SNA Perspective

Volume 13, Number 6
June, 1992
ISSN 0270-7284

The single source, objective monthly newsletter covering IBM's Systems Network Architecture

Integrating TCP/IP Into SNA Part II: Applications

In the multiprotocol environment in which most companies operate today, two of the most common networking protocol suites are SNA and Transmission Control Protocol/Internet Protocol (TCP/IP). Each protocol now represents a significant investment for many corporations. Various reasons motivate companies to integrate these two different networks to some degree. They see an opportunity, by combining the resources of the two networks, to increase access, leverage investment, control costs, and avoid redundancies.

This article, the second in a series on the integration of TCP/IP into SNA networks, addresses issues of integrating the two environments at the application level—in particular supporting TCP/IP access to the range of mainframe applications and resources commonly accessed through SNA. IBM's approach to support multiple networking protocols by decoupling applications from the network is examined in three unannounced IBM products.

(continued on page 2)

LAN Network Manager Update

In recent years there has been a surge in demand among SNA users for LAN network management. Initial IBM products managed LAN adapters but provided limited device management capability. Many customers have taken a cautious attitude toward IBM token ring network management because of limited LAN management capability, product delays, and lack of a clear LAN management direction from IBM.

For the past year, we have been hearing about the "new" IBM LAN Network Manager and a complementary product, LAN Station Manager. This article describes LAN Network Manager (Versions 1.0, 1.1, and Entry) and LAN Station Manager, details their benefits to token ring users, discusses several features including configuration and user interface, defines target customers, illustrates their fault, security, and bridge management options, outlines the connection between NetView and LAN Network Manager, and addresses customer concerns about standards-based network management.

(continued on page 9)

In This Issue:

(continued from page 1)

The Need for Interoperability

The Open Software Foundation (OSF), a consortium of vendors, end users, government agencies, research centers, and universities, surveyed its membership to identify the most pressing problems and unresolved issues facing the open systems industry. Lack of interoperability was cited more often than any other issue.

SHARE, an IBM information systems user group, prioritized the most pressing computing and networking concerns of its more than 2,000 member organizations. Interoperability was ranked as the number one concern for both 1991 and 1992.

IBM's Position

IBM provides services for both SNA and TCP/IP as identifiable and distinct protocol stacks and services. The company believes, however, that the best long-term strategy is to separate the network from the applications.

Common Transport Semantics

In March 1992, IBM unveiled its networking blueprint as an architecture for this long-term strategy. This blueprint includes a transport-layer interface called common transport semantics (see Figure 2 in *SNA Perspective,* April 1992). IBM has not published the common transport semantics interface because it is still in development, but seems to be moving toward opening it up. For example, the company recently presented the interface to X/Open to consider including in its recommendations.

The purpose of common transport semantics is to provide both a mapping and a compensation between the transport services required for an application and the capabilities of the transport system being used. If the transport system to be used is feature rich, little compensation will be needed and, in fact, some of the overhead of the more functional transport system may be eliminated to improve performance. If the underlying transport system is lacking in some features needed by the application, this compensation can make up the difference. In other words, the common transport semantics interface is designed to provide a leveling of the field for all transport services below it and to support the major emerging application programming interfaces above it, including remote procedure call (RPC), message queueing, and the common programming interface for communications (CPI-C).

Dimensions of Integration

In this series of articles, *SNA Perspective* considers the challenge of integrating TCP/IP into SNA in three areas—networking, applications, and systems.

In part one of this series, we discussed the issues surrounding network connectivity—the use of the components of an existing SNA network to support TCP/IP traffic. In this article, we consider two aspects of application connectivity—integration of SNA/mainframe and TCP/IP environments at the application layer and above and integration of the applications of one stack over the networking protocols of the other. In a future installment, we will consider TCP/IP offerings across system platforms.

Application Integration

For many years, products have existed for TCP/IP traffic to access SNA networks and the systems on those networks (see *SNA Perspective*, May 1992). However, getting a connection to the host does not automatically give a TCP/IP user access to all mainframe applications and resources.

Definitions

In this article, we use the term "TCP/IP-to-SNA application integration" broadly to mean access through a TCP/IP network and TCP/IP application-layer services to mainframe-based applications and resources often associated with SNA and usually accessed through SNA. We acknowledge the technical limitations of what we consider to be a useful approach to understanding this complex topic:

- Most of the host resources and applications discussed here are not, strictly speaking, SNA applications. They are usually but not *necessarily* accessed through SNA. For example,

TCP/IP Application Services

The TCP/IP lower layer protocols were discussed in part one of this series (see *SNA Perspective,* May 1992). Today, the TCP/IP protocol suite includes over eighty application-level networking services and application enablers. These are openly developed through a request for comment (RFC) process. The most popular of these include:

- **Telnet**—A virtual terminal protocol used on top of TCP/IP (and in some other networks as well). It allows the client to access the resources of the server as if the client were a local terminal. Telnet was designed for line mode terminals, though the client may be a system or application.
- **File Transfer Protocol (FTP)**—FTP allows the transfer of various file types between arbitrary host computers and provides format conversions as required.
- **Network File System (NFS)**—Originally developed by Sun Microsystems, NFS has become a de facto standard for a distributed file system in the internet market. It allows users to share files over a TCP/IP network on various platforms and operating systems from different vendors. NFS provides end users with a transparent means of accessing the required information by furnishing the communication between the user machine (client) and the remote source (server) of the target file.
- **Trivial FTP (TFTP)**—Provides file transfer using the User Datagram Protocol (UDP). It lacks most of the features available in FTP in that it can only read from or write to a server. Its benefits are simplicity and small size and it operates with little overhead. The main drawback of TFTP is its lack of provision for security or user authentication.
- **Simple Mail Transfer Protocol (SMTP)**—The most widely used TCP/IP application, SMTP provides an electronic mail protocol to permit transfer of mail items between different vendors' systems, relying on TCP/IP at the lower layers for delivery.
- **Domain Name Server**—Provides an automated name/address resolution system so that users can specify a remote system with a symbolic name instead of its real IP address. The domain name system consists of a server application for translation between high-level machine names and the IP addresses and a complementary client process called the resolver, which makes requests to the server if it does not find a name/address match in its cache.
- **Simple Network Management Protocol (SNMP)**—SNMP is an increasingly popular protocol for multivendor network management even beyond TCP/IP networks. An SNMP network management station monitors and conrols the network through agent processes in systems, workstations, routers, and other network elements.
- **Remote Execution Command (REXEC) protocol**—With REXEC, a client system can send a command to the daemon (server) to handle execution of jobs in the daemon's system.
- **Kerberos**—The Kerberos authentication and authorization system provides an encryption-based security function to enable each member of a client/server pair to authenticate its partner. Named after the three-headed dog guarding the entrance to Hades in Greek mythology, Kerberos has been accepted as a standard by the Open Software Foundation as an element of its Distributed Communication Environment, and is becoming increasingly popular in the internet market. ■

Professional Office System (PROFS) is a mail package under VM but is often considered an SNA mail system.

- Some of the TCP/IP applications discussed here, such as SQL and LPR/LPD, are not part of the official TCP/IP suite but are often found in and associated with TCP/IP environments.
- Native TCP/IP access often does not require SNA. Many solutions involve native TCP/IP access to host resources *instead of* SNA rather than *through* SNA. For example, VM's Shared File System can be accessed either from an SNA network through VTAM or from a TCP/IP network through FTP without any SNA involvement.

