Communications Network Management enhancements for SNA networks: An overview

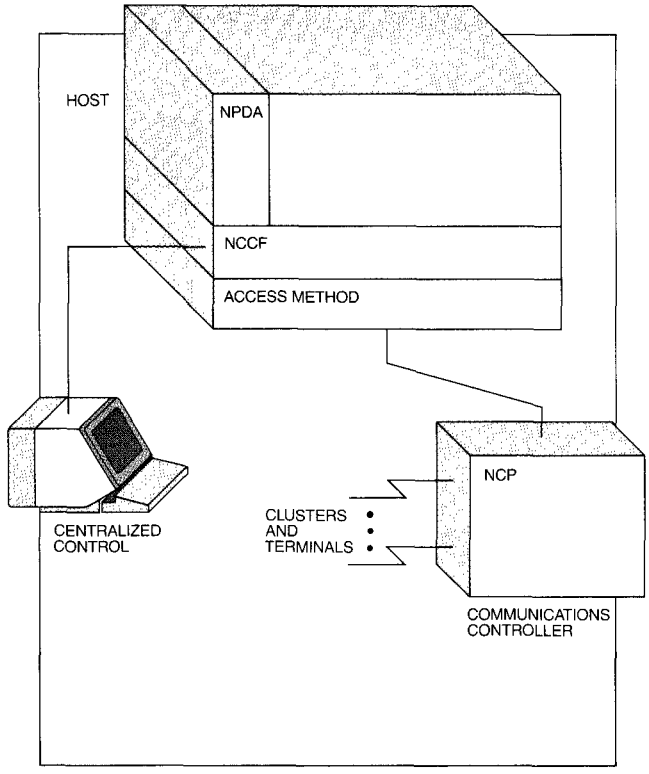
by T. P. Sullivan

Hierarchical growth and diversification of communications networks have imposed new requirements on Communications Network Management. This essay presents the evolution of support included in IBM's Systems Network Architecture to meet these needs. Four main provisions of network management are discussed: (1) the collection and presentation of downstream network data on behalf of network resources by a Threshold Analysis and Remote Access program; (2) centralized network operator terminal access to local and remote systems by a Terminal Access Facility; (3) unsolicited alerting of the network operator by the presentation of data from network resources by a Network Problem Determination Application; and (4) the collection and presentation of data for the logical network by a Network Logical Data Manager.

When Systems Network Architecture (SNA)[1] was first introduced in 1974, its functions supported single-system user data processing networks. In 1976, networking capabilities were added that allowed communication between hosts and allowed end users to communicate with multiple applications in multiple hosts. The variety of configurations made possible with SNA,[2] compounded by user network growth and geographical dispersion, highlighted the need for a Communications Network Management (CNM) capability. CNM is a set of tools, techniques, applications, and network functions that assist the customer in planning, operating, maintaining, and controlling an applications network. (An index of terms is given in the Appendix at the end of this paper.)

The user application network consists of processing hardware, application programs, communications software, communications hardware, and terminals. The application network is tailored by the network owner to provide functional capability necessary to his business. An example of such an application network is a data base/data communication system to provide support for banking transactions. Such a system provides the teller with current information on customer accounts, thereby allowing updates for deposits and withdrawals. The network might also provide a balancing mechanism for the teller's cash drawer. The same system might also support automated teller terminals to allow customer access to account information and services on a twenty-four-hour basis.

The function offered by such an application network is an integral part of the normal operations of the user community. When the system function is not available, customers are not served. If network



response is slow, customer service is also slow. This level of integration of application network function into day-to-day operations dictates a user application network that operates continuously. Continuous operation of a user application network requires a management system that recognizes and responds to problems in real time. In response to the customer's growing dependence on a supporting management system, the first CNM facilities supported by SNA protocols for gathering data were introduced in 1978. The Communications Network Management facility that was introduced in 1978 is shown in Figure 1.

The emphasis of this early support was that of centralized control. The base for the CNM function was the Network Communications Control Facility (NCCF)[3] that supported the execution of VTAM and TCAM commands and the receipt of network messages through a single terminal. NCCF also supported automated operator functions that expedited error recovery and improved operator productivity. The facility further provided access to an application through which the network operator could monitor, identify, and isolate network problems throughout a tree-structured network of SNA elements. This application was the Network Problem Determination Application (NPDA).[3]

NPDA was an application of NCCF that collected error statistics from hardware devices and presented the user with a hierarchical view of error activity. That is a view that was consistent with the hierarchical Systems Network Architecture (SNA) networks that were installed. The devices supported were primarily SNA devices. The collection of statistics was initiated by the host network operator, and the data were solicited from the network. NPDA provided an important first step in assisting customers with problem determination within their communication networks.

Continuous operation of a user application network requires a management system that recognizes and responds to problems in real time.

During the same time, SNA flexibility continued to expand. In 1979, major enhancements were made to support availability (multiple active routes, class of service, flow control, etc.) and additional configurations (dynamic configuration, parallel links, etc.). The network nodes that SNA defines could be configured into a large number of network topologies. Thus CNM was required to expand to keep pace with growing needs in managing customer application networks. Enhancements were required in the areas of downstream network management, operator access, alert generation, and logical data presentation. These requirements are described in the following section.

