An integrated network management product

by D. Kanyuh

The NetView™ program is the cornerstone of IBM's network management concept. It allows enterprises to consolidate their network operations at a centralized point and is a key element in providing the function to perform the major disciplines of network management. This paper describes how and why the NetView program originated, the components that make up the product, the network management functions provided by these components, such as operations, problem management, and performance management, and the contribution of the NetView program to the open network management direction.

IBM's approach to network management involves two related concepts. The first of these is to provide a family of products that allows enterprises to manage their networks from a centralized point (Figure 1). This family offers the major disciplines of network management—operations, problem management, change management, configuration management, and performance and accounting management. The NetView™ program is an important member of this family.

The second concept is to use distributed points of control throughout the network to support both Systems Network Architecture (SNA) and non-SNA systems and products. These points of control are used to collect network management information, forward it to a central site, and act as operations receiving points for commands coming from the central site.

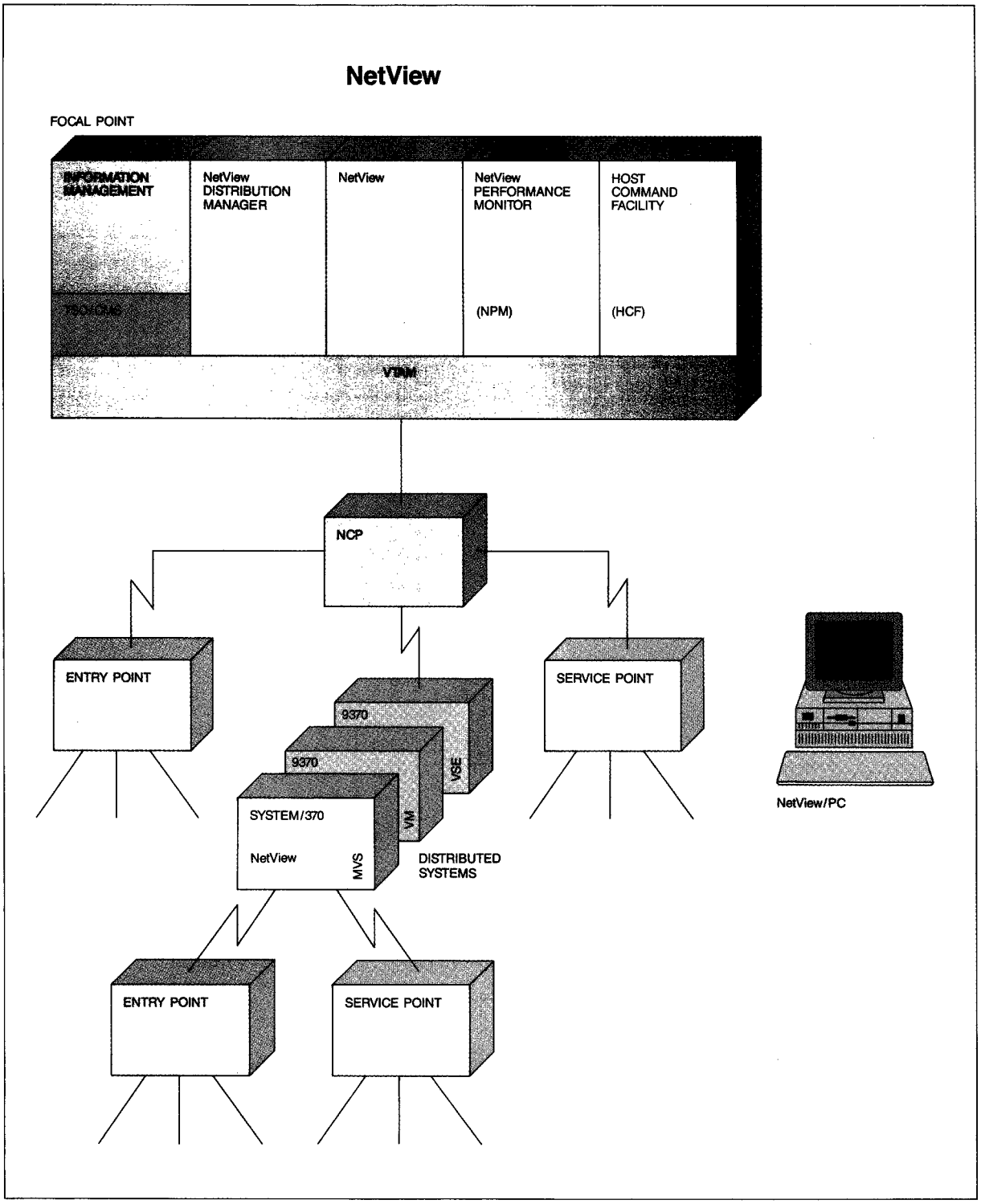
These distributed points are provided by the open network management functions of NetView, such as the Service Point Command Interface (SPCI) working in conjunction with NetView/PC™[1] or user applications.

The centralized and distributed points of control are tied together by IBM's SNA-based network management architectures. As an example of our open management direction, the NetView program provides the capability for all products, IBM or non-IBM, to contribute to the problem management function by providing a generic architecture to embody the alert structure.

At the foundation of the network management concept is the NetView program.[2] NetView is an integrated product formed by consolidating five previously available IBM network products. There are four major components of NetView: Command Facility, Session Monitor (including support for the IBM 4700 Communication Finance System), Hardware Monitor, and Status Monitor (Figure 2). These components are combined with usability and installation enhancements such as help, browse, and installation aids. The components work together to provide an enterprise with a common operations interface to manage and automate its network, to aid in problem determination, and to improve performance. NetView has extensive facilities for open network management both at the focal point and in communication with the distributed points of control.

The motivation and method behind the formulation of NetView will be discussed next.

Figure 1 IBM's network management system products



The origins of NetView

The largest and most important force behind the formation of the NetView program was the user—in particular, IBM's networking customers. Not only was the initial decision to develop NetView a direct result of what the marketplace wanted, but major design points were also based on users' input and feedback.

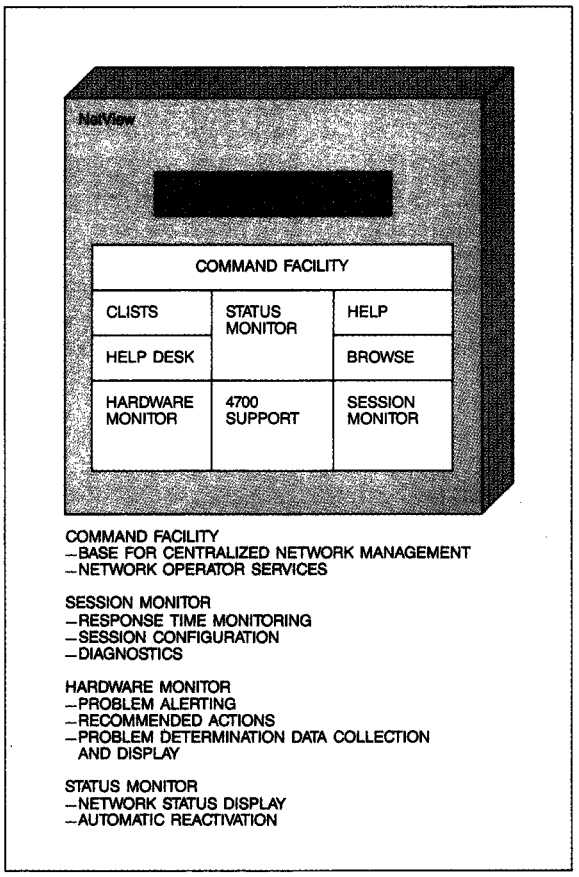
The need to simplify the installation and operation of our network management products came to us from three independent groups of users: a communication network management marketing task force, the Communications Programming Customer Council, and the user organization, SHARE. In a SHARE White Paper,[3] a detailed account of the product integration was given, including the need for help facilities and a common presentation services/user interface.