IBM Solutions

As discussed in the first article of this series, although many vendors supply solutions to meet these user requirements, we have chosen to focus on IBM solutions. Also, although we will introduce both native (host-based) and gateway (non–host-based) approaches, our focus is on native solutions.

IBM provides a number of ways to use host resources through TCP/IP and that number has been steadily growing. IBM was somewhat slow in ramping up to match the unexpected TCP/IP market growth because, along with many other vendors, IBM had considered TCP/IP a tactical step on the way to OSI. However, IBM has dramatically increased its TCP/IP investment in the past few years. The resulting products have been rolling out at an increasing pace and 1992 could be designated IBM's Year of TCP/IP.

An increasingly popular role for the mainframe is as a network server rather than a network controller. In this era of downsizing, IBM knows it must tailor the mainframe to this market.

Application Access

Many mainframe applications may be accessed with the Telnet terminal protocol using the Telnet server in TCP/IP for VM and MVS. IBM's products support the tn3270 extension to Telnet so that TCP/IP users can access applications in full-screen 3270 mode. However, the users' systems must also support tn3270 or equivalent. (See *SNA Perspective*, June 1991.)

Going in the other direction, users on the mainframe may access applications on other TCP/IP hosts using the Telnet client support in TCP/IP for VM and MVS. Third-party software from companies such as A-NET allows 3270 users to access Telnet in popular ASCII full-screen mode such as VTxxx emulation.

Electronic Mail

Mail in UNIX environments is most often provided through the Simple Mail Transfer Protocol (SMTP). Customers can use SMTP as a native mail package on the host or may prefer an interface between SMTP and an existing host mail package.

Electronic mail exchange between SMTP and the mainframe's various mail environments can be provided through gateways that run on MVS, VM, and OS/400 platforms. An example of such a gateway is Soft-Switch Central, which IBM resells.

For SMTP to PROFS mail interchange under VM, the customer needs an extension to PROFS called Extended Mail which can communicate with SMTP Note in IBM's TCP/IP for VM. In addition to PROFS, SMTP can communicate with VM's underlying Remote Spooling Communication Subsystem (RSCS).

On MVS systems, IBM's TCP/IP for MVS does not support SMTP access to DISOSS. However, SMTP mail may be sent to the job entry subsystem (JES) spool through RSCS/NJE, which can be used by several MVS mail packages from other vendors.

Data Access

With connection to the IBM host, TCP/IP users can obtain access to host direct access storage devices (DASD), the high-speed, high-capacity storage of the mainframe system. One popular application is to use the mainframe DASD to back up systems on TCP/IP networks.

FTP provides for the transfer of files between systems, including read/write access and ASCII/EBCDIC data conversion. Access control can be provided by passwords through RACF or other means. The trivial file transfer protocol (TFTP) provides similar access but without password protection or directory capability.

In addition to this basic FTP capability, IBM is enhancing its FTP support to further exploit host access. For example, TCP/IP for VM V2R2 enhances FTP support to allow transparent access to disks that are part of VM's Shared File System. In addition, in TCP/IP for MVS, FTP supports Parallel I/O Access Method (PIOAM) which supports "striping," the ability to write a file across multiple DASD devices in parallel.

File Access

NFS is a distributed file service that allows users to share files across a variety of machine types and operating systems. In the VM environment, NFS can use Conversational Monitor System (CMS) minidisks. Most IBM implementations of NFS are purchased separately from the TCP/IP base package.

IBM has implemented NFS client and server under VM, AIX (S/370/390, RS/6000, PS/2) and OS/2; NFS client under DOS; NFS server under MVS; and has stated that NFS server will in the future be a feature under OS/400.

Data Sharing

Data sharing between IBM environments includes relational data as well as file sharing. With regard to relational data, IBM plans to provide increasing interoperation between distributed relational databases and its traditional mainframe database interface to DB2. This interoperation will be based on the structured query language (SQL). Although SQL is not a TCP/IP standard, it is the emerging multivendor standard and popular in the same markets as TCP/IP.

Print Sharing

Although the line printer protocol is not defined by any RFC and therefore is not strictly a TCP/IP protocol, it has been a popular component of UNIX for many years. Support for both line printer requester and daemon (LPR/LPD) is available in Version 2 Release 2 of TCP/IP for VM and is expected in TCP/IP for MVS V2R2. LPR (client) on the host allows host users to send data to be printed on LPD print servers on the TCP/IP network. In the other direction, LPD (server) on the host provides access to VM-supported printers for users on the TCP/IP network.

Shared Display

Developed at MIT, X Windows is a portable graphical user interface which is a de facto standard in the workstation market. X Windows provides an API for program access to a bit-mapped display. The terms server and client are used counterintuitively with X Windows, different from most TCP/IP applications—X-server is the program on the user's workstation that manages the display services and X-clients are the local or remote applications that send data to be displayed. IBM TCP/IP for VM and MVS both implement the X Windows client function, but currently only VM supports the server function.

To integrate X Windows with its existing products, IBM provides an interface to its Graphical Data Display Manager (GDDM) so that GDDM output can be sent to X displays.

Network Management

IBM has begun providing NetView-based functions for integrated SNA, TCP/IP, and OSI networks being managed with SNMP and CMIP as well as IBM's proprietary management protocols. See the January and February 1992 issues of *SNA Perspective* for in-depth descriptions of these integrated network management capabilities.

Application-to-Network Flexibility

IBM is increasingly providing the means for TCP/IP users and applications to access mainframe applications and resources. Some of these application-to-network options are based on an architectural approach; others are more near-term, focused-function products.

The architectural approach is intended to support many application types over many network types. Products based on this approach tend to reach the market later but are also designed to meet long-range needs. Further, because of their greater capability, they may consume more resources, have an impact on performance, and carry a higher price tag. IBM has unveiled its architectural direction for

generalized application-to-network flexibility in its networking blueprint.

On the other hand, products based on the focused-function approach usually interface one or few application types to one or few network types. These are available more quickly but can have a shorter life-cycle. However, they also tend to be less expensive and have less impact on the system.

An example of a focused-function product is IBM's forthcoming CICS-sockets interface, which is discussed below. Other examples include internet RFC 1006, which provides an interface for OSI applications to run over TCP/IP, and an RFC that defines support for NetBIOS over TCP/IP.

When discussing its networking blueprint, IBM mentions two examples it is developing that are based on the architectural approach in the networking blueprint—CPI-C over TCP/IP and TCP/IP sockets over SNA (SNAckets). These two and the CICS-sockets interface are discussed below.

Coming Soon: CICS over TCP/IP Sockets

IBM has been discussing, with several users and at a recent SHARE meeting, its plan to introduce a sockets interface to access Customer Information Control System (CICS) applications over TCP/IP (see Figure 1). Because of IBM's detailed discussions on and demonstrations of this product and its pace of TCP/IP announcements, *SNA Perspective* expects this announcement soon.

This is a significant development since CICS, IBM's foremost transaction processor and primary application subsystem on MVS hosts, is the "owner" of a great deal of the centralized data in many enterprises. Natively, access to CICS applications has been through COBOL programs and usually via SNA networks. Although many users on TCP/IP networks require access to CICS data or applications, these users are generally from environments where the preferred language is C and where application access is through function calls and sockets.