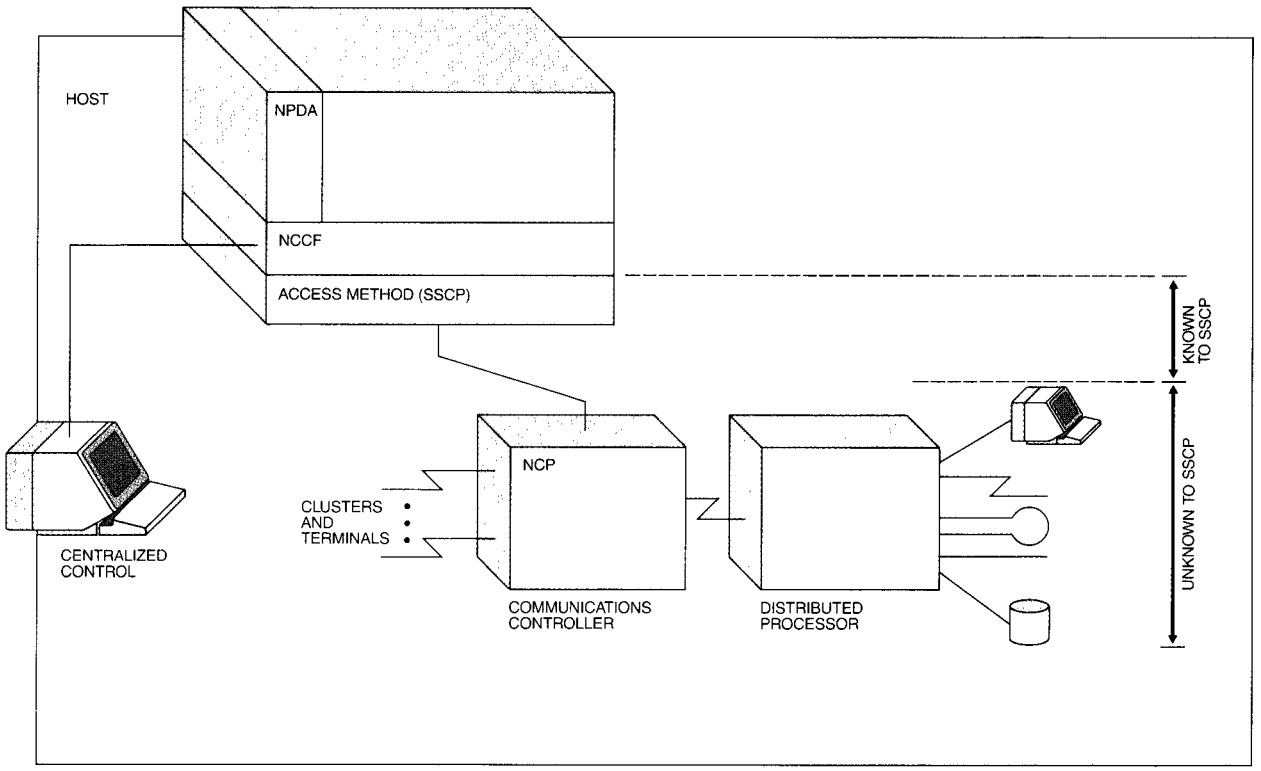
Required enhancements

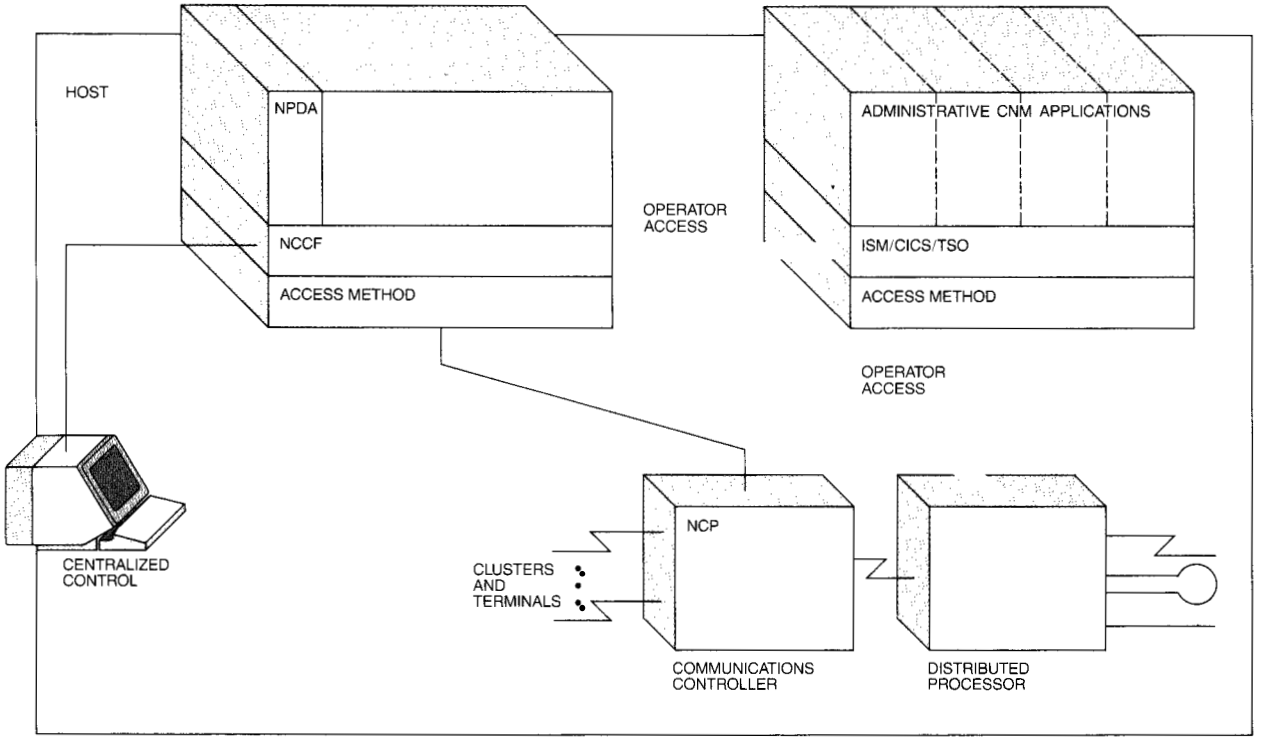
Downstream network management. In 1978, a single-system SNA network supported remote attachment of operator stations and remote execution of simple application programs. As more intelligent

controllers were attached to the network, they in turn supported attached stations of their own. With the addition of processing power, storage, and DASD, the controllers became small distributed processors. The controller and/or small distributed processor was known by a System Services Control Point (SSCP) of SNA, but the stations attached were not. The SSCP is the system component that delivered the SNA problem determination data to NPDA. The centralized control aspect of CNM had to be extended downstream as controllers and distributed processors connected in multilevel networks formed subnetworks of their own. Communications Network Management (CNM) data had to be collected for the resources outside the domain of knowledge of the SSCP and brought back to a single point in order to maintain the centralized control philosophy of CNM.

In the tree-structured network of Figure 1, a single SSCP controls the entire SNA network. The user application network parallels the SNA network, and no unique CNM extensions are required. In Figure 2, a subnetwork is attached, which itself has resources managed from its own domain. The SNA host has no knowledge of the resources downstream of this cluster controller that is utilized as a distributed processor. A user application subnetwork for which CNM support was required was an IBM 3600 Finance Communication System, with distributed applications and remote workstations that were unknown to the SSCP. In order for network management to remain effective, CNM data were to be

As more intelligent controllers were attached to the network, they in turn supported attached stations of their own.





collected on behalf of the resources downstream from the controller.

Operator access. In addition to extending CNM data gathering to the downstream subnetworks, remote operation of the distributed processor was required. The central operator needed the ability to re-IPL the processor, access its system log, run diagnostics, and so forth. Such capabilities would not only strengthen the centralized control philosophy but also save dedicated terminals and operators at the remote locations.

Since the entry of CNM on SNA, customers have augmented the dynamic data from the network (as represented by NPDA) with their own administrative applications. These are often referred to as problem and change managers, and they generally provide full-screen entry and presentation to track problems and to monitor approval cycles for the installation of new network elements, etc. These data are usually written by IMS or CICS application programs. The network operator(s) must interact with multiple terminals. This concept is illustrated in Figure 3.

