is concerned with the generation and maintenance of a configuration database that contains knowledge of all physical and logical network resources and their relationships. Configuration management is not concerned with effecting or managing changes to the information system resources, but rather with knowledge of the location of network components (current topology), their identifying attributes, their status (active, online, etc.), future planning, and the process for gathering the configuration data.

The requirements for configuration management include the following:

- A single definition of configuration data for each network resource
- A common repository for the configuration database, which may be a distributed database
- An ability to share configuration data among people, applications, and subsystems
- The capability of dynamically updating the configuration database

A common repository for configuration data is very important, because it allows a single definition of each terminal as input into the definition process of network components such as communication controllers (37XX/NCP) and subsystems (VTAM). In addition, configuration data may be used for inventory management, network design, network configuration or reconfiguration, change management, problem management, and operator support. The direction of SNA network management architecture is to provide architecture to support solutions to configuration management requirements such as these.

Performance and accounting management

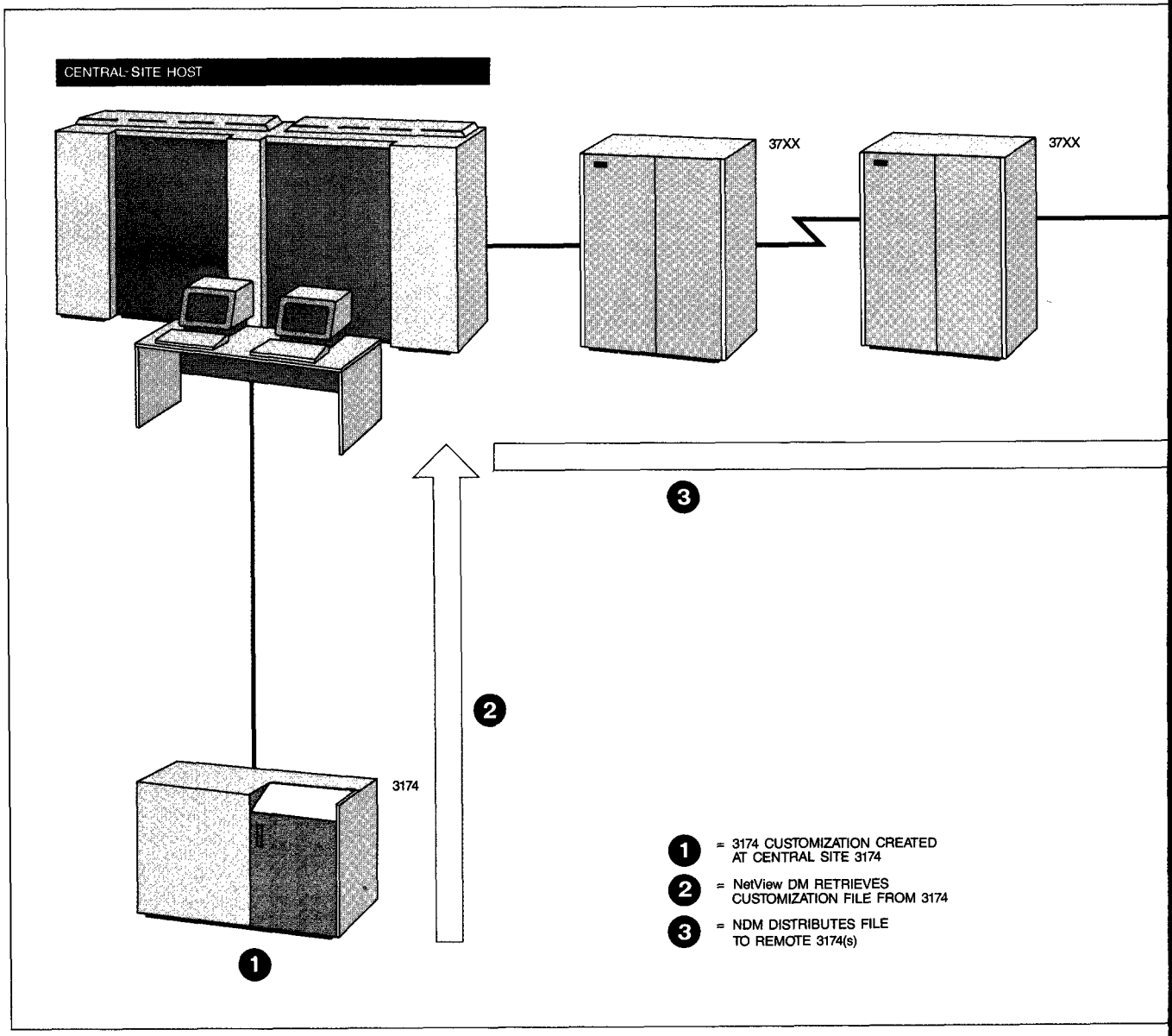
Network owners want to measure availability, monitor service levels, and account for resource usage. Because the data collection points necessary to perform these functions are similar, performance and accounting management are grouped as a single category for SNA network management.