To access CICS data over TCP/IP today, Telnet is usually used, most often in conjunction with tn3270 (see *SNA Perspective*, June 1991). In the tn3270 approach, a workstation with both a 3270 user application and tn3270 Telnet support can access a CICS 3270 application. The workstation acts as a 3270 device. The 3270 traffic is encapsulated in IP packets by tn3270 and sent across the TCP/IP network to the mainframe, where the TCP/IP software on the host passes the frames to CICS. (VTAM is only involved, in this scenario, for the 3270 session establishment.)

This approach has three primary limitations. First, the TCP/IP end user or application is required to act as a CICS workstation, using a CICS interface (usually 3270) rather than a more familiar interface. Second, these solutions are usually application-specific; even tn3270 allows only access to 3270 CICS applications and does not support printers. Finally, the use of 3270 requires SNA involvement as well as TCP/IP. A significant benefit of this approach, however, is that the host applications remain unchanged.

With the forthcoming CICS-sockets interface, users on TCP/IP networks will be able to obtain access to CICS applications using a familiar interface with native functions. In this model, CICS is accessed via the socket interface such that it appears to the TCP/IP user or application as another sockets application.

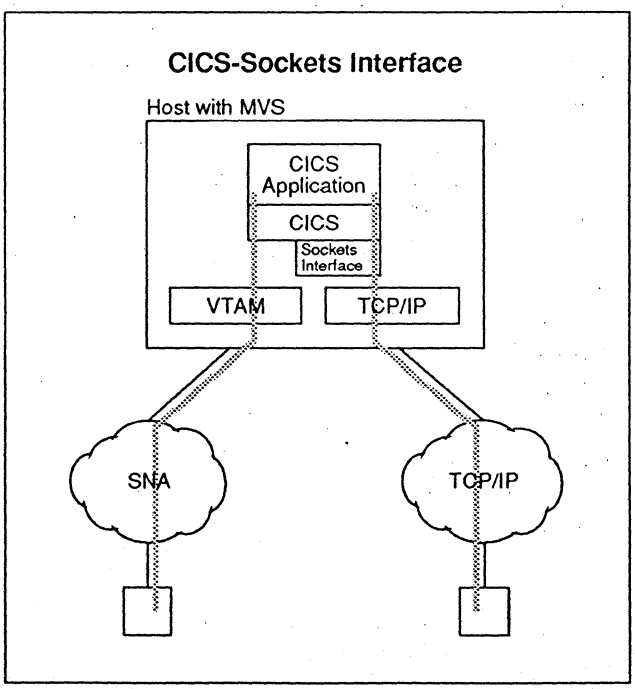

Figure 1

Readers should note that, while *SNA Perspective* believes this interface is a significant benefit, all CICS applications to be accessed using this interface will need to be adapted to support sockets. Also, although IBM is generalizing CICS to run on all SAA platforms, as discussed in *SNA Perspective*, December 1991, this interface is designed only for MVS environments.

SNAckets: TCP/IP Sockets over SNA

Although the CICS-sockets interface will likely become a popular product, IBM architects are probably hoping that customers will plan to migrate to a more architectural approach based on IBM's networking blueprint. IBM has not discussed a timeframe for SNAckets and CPI-C over TCP/IP. Based on market need, *SNA Perspective* expects SNAckets will be announced much earlier that CPI-C over TCP/IP.

IBM committed in March 1992 to support sockets over SNA, a capability which IBM informally calls SNAckets. It is important to note that, although we like the name, SNAckets is actually an implementation of sockets over LU 6.2. SNAckets will, work over either APPN or subarea SNA networks that support LU 6.2.

Sockets are a common interface on Unix systems. Sockets appear to an application as a transparent byte stream. A TCP/IP socket refers to the combination of the internet address and a port identifier which identifies the higher-level process to which incoming packets must be delivered. Thus, sockets can be used as a means of process-to-process communication. A sockets connection is roughly analogous in SNA to a session.

CPI-C Over TCP/IP

IBM stated in March that CPI-C will support TCP/IP transport as well as SNA and OSI (see Figure 2). The company has already architected this solution and is working with a customer to develop a prototype. For more details on CPI-C, see *SNA Perspective*, March and May 1992.

One of the challenges in developing CPI-C over TCP/IP is that CPI-C was designed to run over block-mode transport such as LU 6.2/APPN and OSI, while TCP/IP transport expects a streams-mode interface such as sockets or AT&T's newer transport layer interface (TLI). A benefit of architecting this block-over-streams mapping is that it can be used for other application-transport combinations.

TCP/IP Host Access: Gateway or Native

Two approaches have been used by several vendors to bring TCP/IP users to the host environment—gateway (TCP/IP to SNA gateway) and native (TCP/IP directly accessing host resources).

Gateway

In general, the gateway or protocol conversion approach is less expensive, is less complex to install, and can be a sufficient solution if only light TCP/IP traffic is expected. On the other hand, the gateway option tends to be limited in function and scope and inefficient in performance and overhead. It also usually has some host software component to contend with.

There are several suppliers in this market. OpenConnect Systems (formerly Mitek) of Carrollton, Texas, is a leader in using the gateway approach, offering a wider range of functionality than most gateway products. The OpenConnect product usually runs on an RS/6000 or Sun workstation, with a control program running on the mainframe. NCR Comten supports TCP/IP on its communication controllers. IBM also has TCP/IP gateways to the host on its AS/400 and RS/6000 midrange systems.

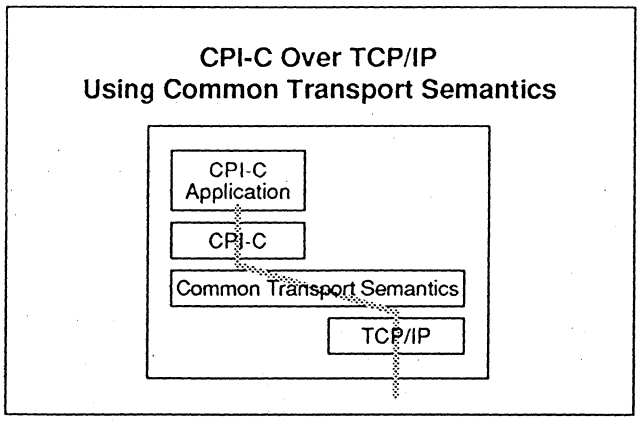

Figure 2

Native

Next to IBM's product, the best known TCP/IP "native" solution for MVS systems is SNS Network Integration from Interlink Computer Sciences of Fremont, California. Interlink has long been a supplier of DECnet-to-SNA integration solutions and acquired the TCP/IP technology from ACC of Santa Barbara, California. For TCP/IP on both VM and, to a lesser extent, MVS systems, IBM's primary competition comes from Fibronics of Hyannis, Massachussetts.

IBM's TCP/IP for VM and MVS

TCP/IP for VM was IBM's first platform to support TCP/IP. It was introduced in July 1987, prior to AIX/370. TCP/IP for MVS was announced in September 1988.

With the exception of AIX for the RS/6000, the VM implementation of TCP/IP is the most complete version of the TCP/IP protocol suite available from IBM. In contrast to the current Version 2 Release 1 of TCP/IP for MVS, TCP/IP Version 2 Release 2 for VM offers more application protocols. *SNA Perspective* believes that IBM will soon announce Version 2 Release 2 of TCP/IP for MVS. This will likely fill in some holes in the current release vis-à-vis the VM release, such as Kerberos (client/server) NCS, LPR/LPD, and REXEC (daemon).