Since these management system functions have no need to collect data from the network, and thus have no affinity for any particular SNA domain, they may be placed at any node that contains appropriate support capability. The management system functions may be accessed via normal SNA session protocols. The system administration functions, however, must be accessible from the NCCF/NPDA network operator.

In today's SNA environment, the network operator, in attempting to interact with a series of tools on various software bases, finds that there are two alternatives: (1) to dedicate separate terminals to each application so as to allow simultaneous interaction; or (2) to set up and take down individual terminal sessions (via logon/logoff). The dedicated-terminal alternative is an inefficient use of terminals. Individual terminal sessions can also be very inefficient and cumbersome when the operator must alternate between two or more applications to perform a given CNM function. Since network operations is a key CNM function, a solution that requires network operator logoff is unacceptable. Also, in a

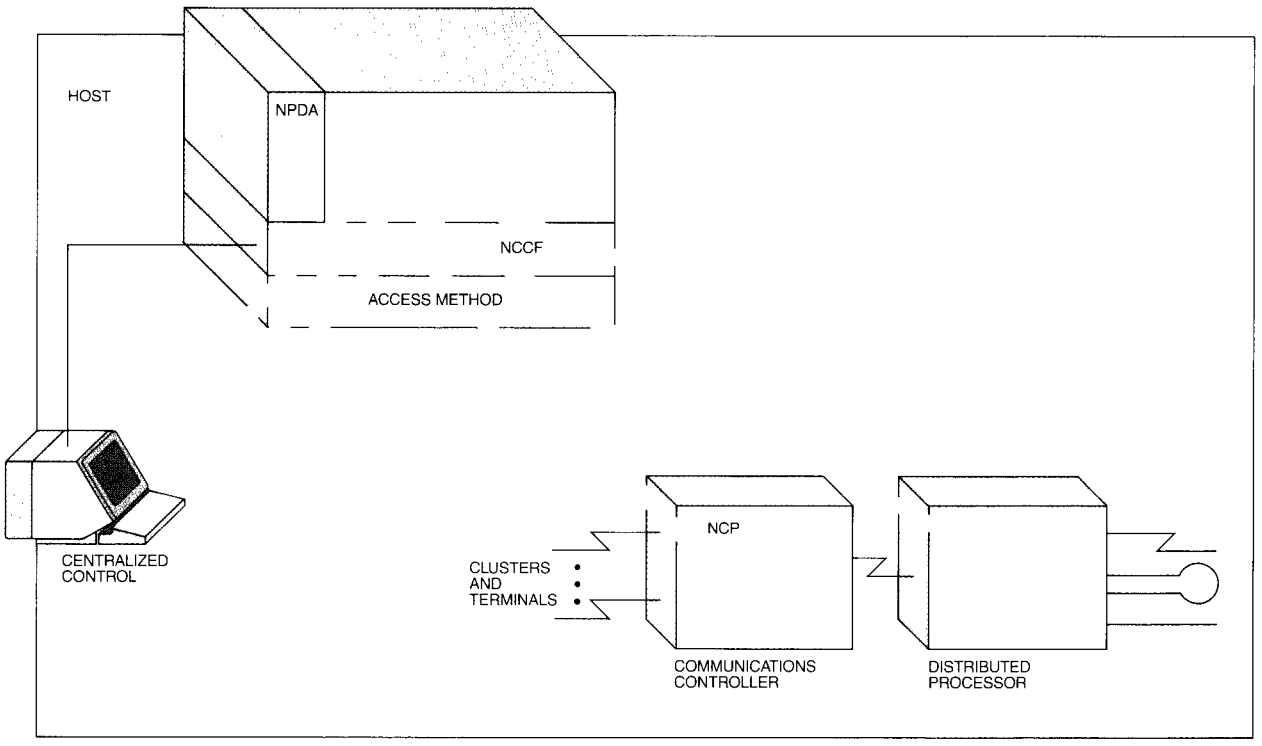
distributed network, remote operation of a multitude of nodes from a central point is required by certain users.

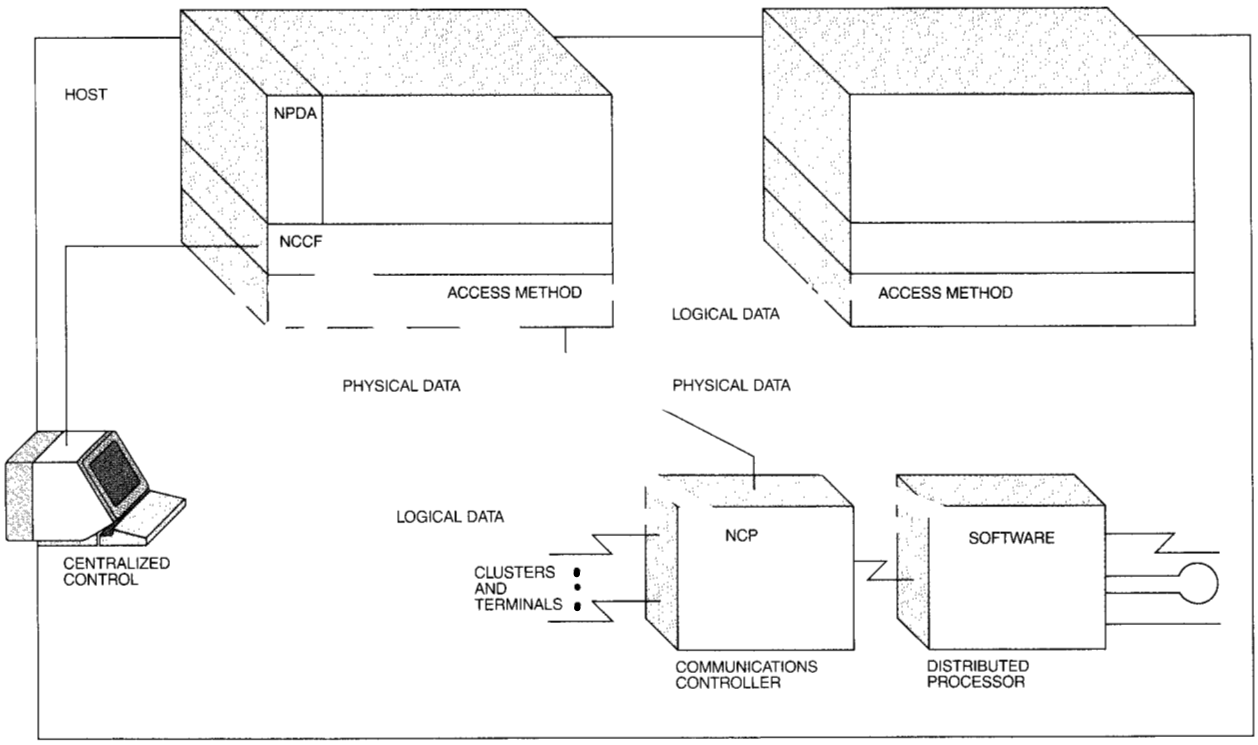
Alert support. The initial CNM support and the SNA protocols utilized solicitation as the predominant mechanism for gathering data. Solicitation was chosen primarily to control the volume of error data flowing in the network. The data were presented to the user, using the NPDA screens, to direct and allow the user to assess the hardware error status of a tree-structured network. Product-specific screens reported such errors classified as temporary, as communication line errors, or errors classified as permanent, indicating a nonoperational hardware element.