In 1984, Network Logical Data Manager (NLDM) introduced the support of response-time monitoring, which allows the network operator to monitor certain predefined end-user service levels for specified LU-LU sessions. *Response time* is measured by the time elapsed between the instant an LU recognizes a request from its end user and the instant it receives the reply from the session-connected partner LU to which it sent the request. The response-time values can be sent unsolicited, based on the exceeding of predefined thresholds, or they can be solicited by the network operator. The information is carried in specially defined Response-Time Monitor (RTM) message units.

With the announcement of NetView in 1986, NLDM (and its functions) became the base for NetView's session monitor.

The NetView[10] and NPM (NetView Performance Monitor) products provide functions for performance and accounting management. The NetView product provides the capability to perform the following operations:

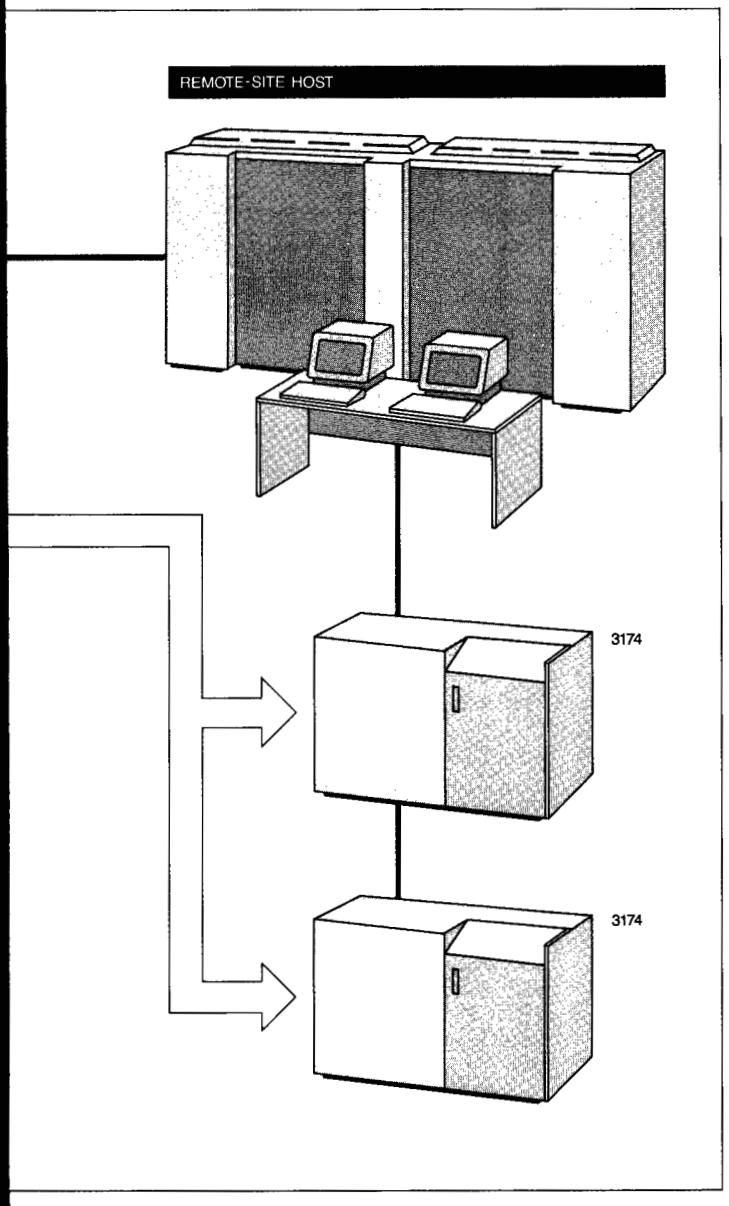
Figure 1 Example of 3174 customization flow from a central site