The reason IBM has released versions of TCP/IP for VM before MVS is related to the development of the product. IBM mainframe TCP/IP development had been done in the VM environment and then ported over to MVS, in part because VM and Unix share a common ancestry and in part because VM had been more popular than MVS in the university environment where TCP/IP was also flourishing.

Porting from VM to MVS is not without its restrictions. The implementation of TCP/IP designed for VM, when ported to the MVS environment, may not operate as efficiently if it is not redesigned to exploit MVS. *SNA Perspective* understands that early releases of TCP/IP for MVS, due to budget constraints, were hampered in performance and overhead due to the porting but that recent releases, due to IBM's increased investment in TCP/IP, have been more efficient in the MVS environment.

Summary

The change of focus in the enterprise computing environment requires that systems to be adapted to meet the needs of users. This means, increasingly, that TCP/IP users must be accommodated within a traditionally SNA world.

IBM's position is to support SNA, TCP/IP, and OSI across its product line. Primarily, these have been implemented as separate protocol stacks. But in the long term, the company sees the need to separate applications from networking for each stack so that customers can select applications and networks independently, each on its own merits. By decoupling the the applications from the network and providing a means to compensate for their differences, IBM sees the common transport semantics element of its networking blueprint as an integral part of future application-to-network connectivity.

IBM's current TCP/IP products usually include both transport/network layer protocols and application layer services. However, NFS support is sold separately for TCP/IP host and workstation offerings and several other applications are separately supported on the workstation products. *SNA Perspective* believes that, with the company's drive to decouple applications from the network, IBM will likely continue this trend to break off application support into separate products.

IBM seems to have been focusing on adding TCP/IP applications to its host-based products. With the basic application sets almost complete in the V2R2 release, *SNA Perspective* expects IBM to shift its focus on greater integration of these TCP/IP features with host resources.

In a future installment in our TCP/IP series, *SNA Perspective* will consider the experience of several end users in integrating TCP/IP into SNA environments. We will note their needs, discuss how these needs have been addressed to date, and look at what solutions they require in the future. The focus will be on the common problems faced by many enterprises and the solutions that can be implemented to meet the needs of this changing and evolving networked environment. ■

(continued from page 1)

LAN Network Manager

IBM's product for managing token ring LANs is LAN Network Manager. Three versions were announced at the same time: LAN Network Manager 1.0, LAN Network Manager 1.1, and Entry. Version 1.0 is currently available; the expected date for general availability of the other two has been pushed out from April to December 1992. This article focuses on LAN Network Manager 1.1. (See Table 1 for a brief description of the differences between the three products).

The price of LAN Network Manager Version 1.0 is $3,995; Version 1.1 is $4,995. LAN Network Manager Entry costs $1,395. Upgrade pricing from older IBM LAN management products such as LAN Manager is available.

Because of the delay in releasing LAN Network Manager 1.1, IBM users are being cautious about buying. This delay compounds several other user concerns including frustration about the continuing lack of IBM LAN management direction, lack of information about the LAN Network Manager product, confusion over product features and functionality, and concerns about the future of the product.

SNA Move to LANs

SNA users have increasingly been moving from traditional subarea SNA networks with communication controllers and cluster controllers with SDLC to SNA gateways and 3270-capable workstations installed on token ring LANs. This migration has created a problem for network administrators in managing their growing base of multivendor LAN networks and devices—bridges, routers, hubs, PCs, and SNA gateways. IBM's traditional SNA management platform, NetView, has been unable to provide adequate management capabilities for LANs.

SNA network administrators face several problems in managing LANs:

- Controlling unauthorized user access
- Managing connectivity problems in cabling, workstation adapters, bridges/routers, hubs, and other network devices
- Capacity planning
- Defining performance monitoring and tuning methods
- Operating LANs remotely from NetView
- Managing the software and application programs resident on the workstations, bridges, routers, and hubs

LAN Network Manager replaces IBM's earlier LAN Manager product (not to be confused with Microsoft's LAN Manager network operating system). Operating in a PS/2 running OS/2, LAN Network Manager can manage multiple token ring LANs and their attached devices: the IBM 8209 token ring to Ethernet bridge, the IBM PC bridge software program, the 8230 token ring control access unit (CAU), and the adapters for workstations, 3745s (TIC interface), and 3174s. Token ring devices can be managed locally by LAN Network Manager or through NetView. (See Figure 3 on page 10 for a topology with LAN Network Manager and LAN Station Manager.)

LAN Network Manager 1.0, 1.1, and Entry Feature Comparison

	Local LAN User Interface	Multi-segment TR Mgmt	Single-segment TR Mgmt	Alert Filtering	NetView Support	Graphics/ Automation Support
1.0	Yes	Yes	Yes	Local + NetView	Optional	No
1.1	Yes	Yes	Yes	Local + NetView	Optional	Yes
Entry	No	No	Yes	NetView	Required	No

Table 1

LAN Network Manager 1.1

LAN Network Manager Version 1.1 adds the following features to Version 1.0:

- Optional OS/2 command line automation

- Optional graphical user interface which provides a color topology map of the network
- Extended 8209 token ring to Ethernet bridge management via additional filters
- Enhanced NetView command interface

LAN Network Manager 1.0 was supported by only eleven commands from NetView. Commands entered at NetView were parsed and then passed to LAN Network Manager. This is no longer the case with Version 1.1—NetView commands are forwarded to LAN Network Manager to be executed there. All commands available at LAN Network Manager are available to the network administrator from NetView including building station profiles and setting LAN Network Manager 1.1 system parameters.

LAN Station Manager

A new IBM software product, LAN Station Manager, works in conjunction with LAN Network Manager to provide LAN management support above the adapter level for user workstations and the 8230 CAU.

LAN Station Manager with LAN Network Manager 1.1 provides the following benefits to SNA network administrators:

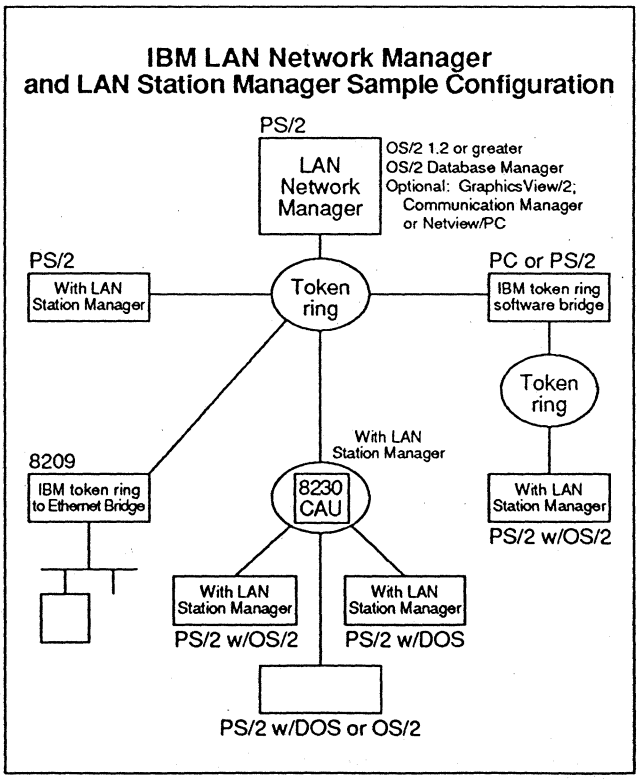

Figure 3

- OSI network management protocol between LAN Network Manager and LAN Station Manager
- Availability of data on SNA user hardware and software environments for asset management, capacity planning, and SNA user station management

User Interface and Configuration

SNA Perspective sees the LAN Network Manager setup, configuration, user interface, and management options as a great improvement over IBM's LAN Manager 2.0.