As SNA capability and customer networks expanded, the need to remove product-specific detail from the screens and the need for products to participate in the determination of the cause of the error increased. Data were required for resources downstream from distributed processors and data were required from software elements, in addition to the hardware data already provided. As functions were distributed to other processors in the network, the ability to filter data was also distributed. This reduced the earlier concerns with the volume of error data flowing to the centralized host.

As SNA capability and customer networks expanded, the need to remove product-specific detail from the screens and the need for products to participate in the determination of the cause of the error increased.

The emerging requirement, therefore, was for extensions to the SNA architecture and new CNM support for product alert generation and presentation of the collected data to the network operator, as shown in Figure 4.





Logical data. The error reporting, recording, and presentation mechanisms for CNM dealt with the hardware or physical elements in the network. The NPDA user viewed the physical network, which included information on the status of modems, links, and controllers.

Much of the customer network and much of SNA deals with the logical network.

Much of the customer network and much of SNA deals with the logical network. A logical conversation in SNA, which is called a *session*, may exist between applications or hardware products. When something fails in the logical network, stand-alone traces, storage dumps, or special traps may be required to determine the cause of failure. The objectives of CNM were to reduce the time needed and personnel skill levels required, and to increase the effectiveness of problem determination procedures. New CNM functions supported were required to provide an NPDA-like facility for the logical network. Status information on SNA protocols, SNA data flows, etc. were required, as shown for the configuration in Figure 5.

To summarize, the following four CNM extensions were required in support of SNA networks:

- *Downstream.* The collection and presentation of CNM data on behalf of network resources that were previously unknown to the SNA host.
- *Operator access.* Centralized terminal access to local and remote systems for the purposes of operator control and interaction with administrative CNM applications.
- *Alert support.* The unsolicited delivery of CNM data from network resources and subsequent presentation to the network operator.
- *Logical data.* The collection and presentation of CNM data for the logical network.

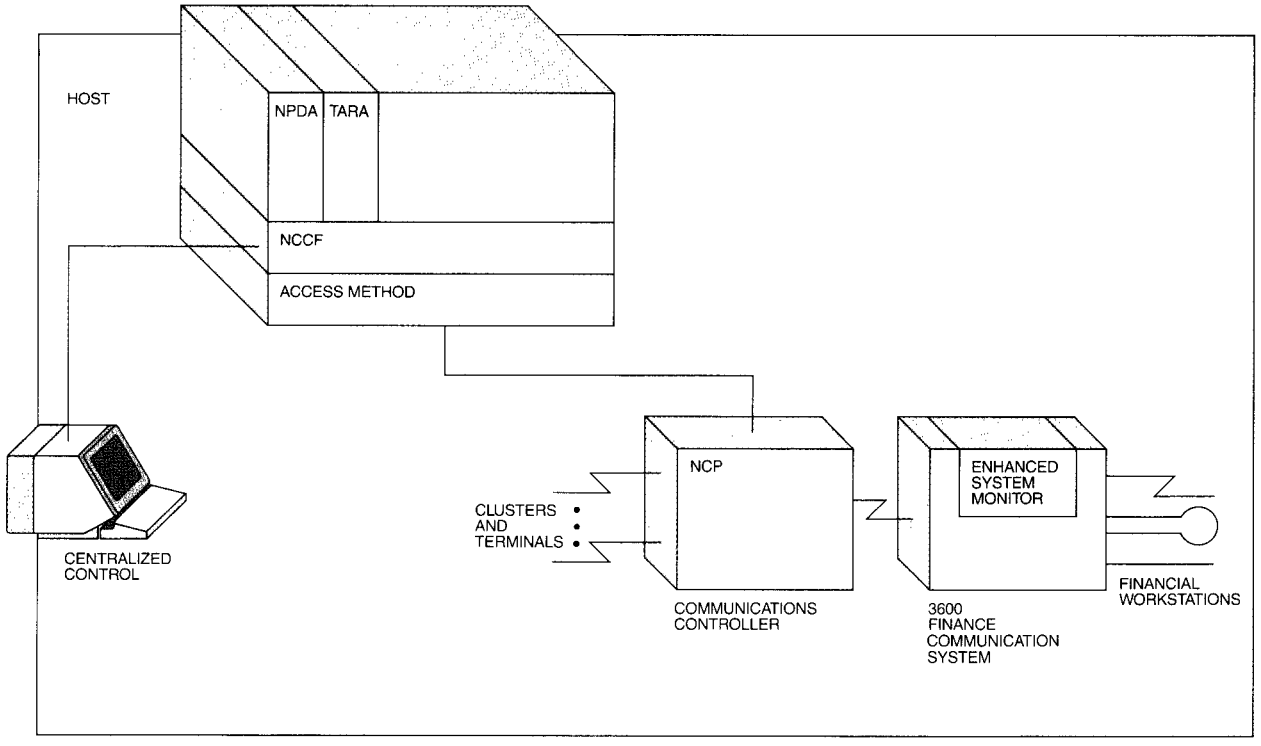
The next section describes the CNM extensions that were developed to satisfy these requirements.

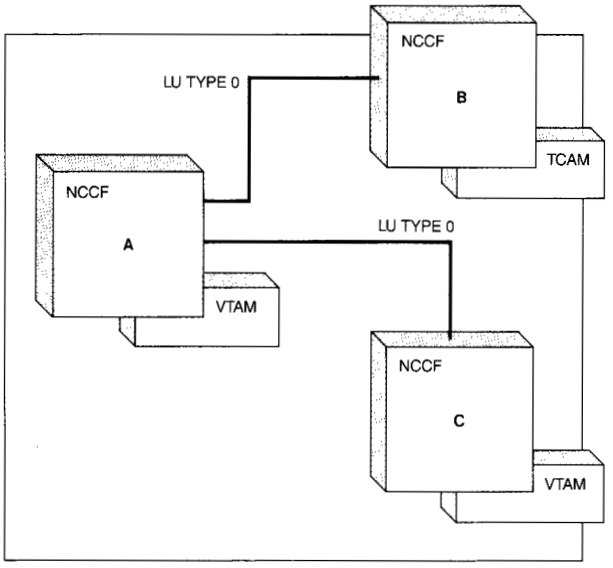
Communications Network Management enhancements