The decision to combine the products was only the beginning of the design. Before the NetView program was developed, a usability test was run on the network management programming products Network Logical Data Manager (NLDM), Network Communication and Control Facility (NCCF), and Network Problem Determination Aid (NPDA), along with two field-developed programs, the Network Management Productivity Facility (NMPF) and VTAM Node Control Application (VNCA). This test, in which users participated, identified several problems with the existing product set. Some of the major areas of concern were consistency of user interfaces from product to product, including program function (PF) keys, colors, and command input areas, and ability to move easily from one product to another. NMPF included a set of tutorials and help desk scenarios which the participants overwhelmingly agreed were an asset.[4]

With this user input, the development of NetView commenced. Once a direction was set, the concepts were reviewed with over 60 customer accounts. This was done through customer calls and surveys, FOCUS sessions, and the customer council. These sources agreed with the direction that the merged product was to take.

The first release tackled the external interface problems and the interactions between the products, now components. The installation process was greatly simplified, reducing the installation time and likelihood of errors. An extensive help facility was incorporated into the product as well as a help desk

Figure 2 The components of the NetView program



offering. Release 2 used this work as a base to answer another pressing requirement: the ability to automate network operations.

A second usability test with users was run, this time on NetView Release 1 before it was shipped. When the results of this test were compared with those of the previous test, it was shown that the NetView program was significantly more usable than the set of products preceding NetView.[4]

The following sections will explain the structure of NetView and the areas of network management that it addresses.

NetView components

Command Facility. The Command Facility is the base component of NetView.[5,6] Through this com-

ponent services are provided for centralized network management. These services include message routing, logging, presentation, and automation. Operator support is also available from the command facility. Commands or CLISTs (command lists—lists of NetView commands incorporated in a simple language facility) entered by the operator can be routed to different domains or systems within a domain.

The other NetView components also rely on the Command Facility as their program base. Macro services, including database access, operating system independence, intracomponent message routing, and screen handling and presentation, are available. The Application Programming Interface (API) for user-written customization also interfaces with the Command Facility.

The Command Facility is the main contributor to the operations discipline in NetView. This function will be explained in more detail later in this paper.

Session Monitor. Diagnostic facilities for the SNA logical network sessions are provided by the Session Monitor. This component collects and correlates data about SNA sessions and provides on-line, interactive access to the data. Through this function, logical network problems and error conditions can be identified in a productive manner. These conditions include "hung" sessions, lost messages, and route problems.

The Session Monitor collects data about same-domain, cross-domain, and cross-network SNA sessions. The following types of data are collected for these sessions (Figure 3).

- Session response time data—This information is measured and accumulated by control units with the Response Time Monitor (RTM) feature. It is sent to the Session Monitor on request.
- Session trace data—Such data consist of session activation parameters, Virtual Telecommunications Access Method (VTAM) Path Information Unit (PIU) data, and Network Control Program (NCP) data.
- Network account and availability measurement data—The Session Monitor provides data on network availability and distribution of usage of network resources. These data are written to an external log.
- Route data—The list of Physical Units (PUs) and Transmission Groups (TGs) that make up an explicit route are included here.
- Session awareness data—The data include information about session activity, identifying the session partners, and configuration.

Hardware Monitor. The Hardware Monitor collects error and information records from network devices (both SNA and non-SNA). It provides interactive presentation and logging capabilities for these records based on customizable filters. These functions assist network personnel in performing network problem determination. These data are also analyzed for probable cause and recommended actions, which can isolate a network problem to that of a specific failing component. The alert feature informs the operator quickly of high-priority problems.

The data collected by the Hardware Monitor can be classified as solicited or unsolicited (Figure 4). Solicited data are received as a result of a specific request for information. Unsolicited data, such as the result of an error being detected or counters exceeded, are received without any action.

The records that are sent to the Hardware Monitor can be one of three types:

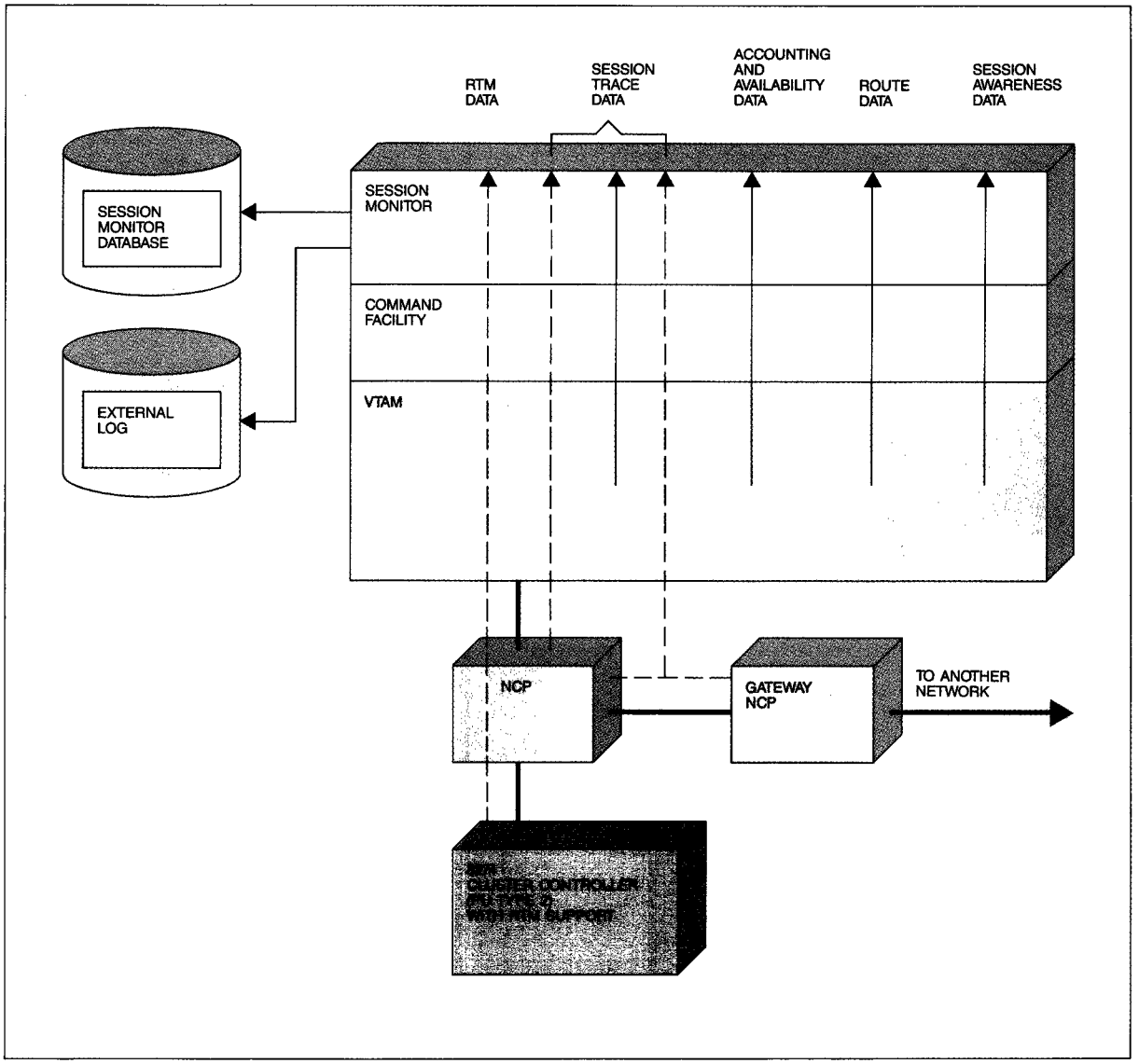
1. Statistics—These are records of traffic and recoverable error counts.
2. Events—Unexpected occurrences in network operation cause event records such as resource activation failure to be generated.
3. Alerts—Events that require immediate attention are alerts. Alerts are determined by the filters defined.