- Collect and display RTM data
- Collect actual end-user response-time data as measured by RTM components
- Display response time interactively (optionally in color), graphically comparing it to a predetermined objective by terminal and by session
- Monitor and test transmission line quality

The NPM product provides the following functions:

- Records performance data collected for various devices in the network
- Allows highlighting of the causes of performance degradation
- Provides data to help isolate performance prob-



lems
- Provides data to help tune the network for greater efficiency

Both NetView and NPM provide accounting exits so that customers can create their own accounting applications. Recognized requirements for performance and accounting management include the following:

- Extension of current functions to small-system networks and to a wider range of devices
- More information to tell the user how to correct problems
- Statistics collection at a central point for availability analysis, capacity planning, and accounting

Network performance can be impacted by the flow of network management data within the network. For this reason, the network management architecture and network management products must provide for carefully tailoring the volume of network management data flow to the needs and resources of the network. Examples of optional data might include trace data, performance statistics, accounting data, and configuration data. The ability to select the level of network management data flowing in the network can be considered a part of performance management.

The SNA network management architecture for performance and accounting management will continue to evolve to address new requirements as well as provide options, where appropriate, to adjust the network management function to the performance needs of a specific network.

Operations management

Network owners want the flexibility to centralize control of some functions and distribute others. This, together with automation of some operator functions, will reduce the cost of operations. NetView Release 2, announced in June 1987, provides enhanced operations management functions that help to meet these customer needs.[11] Commands entered at a NetView terminal can be routed to different system components, domains, or networks to allow a NetView operator to obtain access to an entire network from one operator station. NetView and the Inter-System Control Facility (ISCF) allow bring-up and restart capability, e.g., Initial Program Load (IPL) for a remote host. The customer can use the NetView customization facilities, command list (CLIST) capability, and user exits to provide automation of some operations functions. These NetView functions provide the base for meeting the operations management requirement for complex networks.

The requirements for operations management include the following:

- Centralized network management or decentralized network management capability is required because a small-system network must have the capability of being operated on-site or from a central host site, depending, for example, on the time of day.
- Automated operations are required, ranging from a simple CLIST to automate a trivial or repetitive operator function to artificial intelligence (AI) applied to automating operator decisions.

SNA network management architecture for operations management will evolve to allow NetView to extend support of functions that allow network owners to optimize the location and level of skills necessary to manage a complex network.