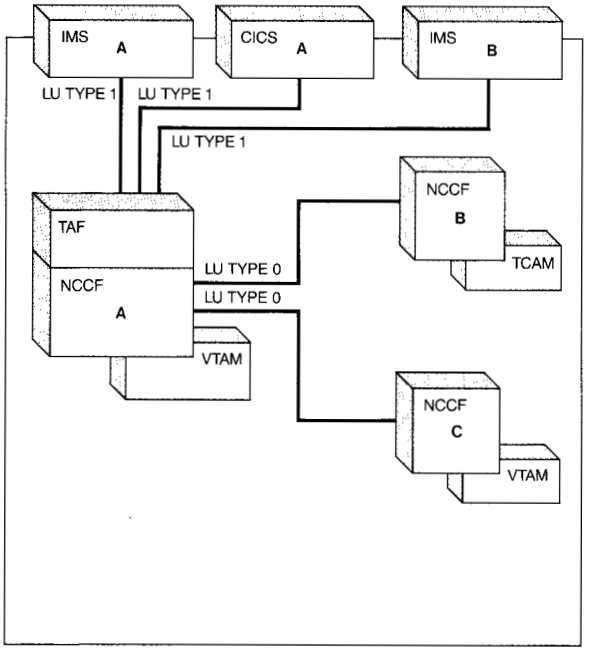
Downstream. Figure 6 illustrates the attachment of an IBM 3600 Finance Communication System to the SNA network. The resources in the 3600 subnetwork were unknown to the SSCP, thus limiting the CNM flexibility of the user's network. Centralized control of the 3600 downstream network was not possible from the network operator's terminal. Dedicated operators were required at each 3600 location, which was often a remote branch.

To satisfy the downstream requirement for 3600 subnetworks, a Threshold Analysis and Remote Access (TARA) program was developed as a feature of NPDA.[4] TARA supports the solicitation of CNM data from the downstream network via the SSCP-Physical Unit (SSCP-PU) session of SNA and extensions to the system monitor that resides in each 3600 controller. Data may be solicited by the network operator, but they are usually driven by the timer-initiated commands/Command Lists (CLISTS) facility of NCCF Release 2. The data include current operational parameters, the status of attached loops, basic and extended counters in the controller and response-time counters in the controller, and response-time counters for the defined workstations. Those data, which were previously unavailable, may now be displayed by the network operator. The screens are hierarchical and consistent with NPDA. The user network has been extended beyond the SNA-based network.

Both solicited and unsolicited communication are supported, and a correlation of requests to replies is provided, without compromising the system security.







Once network data have been collected, the host application—in this case TARA—may provide thresholding support where user-specified levels of error or performance information may be compared on a real-time basis, and the operator may be alerted when thresholds are exceeded.

In addition to data collection and presentation and threshold support, through the extended CNM facilities, local operator functions (IPL, etc.) may be moved to the remote host. TARA is an example of an extension of CNM facilities to downstream networks. Such an extension allows the user to manage more of the elements within an application network and provides the option of determining which element to distribute to local management.

Operator access. Operator requirements for access to CNM information and for network control led to the design and development of the Terminal Access Facility (TAF) feature of NCCF.[5]

To address the access-to requirement, TAF connects to a variety of full-screen, display-oriented network management tools that reside in a variety of software bases (IMS, CICS, TSO, and HCF). Since the user depends on NCCF to support operation control for VTAM and/or TCAM network environments, TAF ensures that messages are not lost while the screen is dedicated to a specific application. A message operator control interrupt and an easy method to swap between operator control and full-screen mode are provided.

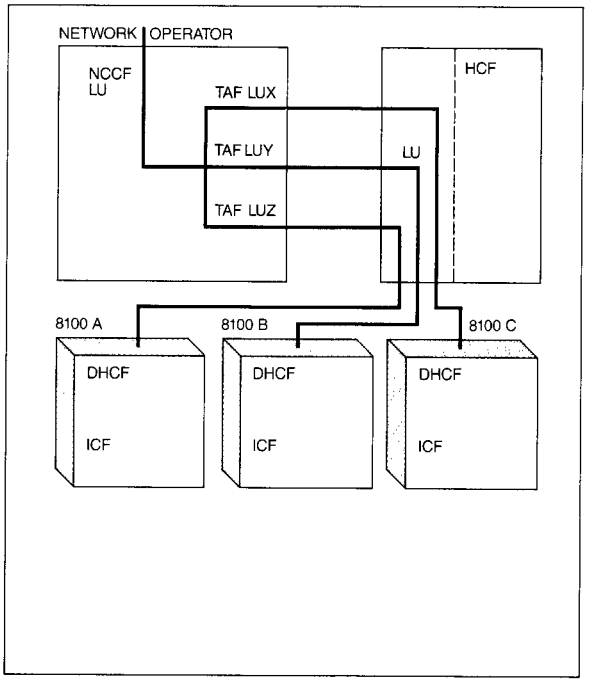
To address the control requirement, TAF combines access to CICS, IMS, and DPPX control functions with those provided by NCCF for VTAM and TCAM. Both solicited and unsolicited communication are supported, and a correlation of requests to replies is provided, without compromising the system security.

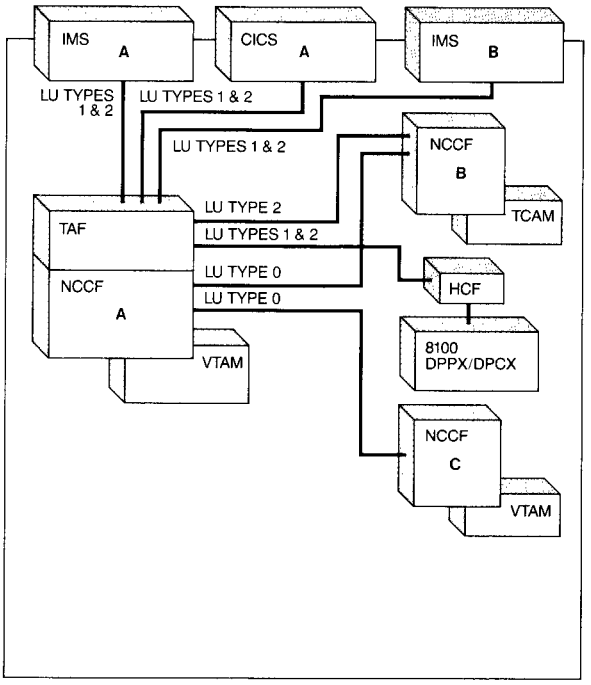
NCCF initially provided a wide range of functions in support of network operator control in a single- or multiple-domain environment. A programmed operator interface was utilized to provide NCCF-to-VTAM/TCAM communication. To support control of a multiple-domain network, an NCCF system is required in each domain, and a specific SNA LU-to-LU protocol (LU0) is utilized to allow an operator's span of control to include multiple SNA domains, as shown in Figure 7.

