Management of multivendor networks

by J. G. Stevenson

Technical advances in multivendor network management capabilities allow customers to effectively manage their networks. Packaged offerings such as NetView® Extra simplify the ability to take advantage of these new capabilities. This paper describes the multivendor environment, customer network management requirements, IBM's initial approach to responding to these requirements, and enhancements needed to provide additional management offerings that automatically handle failures, including detection, bypass and recovery, vendor notification, and restoration of the repaired resource into service.

In an interconnected multivendor world, the need for network management continues to be one of the leading customer requirements. This paper discusses the multivendor environment, customer requirements, and IBM's approach to multivendor management, as well as the enhancements needed to current products to satisfy these requirements. The paper also shows how the network operator, technical support group, and help desk can use this network management capability to effectively manage the enterprise. The paper concludes by describing how all the network management functions work together to solve the customer's multivendor operational problems.

Multivendor environment

Enterprise networks are composed of different types of devices, systems, and architectures that have matured over time to satisfy different user requirements. (See Figure 1.) As these systems grow they support multiple protocols, such as Open Systems Interconnection (OSI), Transmission Control Protocol/Internet Protocol (TCP/IP), Systems Network Architecture (SNA), and DECnet**, and contain multiple logical networks on one or more physical networks. These networks provide not only the transport for data, but also voice. This conglomeration of systems, protocols, and networks makes effective management difficult and challenging.

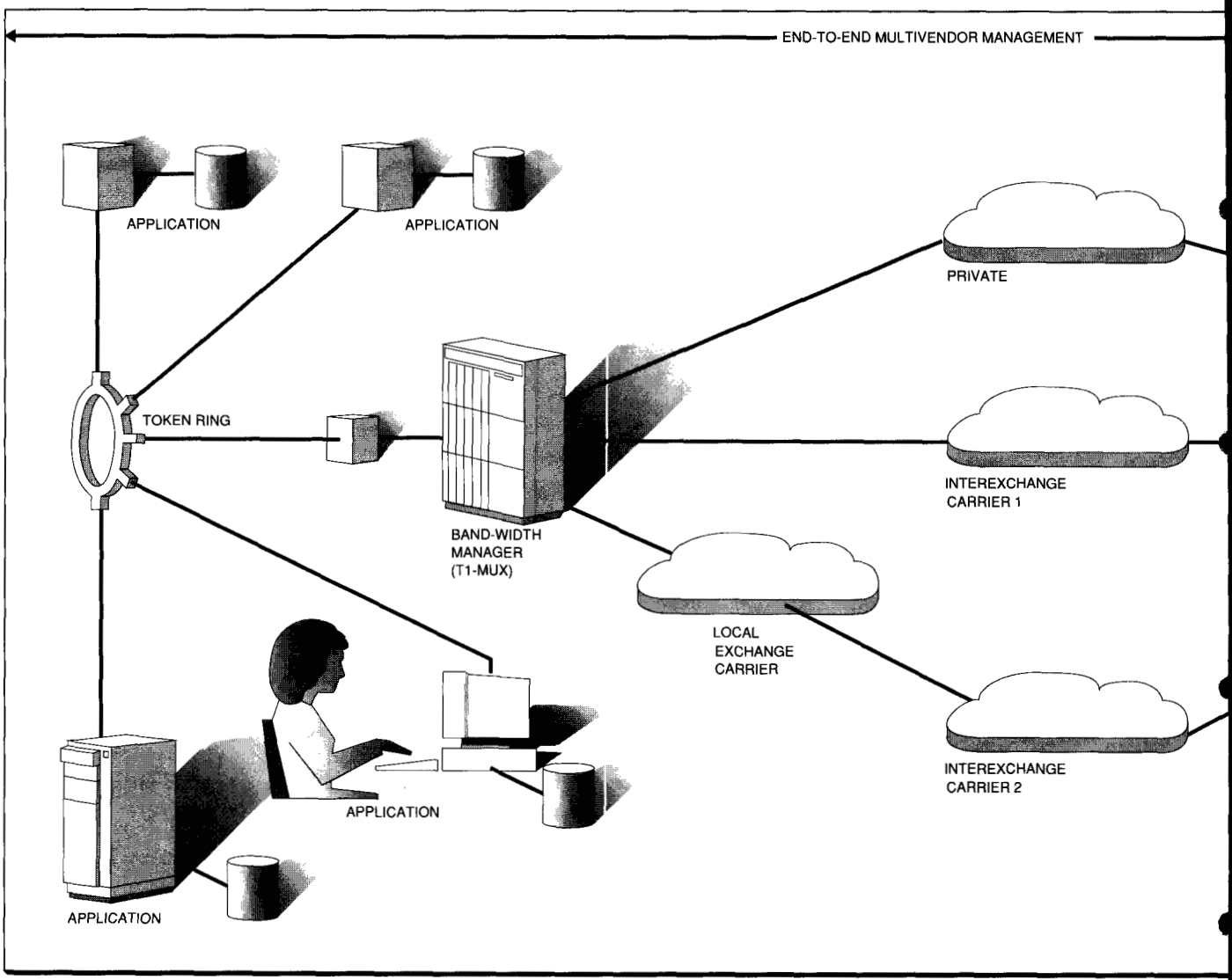
The requirement for high availability of complex networks is the major problem that must be addressed. One must assume that all network components will fail at some time, and that recovery procedures must be established to bypass the failing components.