Integrated voice and data

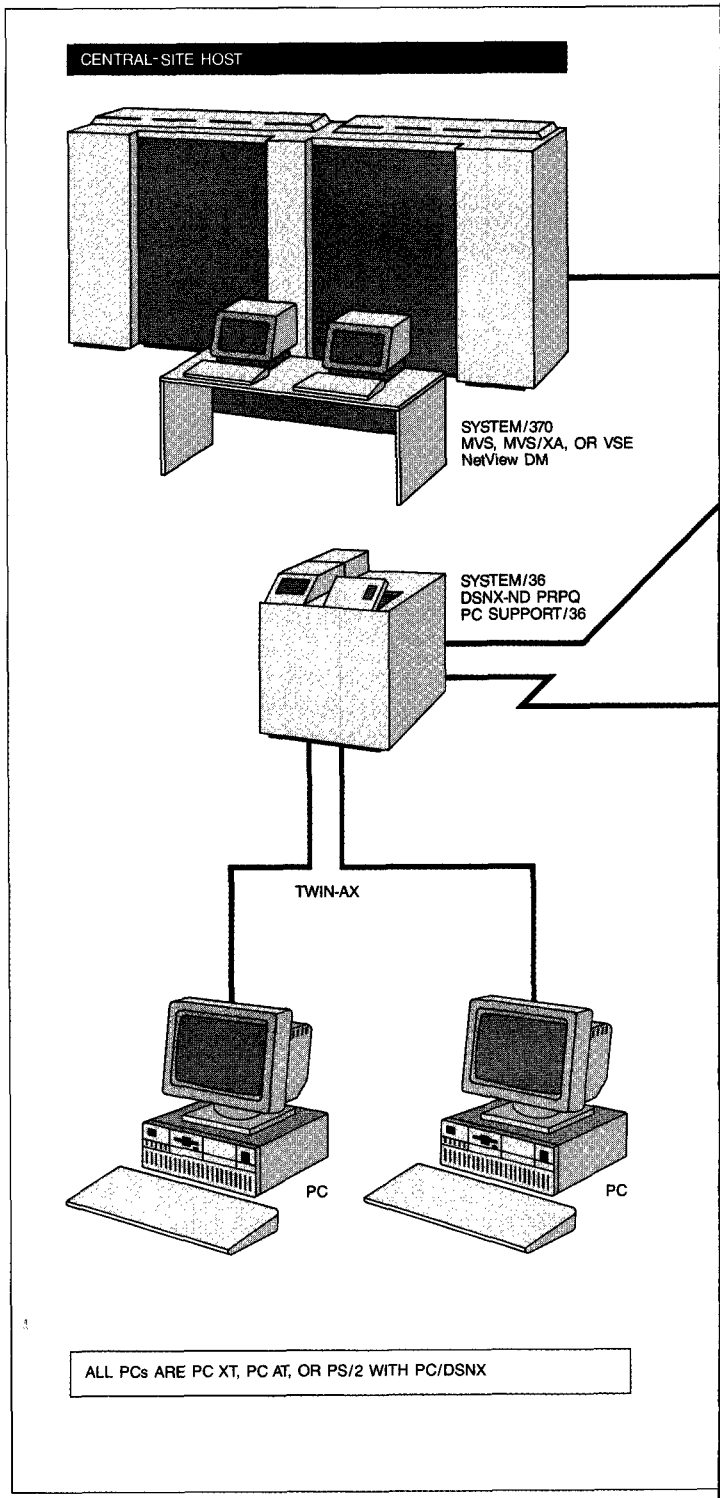
Much of the focus to date has been on the management of data networks. Now it is becoming increasingly important to provide for the management of voice networks and integrated voice and data networks. Plans for managing these environments include not only problem management but also change, configuration, performance and accounting, and operations management as well.