TAF extends the operator control environment of NCCF by establishing an SNA LU1 session with CICS and/or IMS subsystems. Since TAF functions as a Secondary Logical Unit (SLU) on an LU1 session, it appears as a 3767. No code modifications to CICS or IMS were required for the configuration shown in Figure 8.

Using an LU1 session to the 8100 Host Command Facility (HCF), the TAF operator has access to the Interactive Command Facility (ICF) in a given 8100/DPPX system. This provides remote control of that system from the operator's NCCF terminal. By utilizing the TAF facility to create multiple TAF LUs, multiple LU1 sessions to the same HCF may be established, with each session being capable of exercising control over a separate 8100/DPPX system. This allows network control of multiple 8100 systems, as shown in Figure 9.

The alert generated by the initiating component includes information concerning the probable cause of the event and recommended user-action codes.

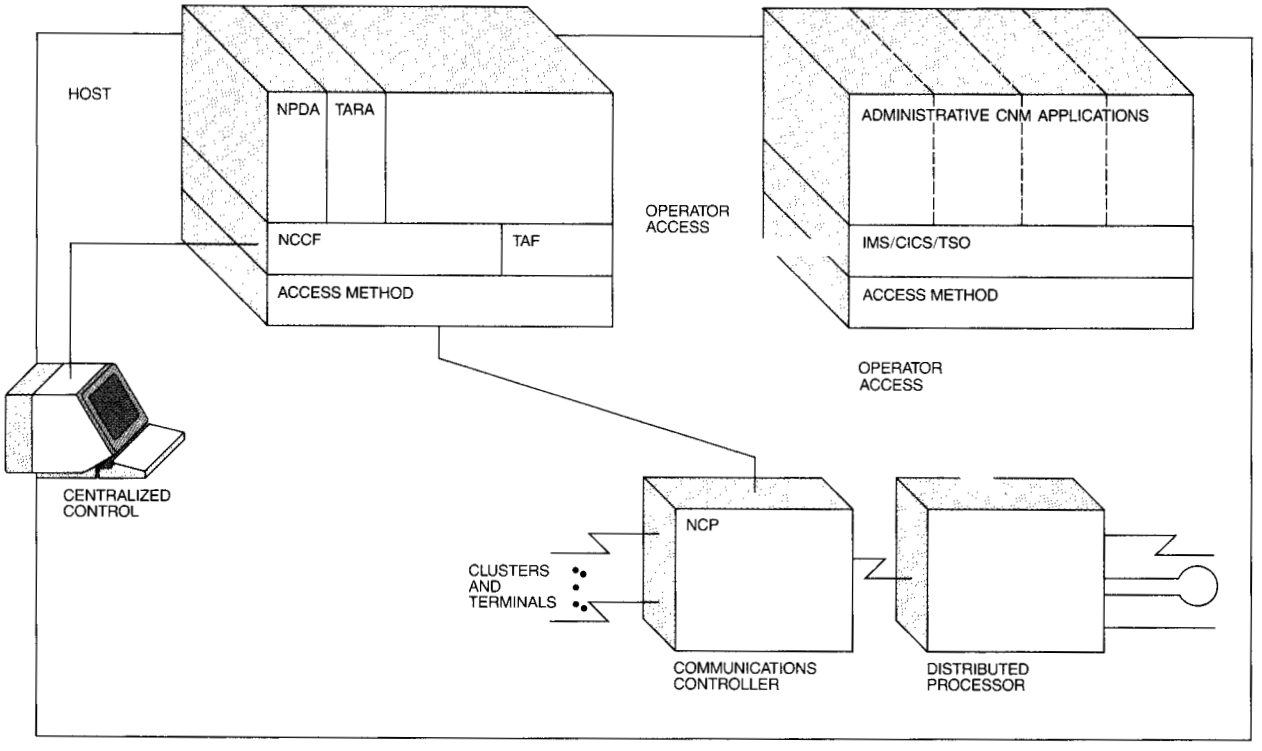


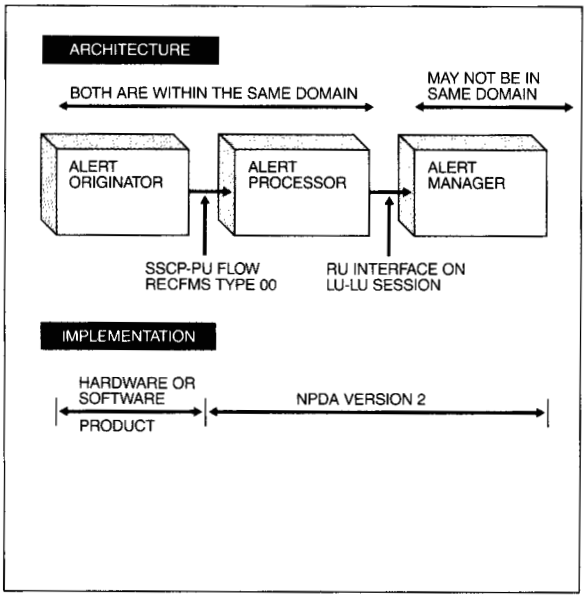


The full-screen mode of TAF, illustrated in Figure 10, achieves system coupling by establishing an SNA LU2 session with the destination system (IMS, CICS, TSO, remote NCCF, HCF). The establishment of the LU2 sessions is under control of the NCCF/TAF operator. When the operator is connected to the destination application, he will interact as though he were directly logged on. Various escape and reconnect options are provided to allow the operator or predefined CLISTs to access and control other network elements within and between the two modes of TAF.

TAF, therefore, addresses operator access requirement by utilizing existing SNA session support and linking to the network operator facilities of NCCF, as illustrated in Figure 11.

Alert support. A network architecture has been constructed and NPDA application support extended to alert generation by SNA components that are capable of recognizing an exception condition that warrants network operator attention. The alert generated by the initiating component includes infor-





mation concerning the probable cause of the event and recommended user-action codes. The alerts were designed to flow unsolicited from the SNA network elements over the SSCP to PU control flow. A Record Formatted Maintenance Statistics (RECFMS) Type 00 Response Unit (RU) was defined for this purpose.