Once a failure occurs, the failure must be recognized, and the recovery option that provides the fastest restoration of service to the end user must be identified and implemented. In today's environment, failure identification and recovery is usually a manual process dependent upon both the reaction time of the operator and documentation of bypass and recovery procedures.

Customer requirements

Customers want comprehensive multivendor end-to-end management functions for voice and data, including both wide area and local area

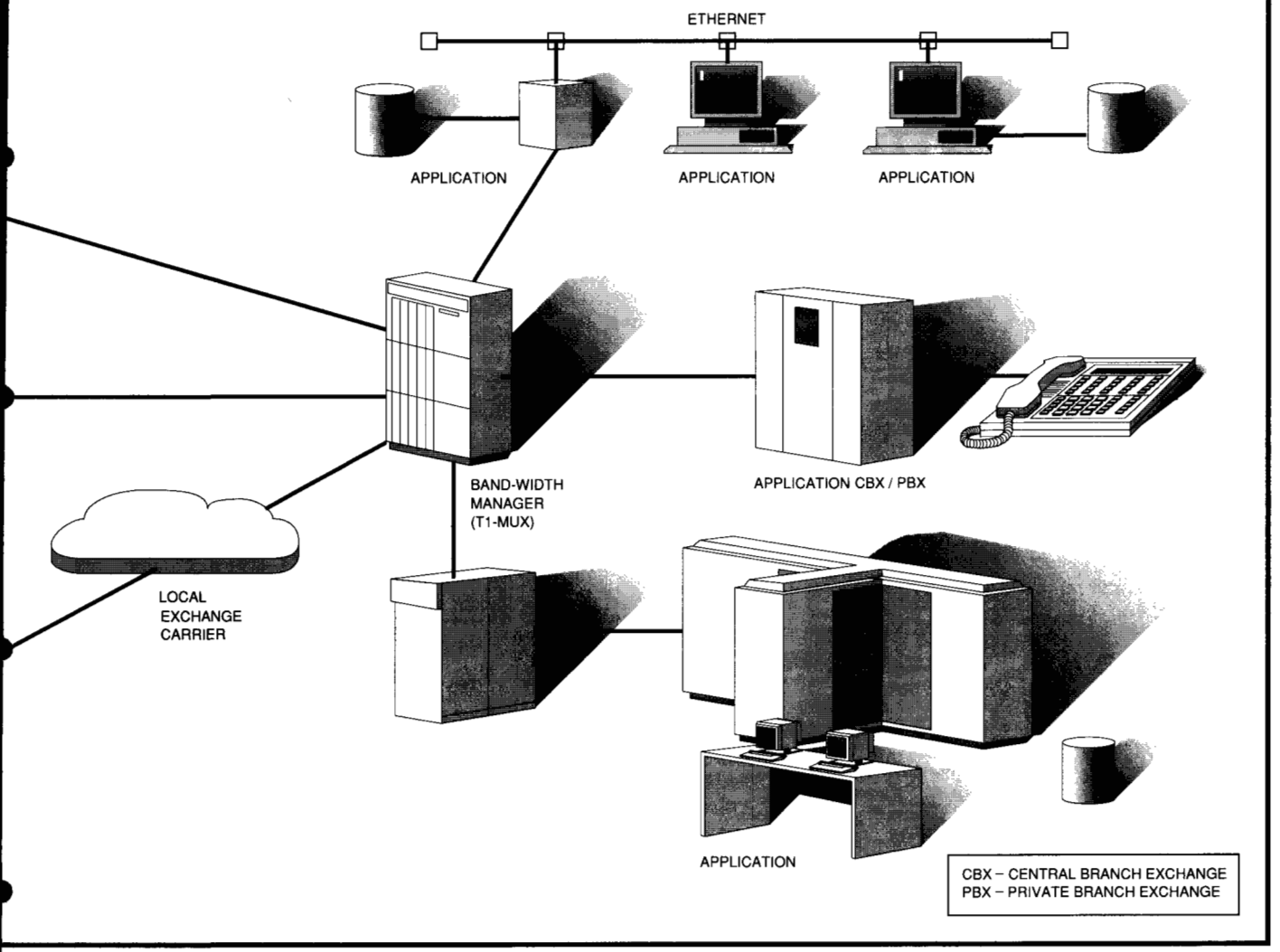
Figure 1 Customer multivendor environment