The main menu user interface of LAN Network Manager is built on IBM's OS/2 Presentation Manager. The network administrator accesses pull-down menus called System, Events, and Resources (see Table 2 on page 11). An OS/2 command interface is provided for developing automated software management programs.

Configuration can be done manually or via the discovery process of the token ring protocol. Data is stored using the OS/2 Database Manager and can be accessed in any of three ways: pull-down menus, the programming tools of the OS/2 Query Manager, or IBM's GraphicsView/2.

Setup requires LAN Network Manager system and adapter configuration. Then the system is booted up and the token ring discovery process takes over to learn the specific LAN configuration and store it in the OS/2 Database Manager. From the OS/2 Database Manager's adapter and profile information, the IBM GraphicsView/2 product creates a color topology map of the network.

Graphics Options

Using LAN Network Manager with IBM's GraphicsView/2 provides network administrators with a graphic representation of the network. The LAN can be displayed at the LAN, LAN segment, and LAN access unit/lobe levels. Colors are used to highlight the status of network devices and interfaces. Network administrators can edit the topology map to directly reflect their LAN physical layout. When a status change occurs on a device or an interface, LAN Network Manager signals users with an

alarm and a color change on the network map. The system immediately logs the change, including the date, time, and type of device, into the database.

Areas of Focus

This article analyzes the following features of LAN Network Manager:

- Configuration management
- Security management
- Fault management
- Bridge management
- NetView support
- Standards-based network management

Configuration Management

Configuration management allows network administrators to manage the physical layout of the network and its components. LAN Network Manager manages its own configuration as well as the configuration of the IBM 8209 token ring to Ethernet bridge and the IBM token ring PC bridge software. LAN Network Manager can configure the IBM 8209 and IBM PC bridge through the LAN bridge parameters accessible from LAN Network Manager's main menu. Some of the accessible token ring parameters include ring data rate, IPX support, forward delay, hop count, frames lost thresholds, and notification interval.

Network administrators will find the following information stored in the LAN Network Manager database:

- A list of all LAN adapters and their current status
- Station, bridge, and 8230 CAU definitions
- Station locations
- The event log

The options provided by LAN Network Manager to access this information are given in Table 2.

LAN Station Manager provides physical and environmental configuration and system information relative to each DOS and OS/2 LAN-attached workstation which is of special interest to technical support staff, capacity planners, and network administrators (see the sidebar "LAN Station Manager").

LAN Network Manager (LNM) Options

System
LNM adapter configuration
Bridge auto-linking, table size
Host NetView connection setup
Adapter timeout/trace authorization
LAN access control setting
Local alert filters definition
Local event filters definition
Security ON/OFF, password
LNM program password
Restart LNM adapter
Exit LNM

Events
Display event log
  Delete event
  Refresh log
  View selected events
Log configuration changes for LAN segments
Set soft error log options
Clear event log

Resources
Segments, stations, bridges, CAUs
  Display all
  Locate
  Add, query, delete, modify
  View sorted list/status
  Refresh status
  Display, profile
Stations only
  Disk drive capacity
  Hardware/software environment
  Workstation adapters
  Attachment data—TR, CAU
Segments only
  Data wrap test
Bridges only
  Link/unlink bridge
CAUs only
  Enable program update

Table 2

LAN Network Manager can use information stored in its database to perform extensive configuration management tasks:

- Update tables on receipt of adapter address insertions and removals
- Resynchronize the tables for LAN devices on a single segment or the entire network after a user-specified interval
- If access control is active, verify this information for each station as it enters the network or during resynchronization
- Delete inactive adapters from the database after a user-specified period

Using IBM's OS/2 Database Manager to store configuration management data, the SNA community may now expect third-party development of local automation and LAN management capabilities using the OS/2 Query Manager and the local automation facility. Possible products could include LAN access management, capacity planning, LAN network device performance, security management and timed station access, and workstation hardware/software management (e.g., operating system version query or SNA user disk capacity management).

A surprising feature is that a SNA network administrator can configure most LAN Station Manager parameters over the network via LAN Network Manager and NetView. Configuration options include workstation location, display, printer, and keyboard type, display, printer, and keyboard serial number, CAU number, and network access times. Display options include disk drive capacity, all configuration options, a workstation-installed adapter list, CAU connection information, and CAU attachment data. This capability can save a lot of time, especially in the area of asset management.

Security Management

Security management prevents unauthorized users from accessing network resources. LAN Network Manager, working with the 8230 CAU and LAN Station Manager, can control access to the ring.

LAN Station Manager

LAN Station Manager is IBM's station management tool for DOS and OS/2 workstations. LAN Station Manager software starts operating automatically when the workstation is turned on. With the December 1992 release of LAN Network Manager 1.1, SNA network administrators will be able to manage the SNA users' hardware and software environment. In addition, LAN Station Manager provides a user interface for customized station management.

LAN Station Manager offers the user several benefits. The network administrator can now track users' physical and environmental data. For example, LAN Station Manager will track what is in each slot of the machine via the internal storage of information captured when the PS/2 system was configured using the IBM installation reference diskette. Items like disk drive capacity and OS/2 version will be automatically available. Other information—such as,office number, telephone number, user name, machine serial numbers, and building number—must be entered via the user interface and can be tailored to the customer's specific needs by the network administrator. It will be apparent to SNA network administrators that one possible use of LAN Station Manager will be inventory management.

Previously, a subset of LAN Station Manager software was shipped with the 8230 CAU and provided security, access control, and station management. This product is based on the old heterogenous LAN management (HLM) protocol developed by 3Com and IBM (see *SNA Perspective*, February 1992). With the latest release, IBM introduced LAN Station Manager support of CMOL, which is a subset of HLM. CMOL can be used for management of various media and devices, including token ring, FDDI, and Ethernet. This gives IBM the option to develop and support Ethernet media and devices using LAN Station Manager. *SNA Perspective* believes IBM will adapt LAN Station Manager software to other platforms, including servers, bridges, routers and hubs. In addition, *SNA Perspective* expects that the station management code in the 8230 will be upgraded to support the new standard. ■

Authorization by Configuration

The CAU helps users control access on the network by maintaining detailed configuration information. This information can be used by LAN Network Manager to enable/disable 8230 ports so that only authorized users have access to the network. Access authorization may be based on adapter address, CAU ID, attachment module ID, CAU port number, time of day, or day of the week. For use with this function, LAN Station Manager can provide to LAN Network Manager detailed station location and identification information, such as office number, telephone number, machine serial number, and building number.

When a CAU-attached adapter is inserted into the network, the CAU and workstation LAN Station Managers report their respective station identifying information to LAN Network Manager, which compares the data to information stored in its database. Any discrepancy may result in the generation of an alert. The network administrator can then either remove the adapter from the network or disable the lobe at the CAU so that the adapter cannot be reinserted without operator intervention. The network administrator may also choose to use this alert option for inventory tracking purposes.