From an architectural point of view, the alert originator communicates the alert to the alert processor, as shown in Figure 12. The alert processor is associated with the SSCP that controls the originator's node. The alert originator and alert processor may be combined in the same network resource. The alert manager may or may not co-reside with the alert processor. The use of an LU-LU session greatly reduces connectivity problems introduced by the several connection mechanisms utilized in SNA networks, since the common denominator of all such mechanisms is LU-LU session passthrough.

```
SEL#  DATE / TIME   TYPE   RES NAME   ALERT DESC;
                                      PROB CAUSE

[1]   11/12 15:30   CTRL   LOOP       LOOP IN OP;
                                      LOOP ADPT/MODEM

[2]   11/12 15:28   CTRL   PRINTER    PRT IN OP;
                                      PRINTER ADAPT
```

```
USER CAUSED:  NONE

INSTALL CAUSED:  NONE

FAILURE CAUSED:  LOOP ADAPTER
                 MODEM
                 STORE CONTROLLER

       ACTIONS:  D000 - If problem is store loop
                        1 or 2 follow your
                        store back up procedures

                 D143 - obtain FE data from
                        event detail
```

```
PRODUCT UNIQUE TEXT:  FEXX   XXXX   XXXX   XXXX

ERROR DESCRIPTION: The product unique text further
     identifies the nature of the problem


          PANEL MESSAGE

QUALIFIERS:  1)  DE01/DE02/DE03/DE04/DE06
```

Any network hardware or software may be an alert originator. CNM application programs can also generate alerts, as in the case of TARA. The receiver for both network- and application-generated alerts is NPDA Version 2.[6] The operator is provided with a hierarchical view of the network that is bounded by and reflects the alerts occurring throughout the network. This view is an extension of the initial NPDA view and includes lines, loops, and devices that are attached to cluster controllers. Also included are application alerts generated by customer-specified error/performance limits being exceeded. NPDA provides alert summary and detail screens and the related user action screens. Figure 13 illustrates sample NPDA screens for IBM 3650 retail controller alerts.

A combination of SNA architectural extensions to carry the unsolicited CNM alert data and enhancements to NPDA Version 2 address the alert support requirement, as shown in Figure 14.

Logical data manager. The Network Logical Data Manager (NLDM)[7] was designed in response to logical problem determination requirements. The intent of NLDM is to establish SNA session awareness in an NCCF application and provide session trace capability that can be viewed interactively to assist in the isolation of undetected errors that frequently result in "hung" sessions. NLDM captures information relative to SNA protocols and data flow such as access method PIUs and selected NCP control information about a session. Also, NLDM can be compared to existing network trace capabilities in the same way that NPDA can be compared to LOGREC. Both NLDM and NPDA eliminate the traditional batch off-line function and provide an interactive structured facility, based on a logical subset of vast amounts of data. By utilizing NLDM to collect and store relevant SNA information in progress and prior to a failure, the need to recreate software problems or run dedicated traces is reduced or eliminated.

The operator is provided with a hierarchical view of the network that is bounded by and reflects the alerts occurring throughout the network.

NLDM utilizes a full screen and is the first CNM application to provide color for highlighting and differentiating information. Figures 15A through 15D illustrate a session history panel, session configuration panel, Path Information Unit (PIU) data panel, and session parameters data panel available with Release 1. The NLDM session awareness data are collected whenever a session begins or ends. Figure 15A is the NLDM presentation of session history for the selected Network Addressable Unit (NAU), which, in this case, is a host application named NCF04000. The start and end times are

illustrated along with the name of the secondary end of the session, the session type, domain, and whether the sessions are active. By choosing the session configuration screen, the operator moves to Figure 15B. This screen identifies the connectivity and logical names of the hardware components between the two ends of the session. In a problem determination scenario, these components could be the cause of an unresponsive terminal.

Figure 15C is a display of the primary trace screen. It illustrates the time, sequence number, direction, and Path Information Unit (PIU) data for the VTAM to NCF04000 session. The last data sent in the SNA session was a PIU sent by VTAM to LU NCF04000, which caused an SNA negative response. Figure 15D presents detailed BIND data to further assist in problem definition of the session.

The control and data flows between NLDM and the access methods also provide the session knowledge to accommodate network enhancements in the areas of connectivity and configuration.

In summary, the following four additional CNM facilities have been developed as enhancements for SNA networks:

- Threshold Analysis and Remote Access (TARA) program to support CNM downstream for IBM 3600 Finance Communication Systems.
- Terminal Access Facility (TAF) to support operator access and control between the network operator and IMS, CICS, TSO, HCF, and NCCF.
- Alert architecture and NPDA Version 2 to support network alerts.
- Network Logical Data Manager (NLDM) to support logical data for SNA networks.

Concluding remarks

With the base for Communications Network Management established by the products described in this paper, the following are requirements that may be addressed in the future.

In the downstream area, additional cascading of hierarchical and peer-coupled subnetworks dictates the investigation of new flows and protocols to support a generalized distributed CNM. The SSCP at

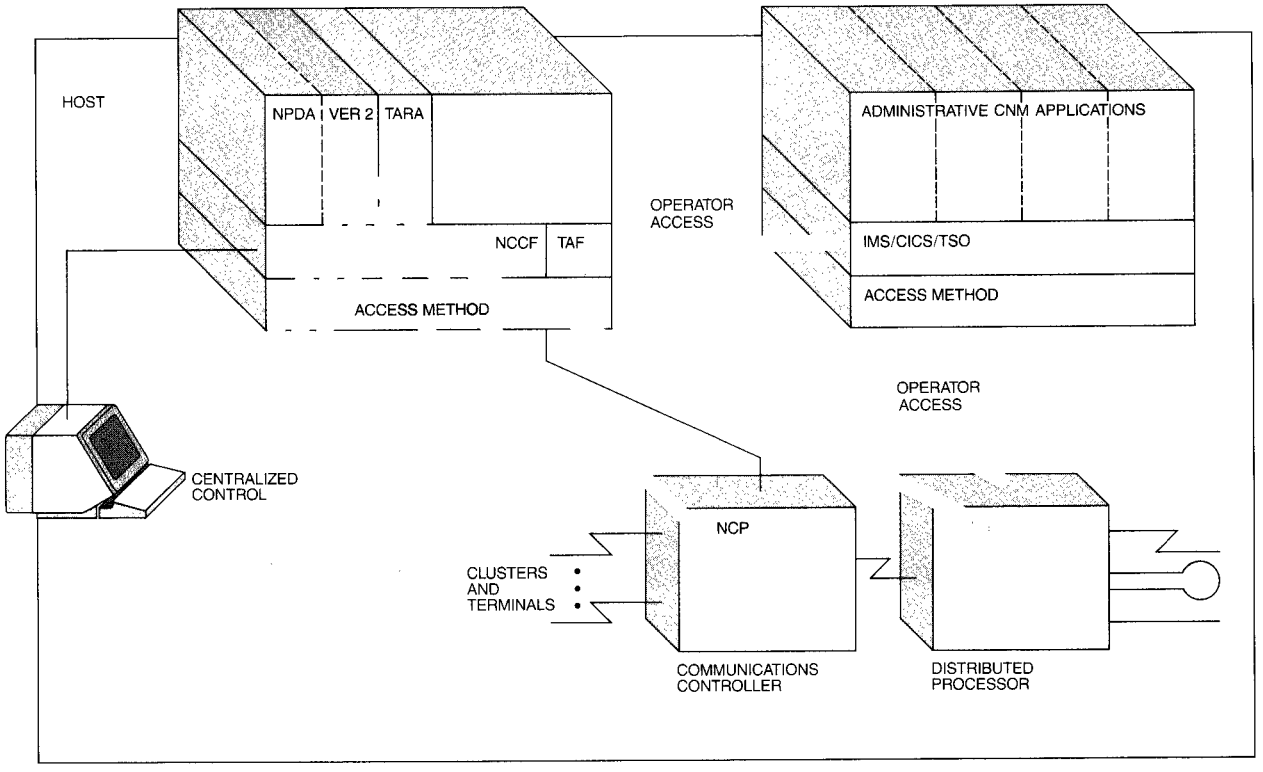
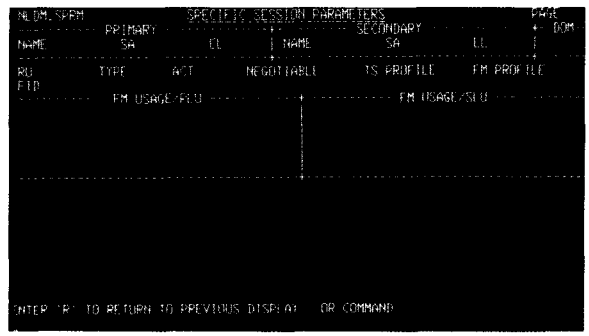