Status Monitor. The display of the Status Monitor allows the user to tell "at a glance" the status of the components in his domain (Figure 5). This status information can then be used to control these resources.

The Status Monitor uses colors to identify the different states in which a resource can be. For example, active nodes are presented in green, inactive in red, and pending in pink.

From the main status summary screen a series of detail panels can be displayed. These panels allow the user to view a subset of the resources (such as all inactive Logical Units, or LUs) and include more information on the selected resources. This information can be node names and description, summary of node status over time, or message traffic counts to and from an application program node.

Figure 3 Session Monitor data collection

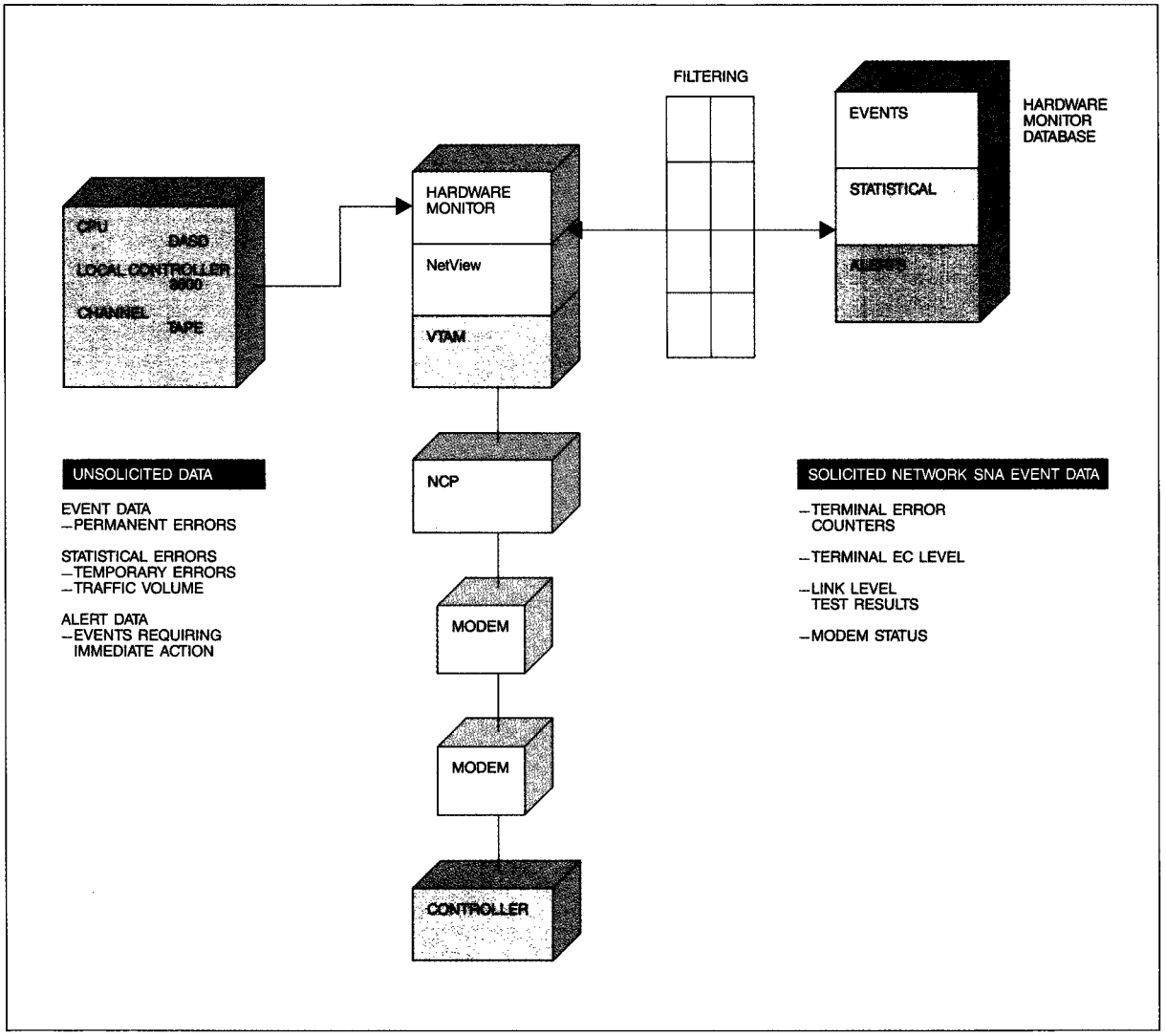


The Status Monitor provides another function, the monitoring of inactive nodes. This component has the capability to reactivate minor nodes that are in the inactive state. These nodes appear in the MONIT column on the display. Once a node is reactivated, its lower nodes, if present, will be monitored and reactivated as well.

Usability features. Working in and around the component structure of the NetView program are several features which enhance its usability and cohesiveness. Included in this area are browse support, extensive help facilities, a unique "ROLL" approach to command entry, and packaged installation aids.

A full-screen browse capability is provided for online viewing of NetView installation files, CLISTs, panels, and the message log. The browse panels provide a scroll field, program function keys, and a find command.

Figure 4 Data collected by Hardware Monitor



The message-log browse has an additional "Important Message Indicator" capability. Messages are user-defined to fall into one of four categories that can set off indicators on certain NetView panels. The operator is then led directly to the message in the log that set off the indicator. These messages can also be color-coded for easy visibility.

Operator assistance is provided by the on-line help facility when using NetView. Helpful information can be viewed for every NetView command, component, and certain displayed panel fields and codes.

A step-by-step approach is used in the help desk to simplify network problem determination. Complex procedures are reduced to simple steps that lead the operator toward resolution of a specific problem. Diagnosis assistance covers NetView, VTAM, and other network offerings such as the IBM 4700 Finance Communication System.

Through the use of a command line on all NetView panels and appropriate program function keys, a NetView command or component can be invoked from the screen of another component. Once a com-