Password

The optional password security feature also helps prevent unauthorized use of the network. Information for creating an audit trail of stations and bridges entering and leaving the network may be queried from the LAN Network Manager database via the OS/2 Query Manager.

These features provide LAN access, control, and security management, all much needed capabilities for token ring users. The asset management information provided via LAN Station Manager will be useful to network administrators who want to perform corporate asset management through the LAN.

Fault Management

Fault management enables detection, isolation, and correction of network problems.

CAUs

For the CAU, LAN Network Manager can increase network availability by providing automatic recovery from a cable or access unit failure in a token ring network. The CAU provides an automatic hardware wrap reconfiguration of a failing ring segment, failing lobe, failing lobe access module (LAM) of the 8230, or failure of the entire 8230. In addition, if a cable between two CAUs breaks, the CAU provides an automatic wrap around the failure. A software wrap capability for troubleshooting and reconfiguration of a failing ring segment is provided on request from LAN Network Manager.

Bridges

Working with bridges, LAN Network Manager can display status information, modify bridge definitions, display bridge profiles, refresh status information, and link/unlink network bridges. Linking to bridges can be done automatically when they become operational after a failure. From LAN Network Manager, the customer can view bridge adapter status, ring status, frame transmission and receive counters, frames discarded count, route status information, and other performance information. LAN Network Manager receives error reports about remote LAN segments from the linked bridges on those LAN segments and reports errors it detects on the remote LAN segments.

Workstations and Segments

Working with LAN workstations and segments, LAN Network Manager can display status information, modify station definitions, display adapter profiles, and refresh status information. Token ring station information can be viewed by LAN segment or individually. From LAN Network Manager, network administrators can view station error codes, ring station address, and information on addressing, state, and attachments. LAN Network Manager can also execute a data wrap test over any network segment.

In addition, LAN Network Manager provides recovery notification messages for alerts when the device that caused the alert becomes operational again. If required, LAN Network Manager can also update the program code in the CAU.

Problem Determination

Network administrators need several capabilities to perform token ring LAN problem determination. They need to be able to verify token ring media connections, check software and hardware configurations, verify that the correct hardware interface signals are occurring, send and receive test messages across the network, access performance levels, and perform protocol analysis or trace analysis.

LAN Network Manager provides many of the above capabilities but a significant limitation is that trace analysis cannot be performed directly from LAN Network Manager. Customers must also purchase the Trace and Performance (TAP) tool. Further, the TAP tool requires a trace and performance adapter which costs $200 more than the basic token ring adapter because of special chips and software. *SNA Perspective* believes that most customers want trace analysis to be built into LAN Network Manager. In addition, a pull-down menu dedicated to fault management, as some other vendors provide, would be useful.

Automation Tools

The product is shipped with several automation management tools based on the SQL database and the OS/2 Query Manager. SNA network administrators may want to build their own custom management programs in order to manage their specific network environments. This process is complicated and requires the network manager to become familiar with OS/2 Query Manager, the operation of named pipes, C programming with the SQL interface, and LAN Network Manager events and status log details in order to write custom automation programs. Possible uses for additional automation tools include:

- Correlation of network alerts and their resolution in the database
- Management of token ring performance via bridges
- Automated notification of unauthorized network access by a LAN workstation or bridge

One limitation is that LAN Network Manager has no automatic screen and status refresh capability when monitoring status information on a LAN segment, bridge, CAU, or workstation. To update status information, the user must select the refresh option for the management area being viewed.

Bridge Management

Bridge management is the ability to monitor status and performance of interconnected LAN segments. LAN Network Manager allows users to manage up to 255 bridges. Up to four LAN Network Manager stations can be connected to each bridge, with one designated as the controlling station and the others as monitoring stations.

Users can set or reset LAN bridge parameters from the controlling LAN Network Manager console. All bridge addresses must be defined in the bridge definition table of LAN Network Manager. Users can add or delete entries in the bridge configuration table, monitor status information, and collect performance information relating to token ring and Ethernet networks. Ethernet port performance data includes the number of network collisions, late collisions, CRC errors, and framing errors. Token ring port status and performance data includes: ring data rate, ring status, and hop count as well as frames transmitted, received, discarded, and not routed.

Users can generate an alert or remove any bridge accessing the network that is not listed in the bridge definition table. Users can also instruct LAN Network Manager to generate an alert based on various status and performance conditions. For example, if the Ethernet bus to which an 8209 bridge is attached becomes inoperative and then recovers, LAN Network Manager can be used to report and log bus status. An alert can also be generated based on the automatic link option for bridges. LAN Network Manager will automatically link with specified bridges at startup time and reestablish a link to a bridge following a link failure.

No 6611 Support

Surprising to many, LAN Network Manager does not directly manage the IBM 6611 bridge/router. The 6611 can, however, pass through requests from LAN Network Manager and return response information from the downstream links, adapters, workstations, and CAUs. For direct 6611 management, SNA network administrators must use the Simple Network Management Protocol (SNMP) provided on products from several vendors, including IBM's NetView/6000 on the RS/6000.

Customers wonder whether the 6611 will be adapted to be manageable by LAN Network Manager or, alternatively, whether LAN Network Manager will be adapted to manage the 6611. Another option could be enhancing NetView/6000 with the ability to manage token ring devices and thus replacing LAN Network Manager.

SNA Perspective believes that the 6611 will continue to be managed through SNMP. We do not perceive an intention on IBM's part to upgrade the LAN Network Manager to manage the IBM 6611 or any other SNMP product. However, we expect that the capability to receive LAN Network Manager data will be added to NetView/6000 and perhaps to future products on other platforms. We expect IBM to attempt to clarify these and several other elements of confusion in its LAN network management strategy before the end of 1992.

NetView Support

LAN Network Manager permits management of multisegment token ring LANs from a central IBM NetView host. This capability requires the installation and operation of IBM Communications Manager or NetView/PC in the same workstation as the LAN Network Manager (see Figure 4).

Starting with Version 2 Release 2 of NetView, the number of LAN Network Manager command options executable from NetView will increase from eleven to over a hundred. All local LAN Network Manager options shown in Table 2 are now available from NetView. In the previous NetView release, NetView would parse and process the eleven commands that were available for LAN management and then send them down to LAN Network Manager. With the current NetView release, all LAN Network Manager commands are forwarded directly to LAN Network Manager for execution.

Alert filtering is provided both by LAN Network Manager and NetView. All LAN Network Manager alerts are logged into the local database regardless of whether the host connection is up. When the host connection is available, only requested alerts are forwarded to NetView, which reduces the flow of LAN error and status information. Both predefined and custom LAN filters are available in NetView and LAN Network Manager. As a convenient feature, LAN Network Manager filters can be selected, created, or modified remotely by NetView.

Using NetView V2R2 along with LAN Network Manager Entry enables customers to remotely manage single-segment token ring or PC network LANs. LAN Network Manager Entry cannot locally manage the LAN—it must interface to NetView.

To set up LAN Network Manager to operate with NetView, the network administrator enters the name of the SNA Service Point for the NetView connection and selects Communications Manager or Netview/PC as the transport medium for host communications. When the Communication Manager or Netview/PC are active, the interface between LAN Network Manager and NetView is automatically established when the LAN Network Manager application is started. During operation of LAN Network Manager, a message is displayed on the main menu to show whether the communications link is up or down.