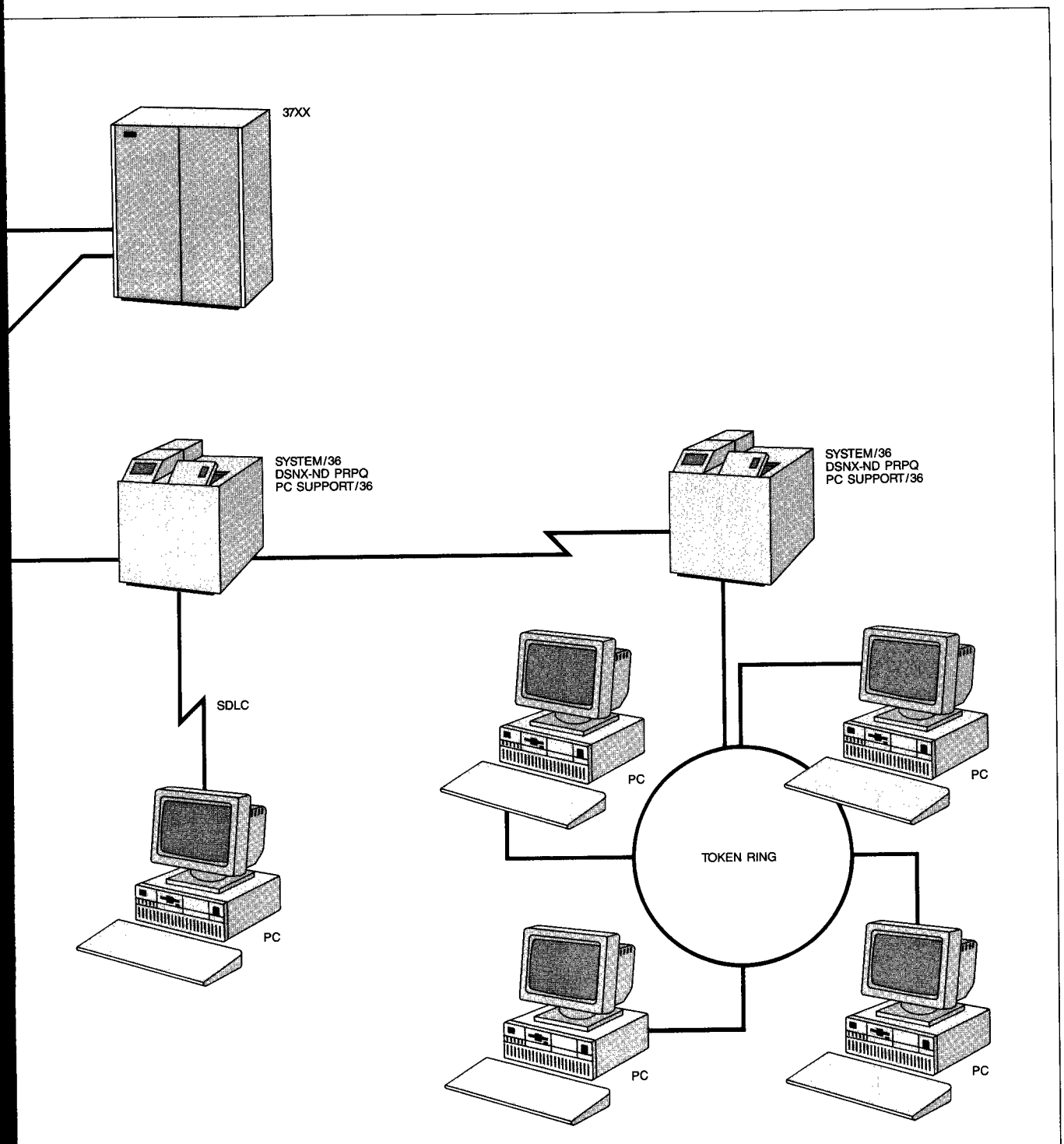
In September 1986, SNA Network Management was extended to include the private branch exchange (PBX) environment by announcement of a NetView/PC application that forwards Alerts and Call-Detail Records received from the ROLM Computerized Branch Exchange (CBX) to NetView and the Network Billing System. This was the first step of many toward providing centralized management for both data and voice resources.

The following are recognized needs for integrated voice and data management:

- Extension of network management features to voice/data integrated devices and to newly emerging link-layer protocols, such as ISDN.
- Correlation of accounting information between session information collected today by NetView and call information available from private branch exchanges and central office switches. This will provide users with the ability to give more granular billing for resource usage.
- Allocation of bandwidth in a dynamic manner based on time of day, operator command, or by program control. For example, a user may want to allocate more bandwidth for voice during day-

Figure 2 Example of central-site PC change distribution configuration




37XX
SYSTEM/36
DSNX-ND PRPQ
PC SUPPORT/36
SYSTEM/36
DSNX-ND PRPQ
PC SUPPORT/36
SDLC
PC
PC
PC
TOKEN RING
PC
PC

time hours, because there is more telephone usage during that period. During the evening, when fewer telephones are in use, the user may want to allocate the bandwidth for bulk data transfer.

Whereas centralized management for both voice and data networks may result in reduced network management costs, the advent of Integrated Services Digital Networks (ISDNs) creates many new challenges, including potential opportunities for improved network management. Using modems that support Link Problem Determination Aid (LPDA), a customer can gather information about the connection between two SNA nodes; however, there is no way to get direct information about the status of the actual connection from within the transmission network. ISDN promises to change this, offering the ability to exchange network management information between the equipment on the customer's premises and the service-providing equipment in the transmission network.

Open network management is a strategy for centralized network management, providing interface points known as entry points and service points.