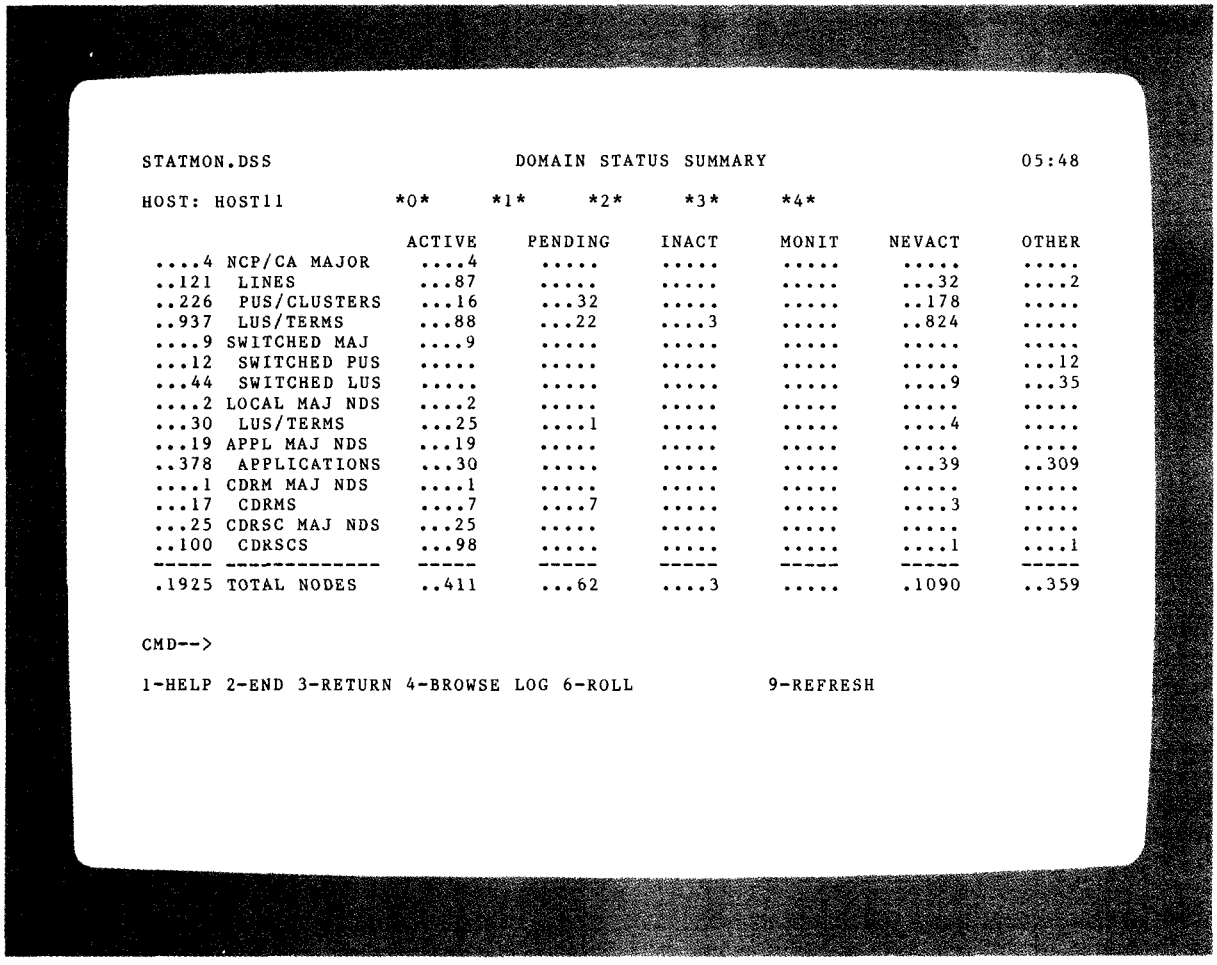
ponent has been entered, it is placed on a "stack." Using a program function key, the user can "roll" through the components on the stack, entering commands and changing screens as he goes.

NetView features an advanced installation process based on a prepackaged sample network and a task-oriented procedure. Together they simplify the user interface and reduce errors. The sample network, which is shipped in machine-readable form, includes VTAM, NCP, and NetView definition statements, along with the tables, CLISTs, and Job Control Language (JCL) to initialize the product. The installer then verifies that NetView is functioning properly by executing a predefined set of scenarios.[7]

Network management functions provided by the NetView program

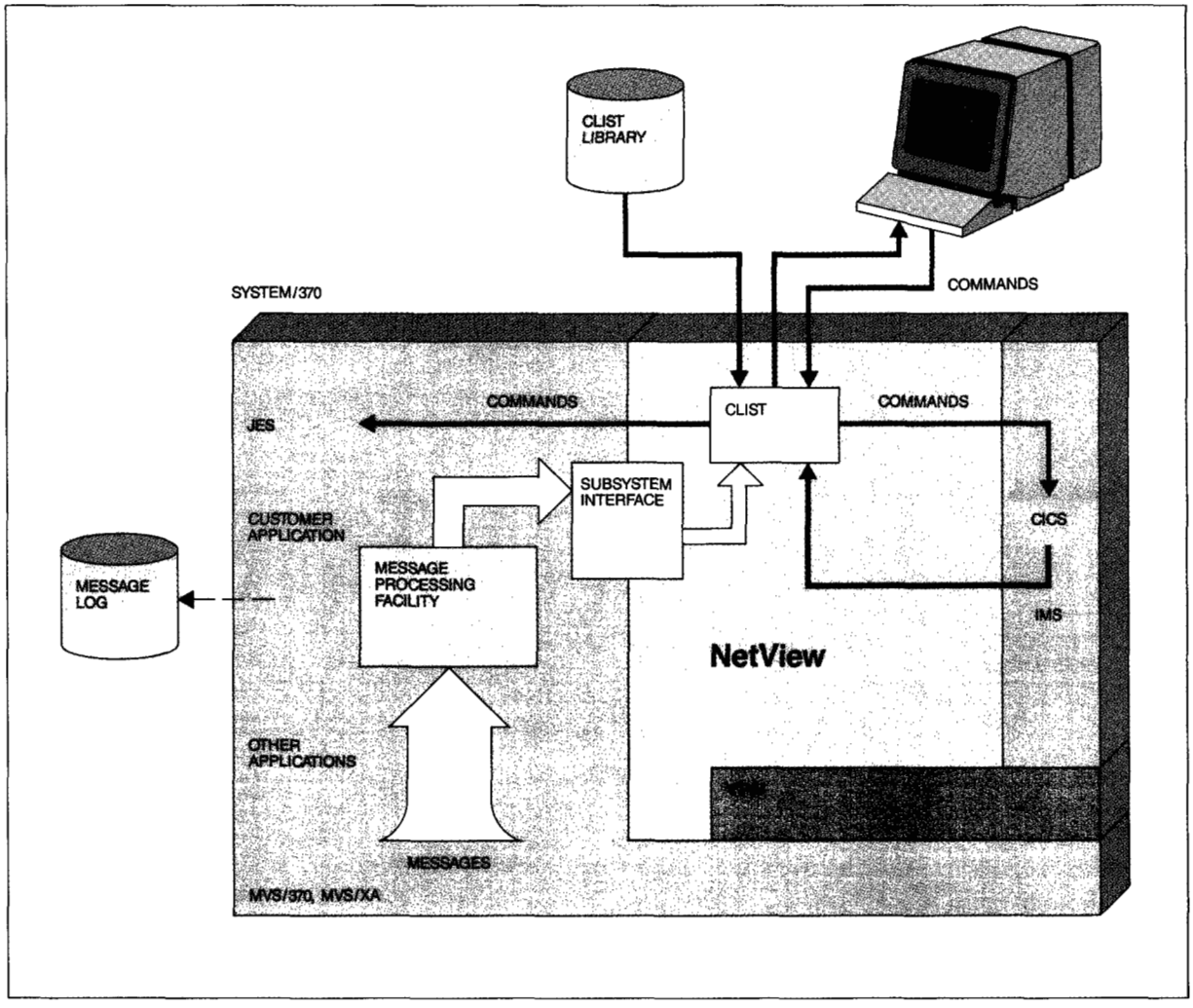
Operational control functions. The purpose of the operational control functions is to provide the facilities and processes for controlling and managing all of the resources in the operational system environment. NetView, through the Command Facility, offers this capability to the network operator for managing both local and remote systems from a consolidated point or from distributed points of control. The operational control strategy is to minimize a human operator's activities through the use of automated operation. Extensive facilities in NetView allow this automation.