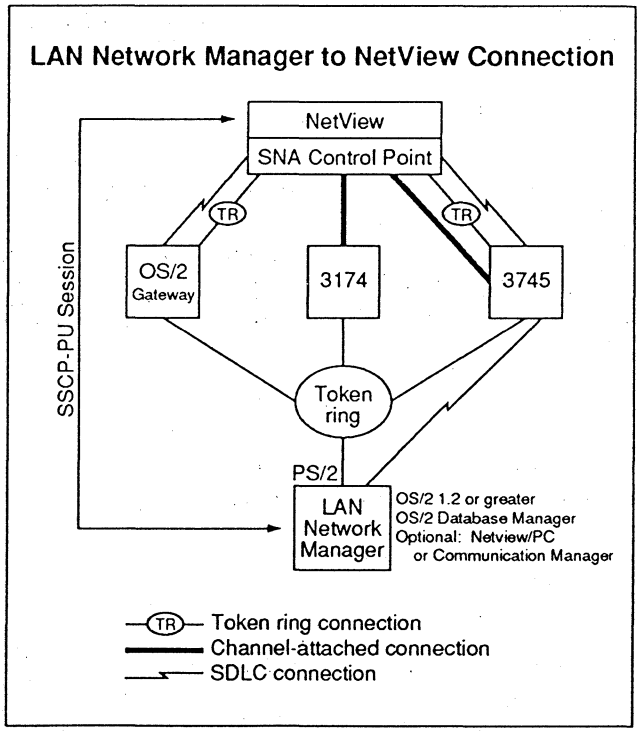

Figure 4

Typically, SNA customers use a 3745 communication controller or a 3174 cluster controller to connect the host system to the token ring for data flow. They dedicate a dialup or leased-line SDLC connection for LAN management from NetView, although NetView also could be accessed through the token ring. If the same token ring segment is used for both the host connection and LAN Network Manager, this can present a problem. If a failure occurs with the token ring LAN segment, it would not be possible to diagnose it from NetView. Ideally, SNA customers can install a backup SDLC dialup or leased line connection for operation of LAN management from NetView.

The management services provided between NetView and LAN Network Manager use alerts over a 3270 SSCP-PU session. With all the attention IBM is giving to APPC and APPN and since APPC support was added to NetView in 1991, *SNA Perspective* wonders why LAN Network Manager does not use APPC to relay alerts and LAN management data. The existing LAN Network Manager alert transport services use the SSCP-PU session and modifications would be required in the transport mechanism to move the alert data to the host via APPC. Perhaps IBM has its hands full getting this delayed product to market with the features already promised, so APPC support is not likely to be here soon.

One issue with communication between NetView and LAN Network Manager is that problems are reported but resolutions are not. LAN Network Manager forwards alert information to NetView to report LAN media or device error conditions. However, when these error conditions are corrected, LAN Network Manager records the corrective actions as "events" and these events are not forwarded to NetView. Thus, the NetView operator can view error conditions occurring on the LAN and take corrective action to fix the problems, but receives no acknowledgment of the resolution of the problem. (For large IBM customers, a possible solution is to use the LAN Automation Option—see the sidebar "LAN Automation Option.") *SNA Perspective* believes IBM will address this problem in a future release of NetView and LAN Network Manager.

LAN Automation Option

For large customers, IBM provides the LAN Automation Option (LANAO) so network operators can manage token ring LANs from a single NetView terminal. LANAO operates on top of the Automated Network Operations/MVS software. With LANAO, network operators can perform the following functions:

- Passively monitor the LAN for exception conditions—beaconing rings, unlinked bridges, bridge congestion, critical adapter failure, LAN Manager alerts
- Automatically detect failed components using the Recovery Monitor to look for LAN error conditions at user-defined intervals, recover from bridge failures, and provide operator notification and reminders
- Actively monitor LAN resource, path, and segment availability, as well as resource additions to the LAN

LANAO provides a menu driven and a script-based programming interface for reacting to error or status conditions reported by LAN Network Manager. The operator or script can monitor a problem via a query request to get updated status information.

SNA Perspective believes the LANAO option to be valuable for monitoring alerts and events reported by LAN Network Manager. However, to operate LANAO, the customer needs to have MVS/ESA or MVS/XA, NetView Release 3, VTAM 3.3, Automated Network Operations/MVS 1.0, and TSO/E 2.1, as well as LAN Network Manager. This means that SNA customers must already have a significant investment in IBM hardware and software in order to make this a viable LAN network management option. ■

NetView's Role in LAN Management

IBM expects that its customers will be divided on the network management platform choice. For those customers who wish to continue with their investment in mainframes, IBM will develop management products that interface with host NetView, IBM's flagship network management product. For customers who are decentralizing or downsizing, IBM provides NetView/6000, which is an SNMP network management product and *not*, as some misconstrue, a Unix-based version of NetView.

Standards-Based Network Management

Standards-based network management allows for multiprotocol, multiplatform, multimedia network management. Many IBM customers support several LAN types and want network management over all of them.

However, in token ring 802.5 and 802.2, media-level management frames only flow on a single ring. These frames cannot directly travel across a bridge and require a proxy or management server in order for them to travel to remote or downstream token ring segments. In addition, a separate set of management flows exist for IBM token ring bridge management. This management implementation is specific to token ring media operation and will not work in multiple media environments.

CMOL

With LAN Network Manager, IBM unveiled the use of OSI-based network management for the transfer of station management data between LAN Network Manager and LAN Station Manager. This is based on OSI's Common Management Information Protocol (CMIP). IBM and 3Com adapted CMIP to manage LAN logical link control (LLC) protocols for token ring, and Ethernet, and other LAN media. IBM calls this CMIP over LLC or CMOL (IEEE 802.1B). The IEEE executive board is expected to cast a positive vote in June for 802.1B.

With the implementation of CMOL, IBM can use an LLC standard that is media-independent and is designed to support some of the OSI CMIP management constructs. However, it should be noted that CMOL management is currently used only between LAN Network Manager and instances of LAN Station Manager.

Not for Ethernet or FDDI

Because of its generic name, many users wonder whether LAN Network Manager will be enhanced in the future to provide Ethernet support. *SNA Perspective* does not expect this to happen. LAN Network Manager technically can be extended to support other media types because of IEEE 802.1B. This would primarily involve assignment of a new MIB and development of new software on the management side to understand this MIB. However, we believe IBM, instead, intends to manage Ethernet media and devices via NetView/6000 and other unannounced products (discussed below) and will continue to use LAN Network Manager for token ring.

FDDI will not be managed by LAN Network Manager either. In May, IBM announced several FDDI products and stated that these would be managed through NetView/6000, using an IBM FDDI Proxy Agent Program to translate between the FDDI standard station management and SNMP.

NetView/6000

NetView/6000 is IBM's version of Hewlett-Packard's OpenView software. NetView/6000 is *not* an implementation of NetView on the RS/6000; rather, it is an SNMP-based network manager.

(continued on page 20)

LAN Management through LAN Network Manager, NetView/6000, and NetView

Platform	Operating System	Management Application
PS/2	OS/2	LAN Network Manager (CMIP) Supports token ring media and devices
RS/6000	AIX	NetView/6000 (SNMP) (based on HP OpenView) Supports Ethernet media and devices
S/370 S/390	MVS, VM	Enterprise NetView (proprietary architecture) Can manage token ring via LAN Network Manager 1.1 Can manage Ethernet via NetView/6000

Table 3

Architect's Corner

Internetworking SNAerobics

by Dr. John R. Pickens

In case you had not noticed, SNA just experienced a lifestyle change. Gone are the days of sedentary decay. Newly arrived is a healthy diet and conditioning aerobics. Despite the competing technopolitical environments—TCP/IP and OSI—of which SNA is a peer, I foresee SNA being a healthy competitor for years to come. Now, more on the metaphor.