A significant feature of ISDN is the existence of a standard, uniform interface between the customer premises equipment and the transmission network for the exchange of control information. Standardization activities related to this interface are focused on call control capabilities (e.g, call setup, call takedown). Expanding the capabilities of this interface to include the exchange of network management information can create a great opportunity for synergy in network management.

True cooperative communication between the customer-premises equipment and the transmission network for the exchange of network management information makes available more information to properly isolate and diagnose problems, resulting in quicker problem resolution. Enhancements to change, configuration, performance and accounting, and operations management capabilities may also be possible. The standardization of a uniform interface between the customer-premises equipment and the transmission network for the exchange of network management information is expected to continue in importance.

The direction of SNA network management architecture is to provide an integrated network management solution encompassing all categories of network management for data, voice, and integrated voice/data environments.

Open network management

Open Network Management[12] provides a structure that allows for extending SNA network management to support non-SNA, voice, and multivendor telecommunication products. Included in Open Network Management are the following:

- Published network management architectures
- Application programming interfaces (APIs) that allow customer and vendor access to the network management data and commands
- Network management products that use these architectures and APIs to facilitate management of both SNA and non-SNA product components of the network

Open network management is a strategy for centralized network management, providing interface points known as *entry points* and *service points*. Both of these interface points report their management data to a *focal point* for network management. A network management *focal point* provides centralized network management support and represents the final level at which network management decisions are made. Examples of products providing support for a focal point include NetView, NetView Distribution Manager (NetView DM), NetView Performance Monitor (NPM), and Info/Management. A network management *entry point* provides network management support for itself and for attached products. It transports both network management and operational data on a common SNA link. Examples of entry points include System/36, System/38, 3720, 3725, 3174, System/88, Series/1, and 3708 Network Conversion Unit.

A network management *service point* provides network management support for itself and attached products that are not capable of providing network management support for themselves, e.g., ROLM CBXs, selected PBXs, and non-SNA components. A product that provides service-point function transports *only* network management data for the supported products. A service point provides a connection through which network management data can be converted to SNA formats and transmitted to the focal point for processing. NetView/PC is an example of a service-point product.

SNA formats and protocols are used to exchange data between the *entry point* and *focal point* and between the *service point* and *focal point*. Commands and protocols used to exchange data between a *service point* and its supported products are determined by the products.

The structure provided by open network management allows non-SNA, voice, and vendor telecommunication products to participate in SNA network management. The architecture and product functions will continue to be provided and extended to allow customers to do this end-to-end network management as part of open network management.

Systems application architecture

Systems Application Architecture (SAA)[13] is a collection of selected software interfaces, conventions, and protocols that are becoming the framework for development of consistent applications across the future offerings of the following three major IBM computing environments:

- System/370 (TSO/E under MVS/XA, and CMS under VM)
- System/3X
- Personal Computer (Operating System/2™)[14]

SNA network management architecture is a component protocol of the Common Communications Support area of SAA.

SAA Common Communications Support is used to connect applications, systems, networks, and devices within the SAA system families. The generic Alert architecture is an example of network management architecture contributing to the Common Communications Support protocols of SAA. The generic Alert architecture defines the formats and protocols for sending Alerts such that all network products, including products from all three SAA families, can forward this network management data to the problem management focal point in the network.

There is a requirement to extend SAA concepts to other areas of network management, e.g., a common interface to the network operator, a network management application-enabling interface, and a common interface to network management databases. The present trend is evolving toward consistency in these areas among the SAA product families.

The present trend is evolving toward consistency among the SAA product families.

Concluding remarks

SNA network management capability has continued to evolve with SNA to support increasing levels of network management in IBM products. This evolution has been seen in each of the network management categories, i.e., in problem management, change management, configuration management, performance and accounting management, and operations management. SNA network management will continue in new areas, such as voice and data integration, as these requirements become clear.

Open network management has added the capability to support Local-Area Network (LAN), non-SNA, voice, and multivendor telecommunication products in the SNA end-to-end network management strategy. As the development of Open Systems Interconnection (OSI) Management standards evolves, enhancements to the end-to-end network management strategy should incorporate management of OSI resources using OSI management protocols.