Figure 5 Status Monitor summary panel



```
STATMON.DSS                    DOMAIN STATUS SUMMARY                    05:48

HOST: HOST11          *0*     *1*     *2*     *3*     *4*

                     ACTIVE    PENDING    INACT     MONIT    NEVACT     OTHER
 ....4 NCP/CA MAJOR   ....4      .....     .....     .....     .....     .....
 ..121  LINES         ...87      .....     .....     .....     ...32     ....2
 ..226  PUS/CLUSTERS  ...16      ...32     .....     .....     ..178     .....
 ..937  LUS/TERMS     ...88      ...22     ....3     .....     ..824     .....
 ....9 SWITCHED MAJ   ....9      .....     .....     .....     .....     .....
 ...12  SWITCHED PUS   .....     .....     .....     .....     .....     ...12
 ...44  SWITCHED LUS   .....     .....     .....     .....     ....9     ...35
 ....2 LOCAL MAJ NDS  ....2      .....     .....     .....     .....     .....
 ...30  LUS/TERMS      ...25      ....1     .....     .....     ....4     .....
 ...19 APPL MAJ NDS   ...19      .....     .....     .....     .....     .....
 ..378  APPLICATIONS   ...30      .....     .....     .....     ...39     ..309
 ....1 CDRM MAJ NDS   ....1      .....     .....     .....     .....     .....
 ...17  CDRMS         ....7      ....7     .....     .....     ....3     .....
 ...25 CDRSC MAJ NDS  ...25      .....     .....     .....     .....     .....
 ..100  CDRSCS        ...98      .....     .....     .....     ....1     ....1
 ----- ------------   -----     -----     -----     -----     -----     -----
 .1925 TOTAL NODES    ..411      ...62     ....3     .....     .1090     ..359


CMD-->

1-HELP 2-END 3-RETURN 4-BROWSE LOG 6-ROLL          9-REFRESH
```

Figure 6 NetView system interfaces



The first set of functions deals with the NetView operator. Security and control are provided by log-on authorization, scope of commands, and span of control. The NetView operator must enter the proper identification and password to gain access to the system. A profile associated with each operator defines what access to the commands, or scope, an operator possesses, and what span of control the operator exercises over resources. The scope capabilities limit an operator to a subset of network functions, and the span of control defines which resources an operator may control in the network.

NetView allows commands entered at its terminals to be routed to different system components, domains, or networks. The cross-domain and cross-network communication of NetView allows an entire network to be controlled from one operator station. As an example, with the Terminal Access Facility (TAF), an operator can log on to several subsystems, including the Time Sharing Option (TSO) and the Information Management System (IMS), without logging off NetView. TAF can also be used in cross-domain communication by logging on to a remote system that has NetView.

NetView is a focal point not only for networking commands but for system commands as well. Using the Multiple Virtual Storage (MVS) Subsystem Interface, NetView can process and route MVS system and

subsystem commands issued from a CLIST or NetView operator (Figure 6). These commands can be routed to a subsystem in the same domain or to another domain. To make the function complete, an MVS operator can also issue NetView line-by-line commands and CLISTs from an MVS console.

Remote operations, including bring-up and restart capability for a target host, are possible through NetView and an additional offering, the Inter-System Control Facility (ISCF). THE ISCF code in the host works with the ISCF code in an IBM Personal Computer (IBM PC) to allow commands to be issued from a central NetView control host and routed to a target host. These commands can be used to perform remotely those functions that would otherwise require manual intervention by an operator at every CPU location (Figure 7).

The automation facilities in NetView comprise mainly two functions: an automation task and a message automation facility. One or more automation tasks may be active in NetView, combining with the message automation support to form a comprehensive set of capabilities.

All operator task functions are supported in the automation task except for full-screen presentation services, since this task has no operator console. This task removes the dependency of NetView on VTAM, allowing those functions which do not require VTAM, such as certain Hardware Monitor operations and message automation, to continue running throughout VTAM outages. The automation task has the ability to restart VTAM and to start the other NetView functions after VTAM returns from an outage. This support allows NetView to be brought up before VTAM is initially active. The most significant result of this VTAM dependency removal is that NetView may be used for system automation in systems that do not use VTAM.

The message automation and CLIST facilities of NetView can be used to control operator functions in multiple console support (MCS), Job Entry Subsystem 2 (JES2), JES3, NetView, and any application that can be accessed by TAF. A NetView CLIST can issue commands to and can intercept messages for processing from any of these systems.

The message table support allows for a variable number of criteria to be specified and compared against an incoming message. These criteria may range from string comparison in the text to the JES job identifier or other attributes associated with the message. The result of these comparisons will then determine the actions taken. These actions include executing a CLIST or command processor and displaying, suppressing, or logging the message. The specifications that define the message table are in the form of IF-THEN statements and can be dynamically changed.

A sample set of message table entries and CLISTs is available with NetView to help the user get started in the automation of his network operations. This set automates areas of the system processes of initialization, monitoring or recovery, and shutdown for MVS, VM/SP (Virtual Machine/System Product), NetView, VTAM, JES, TSO, IMS, and CICS (Customer Information Control System). Examples are given for both single and multisystem environments. Additional customization can then be added to this base depending on the user's needs and procedures.[8]

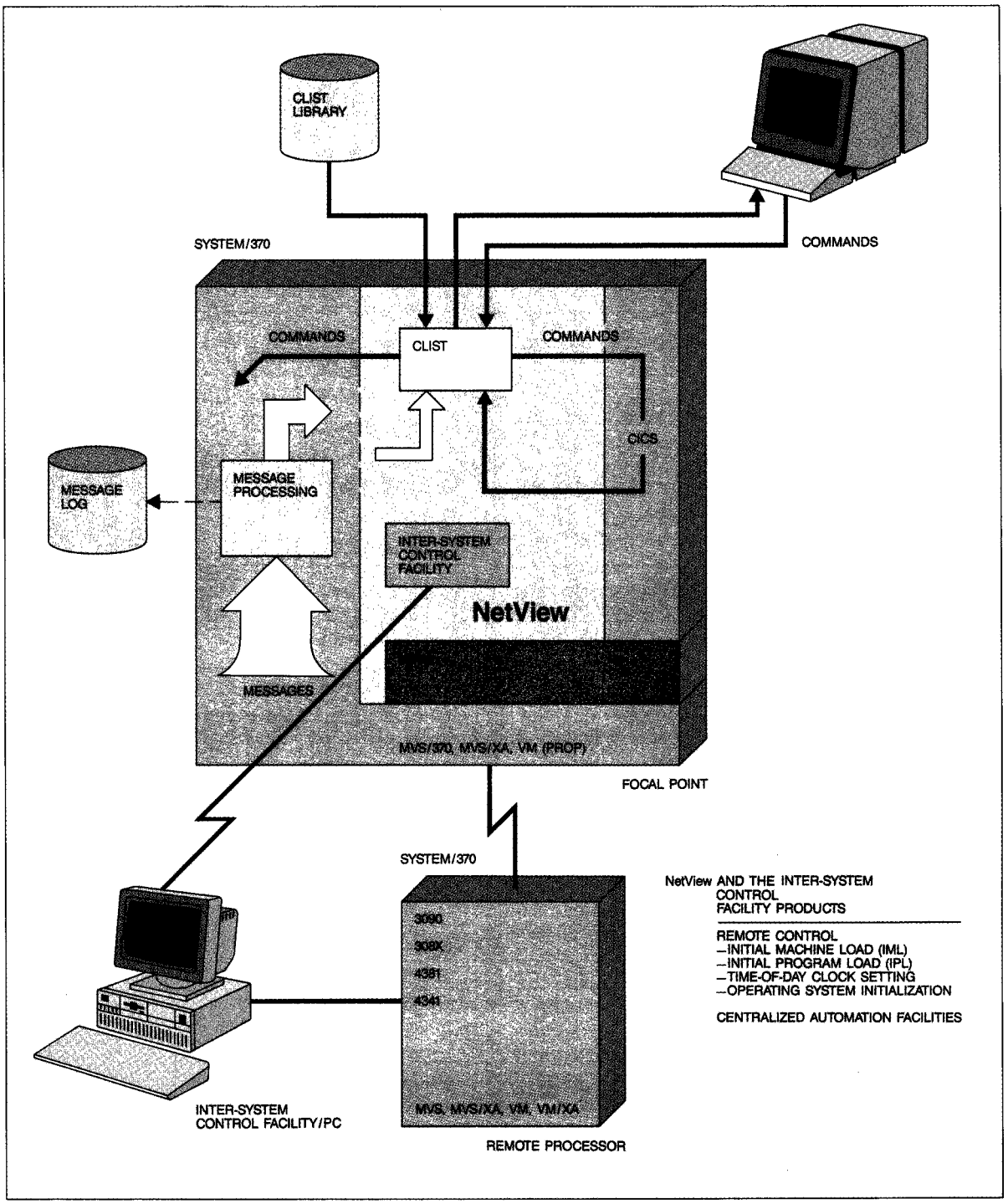
Alerts are the main mechanism for problem detection in NetView.