Getting in Shape

The architecture goals of SNA are many, but key among them is providing the foundation for a scaleable, robust internetwork which meets the networking requirements of users' computing environments. The process of achieving this goal can be likened to the process of achieving physical fitness—without continual exercise (evolving protocols), the body will decay (stabilize). Proper diet must be adhered to (standards, technology); counterproductive activities must be discarded (subarea, old hierarchical protocols). An exercise regimen (architecture direction) of sufficient intensity (de facto standards pace or better) must be adhered to consistently. A sustained aerobics program can result in a healthy body capable of competing in marathon competitions (internetworking).

I remember, in recent years, bemoaning the lack of significant public technical developments in SNA. SNA internetworking had seemingly gone to sleep—the fate of the couch potato. (Monitoring SNA was not as dull as, say, watching paint dry, but it came perilously close.) Subarea networking was, realistically, the only regimen in town. Practicing networkers still focused on its care (tuning) and maintenance (fixed routes). Much ado had been made about the new (fad) architecture regimen—APPN—but not with much sustained activity. At least one major internetworking vendor misread this "stable" state of affairs and committed to replicating the old sedentary subarea way (a move that has since been retracted).

SNA More Active

But recently it seems that the activity level for SNA internetworking has stepped up a notch, or even several notches—both in architecture and in products. What does this say for the long range health of SNA? Is SNA finally operating within its target heart rate?

Consider several recent announcements:

- APPN end node (EN)-network node (NN) open specifications
- APPN NN-NN licensed source code
- SSCP-SSCP flows obsoleted by APPN flows
- APPN/MVS
- Composite NN—VTAM and NCP
- Sockets-over-APPC, CPI-C-over-TCP
- CMIP-over-APPC
- IBM Information Network—Architecture Mall
- Border node—NN version
- APPN revealed to be LU 2 capable
- Dependent LU server (SSCP-LU, SSCP-PU)
- Central directory server—100,000 node networks
- NS/DOS—small DOS version of APPC
- Data Link Switching (DLC-to-TCP tunneling and SDLC-to-LLC2 conversion)

Future Moves

Everyone, including IBM itself, is abuzz about several more upcoming announcements, some imminent and some more long range:

- Remote procedure call, message queuing interface
- Protocol-independent security
- Converged OSI-TCP-SNA transport layer semantics
- Full-duplex APPC
- Third-party session initiation
- APPN+ and gigabit APPN
  - Multicast routing
  - Spanning tree control flows
  - Rate-based flow control
  - Block versus byte transfers
  - Queues at edges
  - Nondisruptive route switching
  - Multiroute connections
  - Fixed/variable cell switching (ATM, PARIS)

Whew!

Is this sweat and muscle? Or is it just arm flapping? What does it all mean?

The Global SNA Internet

Well, a few points are worth highlighting. I believe that IBM is coming close to enabling the global SNA internet—an internet characterized by contemporary generation protocol architecture (link state routing, peer flows, security, and class of service enhancements) and capable of providing service to most SNA session types (LU 6.2 directly and the rest through dependent LU servers).

Many other elements are significant—such as OEM licensing of APPN, directory services enhancements, and CMIP. The runner-up for most notable development is the dependent LU server. But the winner may be APPN/MVS and its effective obsolescence of SSCP-SSCP sessions. The claim (if it is to be believed) is that use of the new APPN flows actually *reduces* resource consumption on mainframes versus what was previously required for network supervision, especially because of the directory caching characteristics of APPN. In addition, it makes possible the deployment of mainframes in even lower-resource configurations by being APPN end nodes, which leaves more cycles for DBMS servers. This is a major tactical and strategic move. I suspect the impact of APPN/MVS on internetworking will be similar to the impact of mainframe-to-token-ring support on the LAN market—everyone will want APPN routing.

Putting Words Into Action

So, with all this muscle flexing and architecture exercising, is IBM up to speed with SNA? Up to the target internetworking heart rate?

Not quite. Much of what is announced is still just that—announced. Some is no more than a hint.

IBM must deliver on its APPN strategy. Multivendor, multiprotocol routers need to be delivered and deployed. Key improvements are needed—the migration toward protocol independent security, toward datagram-oriented router-to-router flows, toward a more general n-level network naming hierarchy, and, ultimately, toward an integrated protocol-independent routing capability (and not its imitator—tunneling).

With the recent developments, SNA appears back on track, alive, well, and committed to getting in shape. With the hints of things to come, SNA appears poised for an energetic future. ■

(continued from page 17)

SNA Perspective believes that IBM will provide the capability for LAN Network Manager to interface to the NetView/6000 through the AIX NetView Service Control Point. We do not expect LAN Network Manager to be replaced by NetView/6000.

SNA Perspective believes that NetView/6000 will be enhanced to receive management data from LAN Network Manager. This interface could be accomplished in a method similar to the LAN Network Manager-to-NetView interface. We do not expect such an enhancement any sooner than eighteen months (see *SNA Perspective*, February 1992).

CMOL versus SNMP

Some wonder whether CMOL (IEEE 802.1B) implementation means that IBM is moving to support OSI rather than SNMP for LAN management. *SNA Perspective* believes that IBM will continue to support both. LAN Network Manager uses CMOL between LAN Station Manager and LAN network Manager and an IBM-proprietary interface between LAN Network Manager and NetView. IBM is building further support for the CMIP management architecture into LAN Network Manager. IBM provides SNMP through NetView/6000.

Conclusions

SNA Perspective believes LAN Network Manager functionality is a big improvement over the original LAN Manager product. We believe that LAN Network Manager will not be extended to manage SNMP devices or Ethernet networks but instead will remain focused on token ring.

LAN Network Manager 1.1 can be completely managed from NetView. The addition of the graphical user interface provides network administrators with a color topology map with which to monitor and service the LAN. The OS/2 command automation utility will be valuable in developing customer-specific token ring management capabilities. LAN Network Manager's asset management and control features combine with LAN security to give the network administrator tools to manage LAN station access and network device inventory control. LAN Network Manager can finally, in conjunction with LAN Station Manager, provide token ring station management above the adapter level and the ability to manage a device's hardware and software environment.

SNA Perspective believes that IBM will provide several additional network management features through LAN Network Manager, LAN Station Manager, OS/2 Communications Manager, and the OS/2 platform. Several items have been discussed in this article: CMIP LAN network device support, multiple media management, LAN device inventory control, APPC communications for transport of network management data, and operation across and support from multiple platforms including the mainframe, OS/2, and RS/6000.

IBM has indicated that it is developing an OS/2-based Distribution Systems Management platform that can support LAN Network Manager. Additional products may include a software distribution system, interoperation between multiple IBM system management platforms, and third-party tools to automate specific management processes (configuration, inventory control and management, asset management, access, and security).

There is much room for growth in IBM's LAN management product capabilities. There is also a need for a clear, comprehensive LAN management strategy, even if the strategy involves several products, protocols, and management standards. SNA users have been demanding that multiprotocol, multiplatform network management be delivered by IBM. *SNA Perspective* believes IBM will address several of these issues before the end of the year. ■