New requirements exist for network management extensions in each of the network management categories, and more requirements will emerge as SNA architecture continues to evolve. Common solutions

are required, whether for the management of small or large systems, whether interconnected via SDLC, X.25, ISDN, or local-area networks, and whether transporting voice or data.

Network management is an integral part of each SNA enhancement, and it is our aim to continue to build on the architecture and products discussed in this paper to meet new network management requirements. SNA network management architecture will continue to map the way to end-to-end network management capability in IBM products and in customers' networks.

Cited references and notes

1. *SNA Format and Protocol Reference Manual: Management Services*, SC30-3346, IBM Corporation (1987); available through IBM branch offices.
2. A physical unit (PU) is an addressable entity, like the SSCP or LU; one PU exists in each node for local control and to represent the node to a control point (SSCP) in a host processor if one is currently controlling the PU. In a type 2.1 node, a control point (CP) exists to perform local control and to provide required PU services for a remote SSCP.
3. R. J. Sundstrom and G. D. Schultz, "SNA's first six years: 1974–1980," *Fifth International Conference on Computer Communication*, Atlanta, GA, North-Holland Publishing Co., Amsterdam (September 1980), pp. 578–585.
4. R. J. Sundstrom, J. B. Staton III, G. D. Schultz, M. L. Hess, G. A. Deaton, Jr., L. J. Cole, and R. M. Amy, "SNA: Current requirements and direction," *IBM Systems Journal* **26,** No. 1, 13–36 (1987).
5. NetView and NetView/PC are trademarks of the IBM Corporation.
6. Generic Alerts are described in detail in "SNA alerting in a multivendor environment" by Robert E. Moore in this issue.
7. *IBM 3270 Information Display System*, GA20-2739, IBM Corporation (1986); available through IBM branch offices.
8. Customization is the process of identifying each control unit with its attached terminals and features as well as with its method of host connection. It results in an updated microcode diskette that is used for initially loading the control unit's microcode.
9. *DSX General Information Manual*, GH19-6394, IBM Corporation (1987); available through IBM branch offices.
10. *Network Program Products General Information Manual*, GC30-3350, IBM Corporation (1986); available through IBM branch offices.
11. D. Kanyuh, "An integrated network management product," *IBM Systems Journal* **27,** No. 1, 45–59 (1988, this issue).
12. *Introduction to IBM's Open Network Management*, SC30-3431, IBM Corporation (1986); available through IBM branch offices.
13. *Systems Application Architecture: An Overview*, GC26-4341, IBM Corporation (1987); available through IBM branch offices.
14. Operating System/2 is a trademark of the IBM Corporation.

David B. Rose *IBM Communication Products Division, P.O. Box 12195, Research Triangle Park, North Carolina 27709.* Mr. Rose is currently manager of Network Management Architecture, with responsibility for the development of the SNA Management Services architecture for network management. After graduating from the Electrical Engineering Technology program at the University of Texas at Arlington in 1960, he joined IBM in the Field Engineering Division in Fort Worth, Texas. Mr. Rose participated in the first trial of programming support provided by the Field Engineering Division (for the IBM 7090), assisted in the first customer installation of an IBM System/360, and then worked as a specialist in hardware and software support for large System/360 systems. In 1971 he came to Research Triangle Park, where he has worked in communication systems performance evaluation and several departments related to SNA development. Mr. Rose received an Outstanding Innovation Award and a Corporate Award in 1982 for his contribution to development of an executable specification for SNA.

Jane E. Munn *IBM Communication Products Division, P.O. Box 12195, Research Triangle Park, North Carolina 27709.* Ms. Munn joined IBM in 1984 in the Systems Network Architecture development group at Research Triangle Park. Initially she was responsible for local-area network logical link control architecture and its integration into SNA, and contributed to the IEEE 802.2 Logical Link Control standards committee. She is currently manager of Communications Architecture, with responsibility for the development of architecture for the IBM Token-Ring Network and the management of communication links, and for IBM participation in standards activities related to local-area networks and network management. Ms. Munn has a B.S. in computer science from the University of Nebraska and an M.B.A. from Duke University.

Reprint Order No. G321-5307.