Problem management. The processes that take place across the problem management discipline include problem detection, the collection and analysis of data, and recovery. NetView plays an important part in each of these processes, both directly in the function it provides and indirectly in its support for user implementation in this area.

Alerts are the main mechanism for problem detection in NetView. By monitoring the Hardware Monitor Alerts–Dynamic panel, the network operator will be kept up to date on error conditions in his span of control. This screen is automatically updated whenever an alert occurs, presenting a one-line summary of this special event. The operator may then select a specific alert and retrieve detailed information.

Data about potential error conditions are collected by both the Hardware Monitor and the Session Monitor components. When an event or an alert is

Figure 7 Extended remote operations and control



received from a network resource, the data are stored by the Hardware Monitor in the database. These data describe conditions in the physical network. Data pertaining to the logical network are gathered by the Session Monitor. For each session, information such as names, configuration, and type is kept. If an error occurs at session activation, information including BIND and UNBIND failures and session setup failures is logged. With the trace function active, PIU and NCP data are also stored on a session basis.

A key aspect of our network management system is that it is open.

As part of the alert, probable cause and recommended action information is included for each situation. This analysis is done either by the sending component or by the Hardware Monitor. The goal is to isolate the network problem to the specific failing component. When statistical records are sent to the Hardware Monitor, an analysis is also done to determine whether the situation warrants an alert. On the basis of the results of these analyses, the operator may need to continue the problem determination process. Through NetView, commands can be sent to modems and NCPs to issue tests and retrieve status information.

Once the problem has been identified, the last process, recovery, can begin. In many cases, CLISTs driven from messages or alerts will automatically bypass or recover a lost resource. When operator intervention is needed, the commands can be entered from a central site to correct problems throughout the network.

Performance management. The NetView program provides function within the performance management area that presents the user with information on response time and availability of network resources. This information can be used for problem isolation and capacity planning.

The Session Monitor collects response time data from control units having the Response Time Monitor feature. The data are associated with sessions by specification of a performance class and response time objectives. These data are displayed for the operator in summary format, by session and collection period (Figure 8), and by response time trends.

Network availability data are collected by the Session Monitor and written to an external log for off-line processing. This information includes the time and date of the BIND and UNBIND, number of PIUs sent and received, and names of the primary and secondary LUs. The Status Monitor component provides an on-line indication of network availability. For a given set of resources, information showing the percentage of time each resource has been in each given status (Active, Inactive, Pending) is displayed.

Open network management facilities

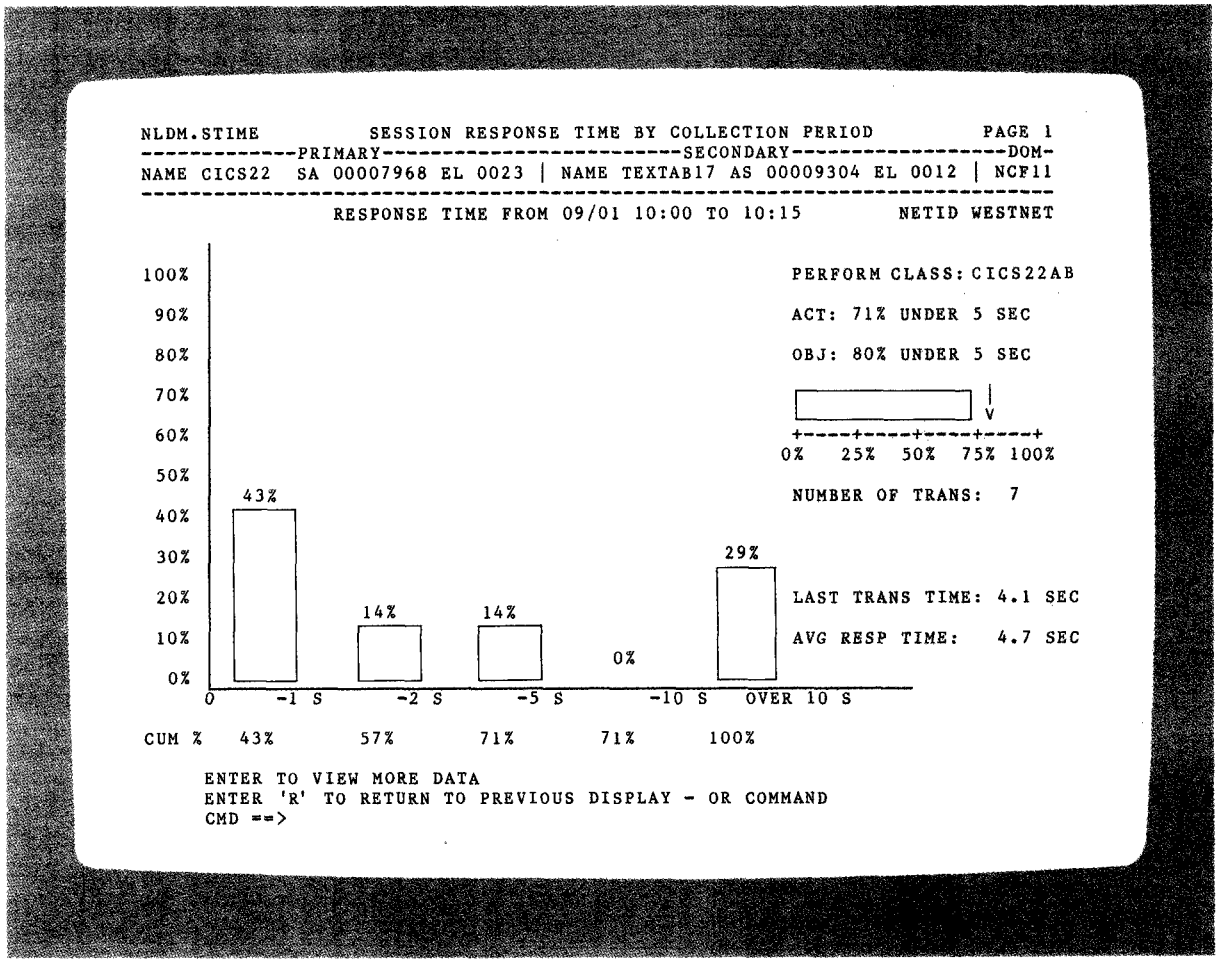
One key aspect of our network management system is that it is open, allowing participation of non-IBM devices and systems. A published set of network management architectures is provided, along with the application programming interfaces of NetView. The following subsections will explain these facilities as they relate to the focal point and to the control points.