Figure 15 Network Logical Data Manager (NLDM) Release 1: (A) session history panel; (B) session configuration panel; (C) Path Information Unit (PIU) data panel; (D) Network Control Program (NCP) session trace data

(A)

(C)

(B)



(D)

individual subnetworks will require the option of routing or handling the CNM data it receives. User network incorporation of non-SNA protocols will continue to seek expansion of CNM coverage. Operator awareness of active configuration status will become increasingly important as configurations become more complex.

In the operator access area, now that the data can be directed to one point, the requirements emphasis will change to address the many variations in the user interfaces of the various subsystems. Levels of programmed operators will be required to give the user flexibility in meeting requirements and automating additional business areas. Operator access will continue to bridge the gap, until the objective of merging all the static and dynamic data about a network resource in one data base (with a distribution option) is realized.

In the alert area, users will want software products to be added to the list of components that assess their own exception conditions and evaluate possible corrective actions. Monitoring and filtering (severity, alert type) requirements against the alert processing support will grow as networks grow.

In the logical data area, a multitude of functions such as performance and accounting have a session affinity that users would derive from the data currently collected. Finally, the active network topology aspects must be exploited as networks grow and as developments such as local-area networks facilitate device movement and highlight the need for dynamic address and location assignment.

Acknowledgments

The enhancements described are the work of a group of talented and dedicated people in the CNM applications design and development group. I thank them all for these accomplishments. In addition, I thank E. H. Sussenguth, P. O. Lindfors, J. E. Drescher, E. G. Huff, and R. G. Beauchaine for

their support. Special thanks are due E. E. Iacobucci, who designed TARA and NLDM internals; J. T. O'Brien, who designed NLDM and the alert manager; R. F. Neumon, who designed TAF; and R. W. Chappell, for his downstream and product interface work.

Appendix: Index of terms

CICS	Customer Information Control System
CLISTS	Command Lists
CNM	Communications Network Management
DASD	Direct Access Storage Device
DPPX	Distributed Processing Programming Executive
HCF	Host Command Facility
ICF	Interactive Command Facility
IMS	Information Management System
IPL	Initial Program Load
LOGREC	Log Records
LU	Logical Unit
NAU	Network Addressable Unit
NCCF	Network Communications Control Facility
NCP	Network Control Program
NLDM	Network Logical Data Manager
NPDA	Network Problem Determination Application
PIU	Path Information Unit
RECFMS	Record Formatted Maintenance Statistics
PU	Physical Unit
RU	Response Unit
SLU	Secondary Logical Unit
SNA	Systems Network Architecture
SSCP	System Services Control Point
TAF	Terminal Access Facility
TARA	Threshold Analysis and Remote Access
TCAM	Telecommunications Access Method
TSO	Time Sharing Option
VTAM	Virtual Telecommunications Access Method

Cited references

1. R. J. Sundstrom and G. D. Schultz, "SNA's first six years: 1974–1980," *IEEE International Conference on Circuits and Computers, ICCC 80, Proceedings*, October 1–3, 1980, Portchester, NY, N. B. Guy Rabbat, Editor, 578–585 (1980).
2. *Systems Network Architecture Format and Protocol, Reference Manual: Architecture Logic*, SC30-3112; available through IBM branch offices.
3. R. A. Weingarten, "An integrated approach to centralized communications network management," *IBM Systems Journal* **18**, No. 4, 484–506 (1979).
4. *IBM 3600 Threshold Analysis and Remote Access, General Information*, GC34-2055; available through IBM branch offices.
5. *Network Communications Control Facility Releases 1 and 2, General Information*, GC27-0429-5; available through IBM branch offices.
6. *Network Problem Determination Application Version 2, General Information*, GC34-2061; available through IBM branch offices.
7. *NLDM General Information Manual*, GC30-3081; available through IBM branch offices.

Reprint Order No. G321-5187.

Timothy P. Sullivan *IBM Corporate Division, 400 Columbus Avenue, Valhalla, New York 10595.* Mr. Sullivan is a consultant to IBM Corporate Headquarters in the areas of telecommunications and network management. He joined IBM in 1964 in the Poughkeepsie Development Laboratory, where he held various technical and management assignments in channels and I/O. During 1973–1974, Mr. Sullivan worked in storage management design and mass storage system development in the General Products Division Laboratory in Boulder, Colorado. In 1974 he returned to Poughkeepsie, where he worked on I/O architecture and later led the system design for distributed language processors in the education industry area of the System Communications Division. In 1977, Mr. Sullivan was promoted to senior programmer and moved to Raleigh, North Carolina, where he worked in the area of design/release systems. From 1978 to 1981, he was responsible for Communications Network Management (CNM) application development and was the program product manager of the Threshold Analysis and Remote Access (TARA), Terminal Access Facility (TAF), and Network Logical Data Manager (NLDM) program products. He assumed his current responsibility in 1981. Mr. Sullivan received an IBM Outstanding Contribution Award for work on channel and I/O simulation. In 1964, he received his B.S. in electrical engineering from the University of Notre Dame, South Bend, Indiana.