Focal point facilities. NetView contains an extensive set of application programming interfaces at the focal point for customization. These include user exits, command processors, subtasks, CLISTS, and screen modification procedures. To provide the appropriate environment for user-written programs, several NetView macros and control blocks are documented for external use. Each interface has its set of coding conventions, including input and output specifications. The facilities offered provide the user with a range in flexibility from simple panel changes to complete network management components.

Exit routines can be written to view, delete, or replace data flowing to, from, or through NetView. Exits can handle specific events, or can automate processes based on message information. Fourteen global exits in NetView apply to all tasks (Figure 9). They are located at all major data routing points. For example, data passing to and from the operator console, to the log, or to and from the access method can be changed or removed.

When an additional service or function is needed, a command processor can be written by the user.

Figure 8 Response time by collection period display



Command processors have a broader influence than exit routines. These modules are invoked by the operator in the same way as NetView commands, accepting parameters if needed. They can output data to the operator's screen using line-by-line or full-screen mode.

If even more control is needed, a mechanism to include a user subtask is available in the NetView program. This capability is designed to allow control of a resource that is used by more than one task.

A CLIST is a set of commands and special instructions that are grouped together under one name. Commands that can be issued from a NetView terminal can be put in a CLIST, CLISTs can be invoked by an operator, another CLIST, the operator log-on procedure, NetView initialization, a user-written command processor, or a message.

The CLIST language provides comments, control and assignment statements, labels, and built-in functions. Parameters may be input with the CLIST, and a global as well as local variable capability exists. Simple control statements such as IF and GOTO are present, along with a more complex WAIT facility. It is also possible to output text to the operator's screen.

The Help facility in NetView is structured to allow the user to perform modifications and customization. The existing panels may be changed to reflect individual procedures and practices. One or more

panels may also be added or replaced at any point in the display hierarchy to allow additional help information.

Interfaces to distributed points of control. In order to control, monitor, and perform problem determination on distributed resources, NetView offers two structured interfaces: Service Point Command Interface (SPCI) and generic alerts. Use of these facilities allows non-IBM or non-SNA devices to communicate with the focal point.

With SPCI, a global command, RUNCMD, is provided that allows native service point commands to be executed at the service point from the host. The service point may then in turn send a reply message to the focal point and have it displayed on the operator's screen (Figure 10). RUNCMD is sent to the service point in the Network Management Vector Transport (NMVT) format. This support[9] allows NetView/PC to attach to NetView and provide its interface to non-SNA products.[1]

Any resource in the network can send an error indication to the focal point. This indication is a generic alert. A generic alert allows coded alert data to be transported to a focal point where the data will be stored and displayed. The coded data are used as an index to a predefined table containing short units of text, or the data may contain the text directly. A user may supply his own table for indexing or use the one provided by IBM (Figure 11).

Generic alerts are used to produce output for the operator containing recommended actions, probable cause, and detail displays. With this facility, a cus-

Figure 9 User exit locations

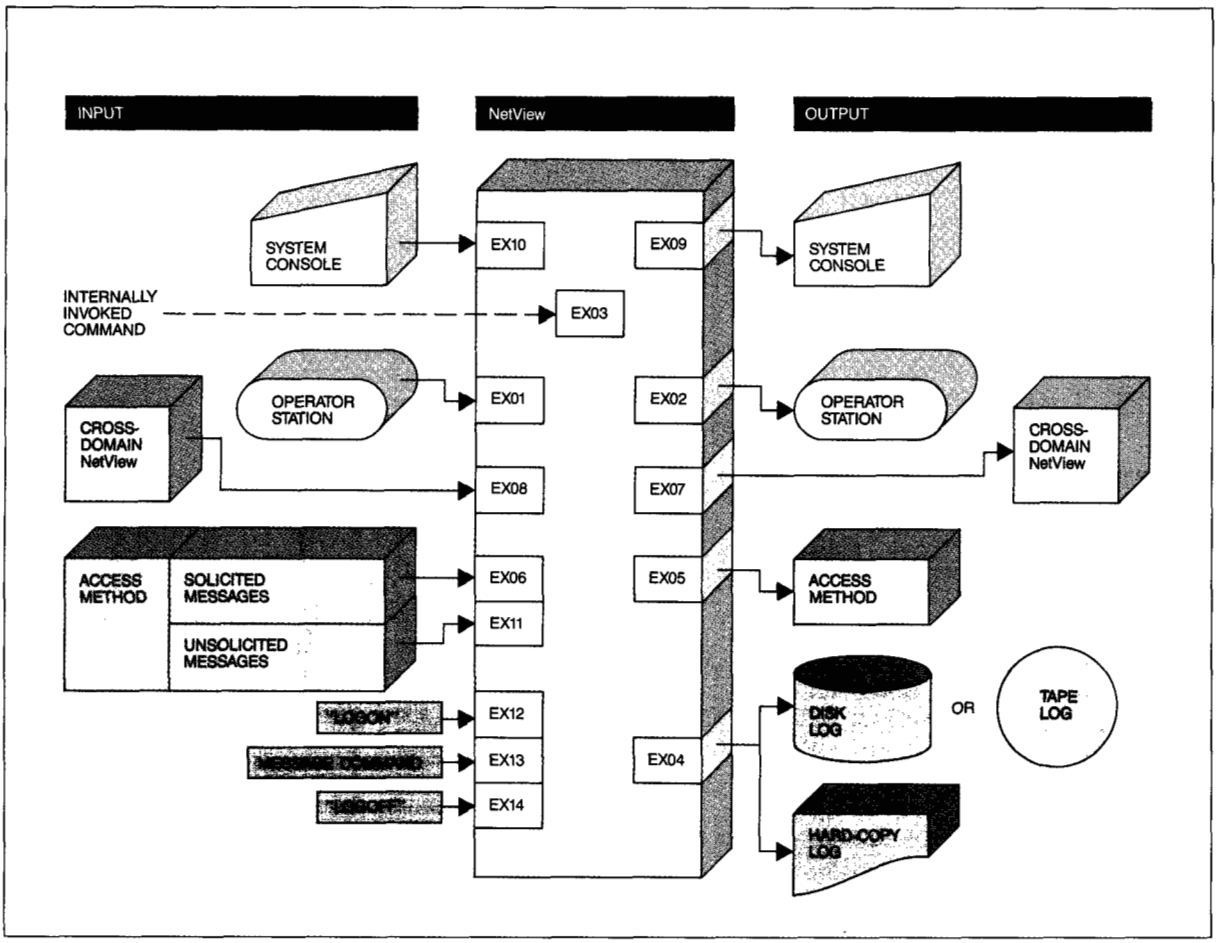
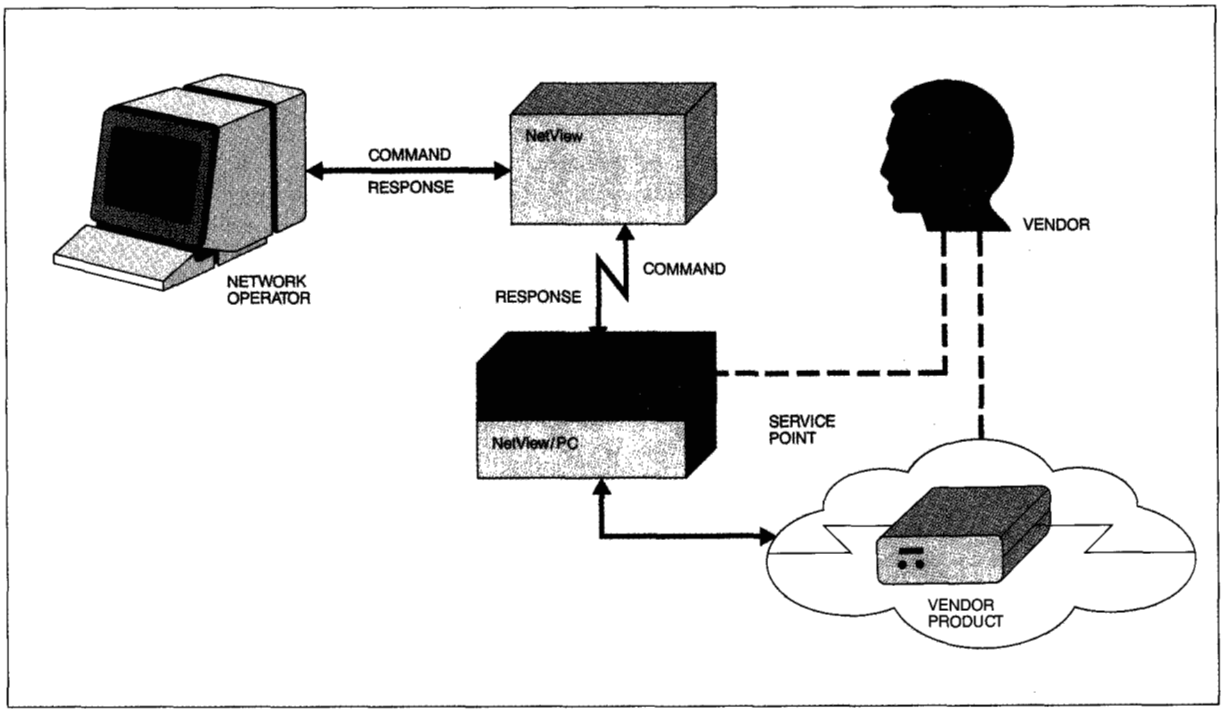


Figure 10 Service Point Command Interface



tomer can use the Hardware Monitor component to coordinate alert conditions from every resource in his network, be it IBM or non-IBM.

Summary

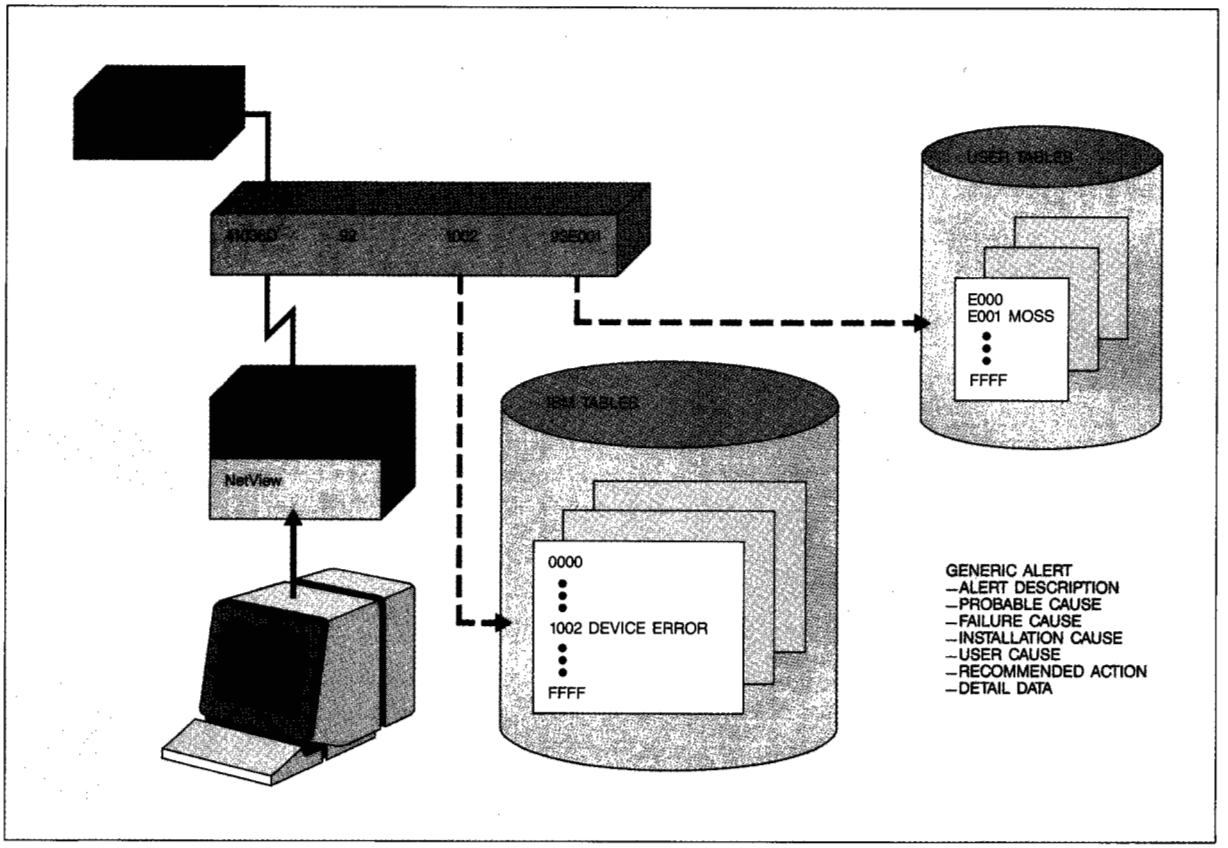
With its comprehensive set of integrated components, the NetView program provides a strategic base for IBM's network management system. It facilitates operational control and problem and performance management of network resources from a central point or several distributed locations. To provide openness, it offers a rich set of application programming interfaces and published network management architectures.

Network management is one of the most important needs in today's networks, and requirements in this area are growing steadily. NetView offers the facilities to meet these needs and the framework to grow along with the networks it supports. The automation support offered today allows for future development of expert-system-based diagnosis and repair of network problems. Performance monitoring, automatic load balancing, and central control and management of large multifocal-point networks are just some of the challenges to be faced and answered by the NetView program as it grows and evolves.

Cited references and notes

1. For more information, see M. Ahmadi, J. H. Chou, and G. Gafka, "NetView/PC," *IBM Systems Journal* **27**, No. 1, 32–44 (1988, this issue).
2. *Learning About NetView: Network Concepts*, SKT-0292, IBM Corporation; available through IBM branch offices.
3. *Communication Network Management Product Integration White Paper*, edited by Michael L. Nault, SHARE, Inc., Chicago (February 25, 1985).
4. For a discussion of the general approach taken in the usability tests, see L. C. Percival and S. K. Johnson, "Network management software usability test design and implementation," *IBM Systems Journal* **25**, No. 1, 92–104 (1986).
5. *NetView Operation*, SC30-3364, IBM Corporation; available through IBM branch offices.
6. *NetView Operations Scenarios*, SC30-3376, IBM Corporation; available through IBM branch offices.
7. *NetView Installation and Administration Guide*, SC30-3360, IBM Corporation; available through IBM branch offices.
8. For more information, see *Automated Operations Using NetView CLISTs*, SC30-3477, IBM Corporation; available through IBM branch offices.
9. NetView/PC refers to this support as Service Point Command Service.

Figure 11 Generic alerts



Denise Kanyuh *IBM Communication Products Division, P.O. Box 12195, Research Triangle Park, North Carolina 27709.* Since joining IBM in 1982, Ms. Kanyuh has worked in the area of network management. She is currently a staff programmer in network management system design. Ms. Kanyuh received a B.S. in computer science from the University of Minnesota and is a candidate for a Master's degree at North Carolina State University.

Reprint Order No. G321-5310.