networks. The functions must address all resources, including terminals, multiplexers, bandwidth managers, concentrators, carrier services, bridges, routers, intelligent hubs, access units, modems, repeaters, host processors, databases, and applications that make up today's multivendor environment.

Customers require systems that allow customer-based management and control, reduce cost, increase availability, maximize responsiveness, and make their companies more competitive. An important goal is to achieve automated operations that reduce complexity and cost, increase productivity, and improve availability by eliminating human error. Figure 2 depicts the major functions that users request. A discussion of these requirements follows.

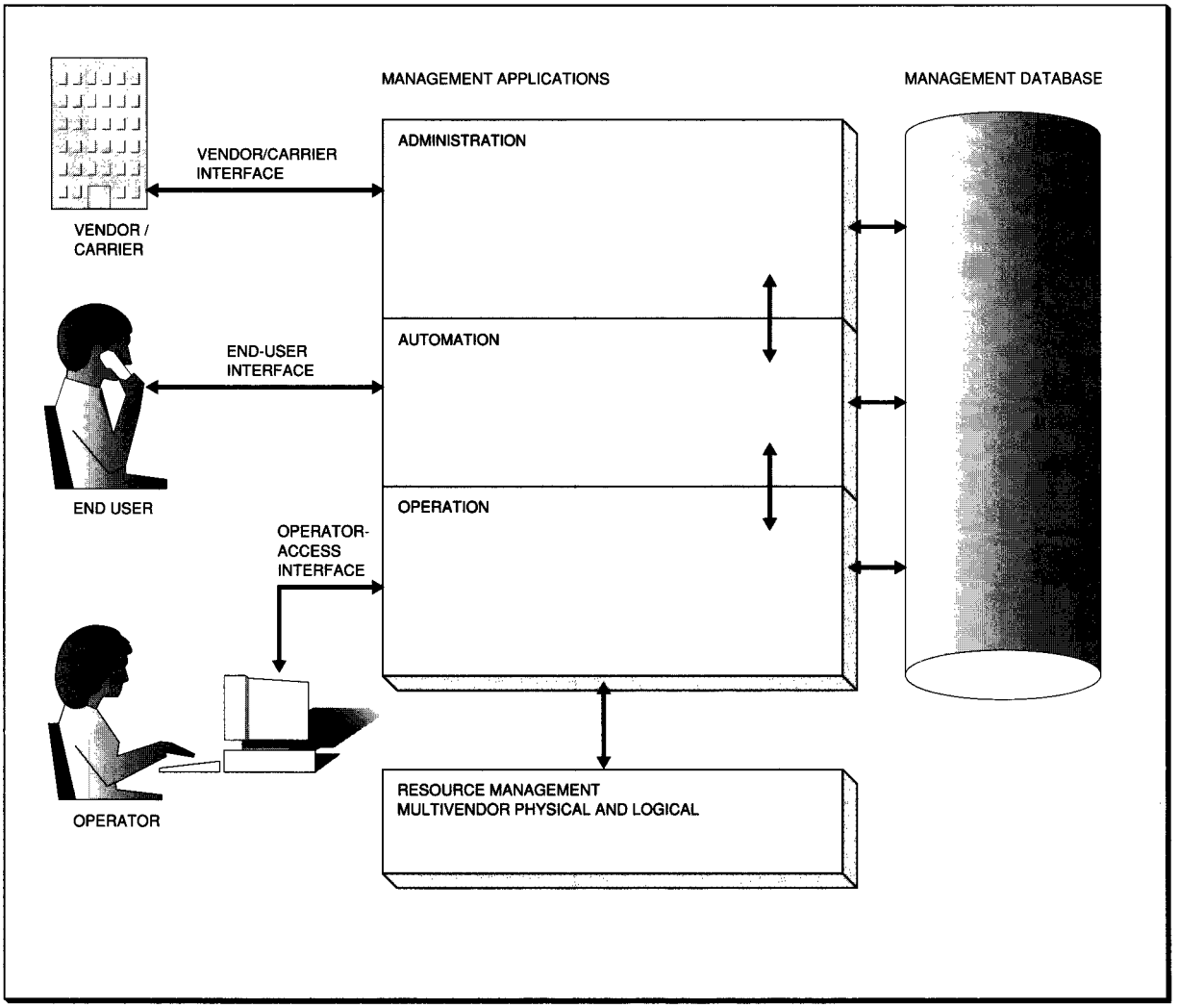
Resource management. Resource management is the capability to effectively manage and control any type of resource. The key functions that all multivendor physical and logical resources must support are the following:



- Event notification—Identifies failures and successful recovery, e.g., alerts and unalerts
- Two-way commands—Allow automation to control the bypass and recovery of failures
- Remote console—Allows a remote operator to take over control of a resource and perform any function that can be performed locally
- Configuration data—Report any dynamic changes about connectivity or asset data
- Performance data—Report any dynamic changes, such as threshold exceeded, or the current performance for the resource or environment

Management applications. Management applications are used in the administration, automation, and operation of a network. Applications used for administration provide the capability to support the disciplines of problem, change, and configuration management. Applications used for automation make it possible to perform unattended operations, including starting, stopping, monitoring of resources, the analysis of all applicable physical and logical data, alert correlation, bypass and recovery, and restoration of repaired components. Operation applications provide the

Figure 2 Multivendor management requirements



capability to understand and control the status of each resource, including the filtering of unimportant events and the conversion of other events into meaningful alerts.

Management database. The management database can be used to support the administration, automation, and operation applications.

Application interfaces. The application interfaces include capabilities to interface with the vendor, end user, and operator. The vendor/carrier interface provides the capability to automate the electronic vendor or carrier notification of problems and update vendor status when problems are fixed. The end-user interface allows the end user to automatically determine the status of the system and to take actions (i.e., reset terminal or log off), without the assistance of other individuals. The operator access interface makes it possible to consolidate all the information and control for multivendor products onto one graphical screen that will allow access to all of the data needed to effectively manage the multivendor environment.

Customers are looking for a set of management functions that completely automate the process-

ing of failures, are flexible enough to accommodate their unique needs, regardless of size, organizational structure, degree of centralization or decentralization, network configuration, rate of change and growth, or level of service provided to their end users. This means that the multivendor management functions must allow for both centralized management of the entire enterprise and the option to distribute control within the enterprise. Customers must be able to select devices and systems to meet their unique needs, while at the same time managing the network to optimize efficiency, productivity, and cost savings.

Multivendor management offerings

The multivendor management approach is to define enhancements that are needed to existing products to permit the customer to select multivendor management functions tailored to the customer's unique requirements. NetView* Extra[1] is a turnkey approach and a new way to address customer requirements for network management. The NetView Graphics and Automation offering and the NetView Multi-Vendor Operation offering are the first of many offerings planned to enable efficient network management and network resource optimization. IBM intends to provide other members of the NetView Extra family of packaged solutions. This offering provides multiple product integration, minimum customer resource investment, fast implementation, on-site education, and support services to address customer needs in the local area network (LAN) and multivendor environments.

It is important to understand that the word *offering*, as used in this paper, includes:

- Products—Both those of IBM and Business Partners
- Enabling software—Software tying the different products together
- Services—Installation, customization, and on-site customer education
- Support—Phone hotline, providing installers or customers with help on installation, customization, usage, PD (problem determination), or PSI (problem source identification) problems

One of the most important aspects of an offering is on-site education. Customers are shown how to use the NetView Extra offering after it has been installed and tailored to their unique needs. They become productive faster by learning how to use the offering to do their job and how to modify the offering for their specific environment.

The customer must first establish processes for problem, change, configuration, performance, and operational management. If the customer does not have good management discipline and procedures,[2] the NetView Extra offering will not solve the customer's basic problem.

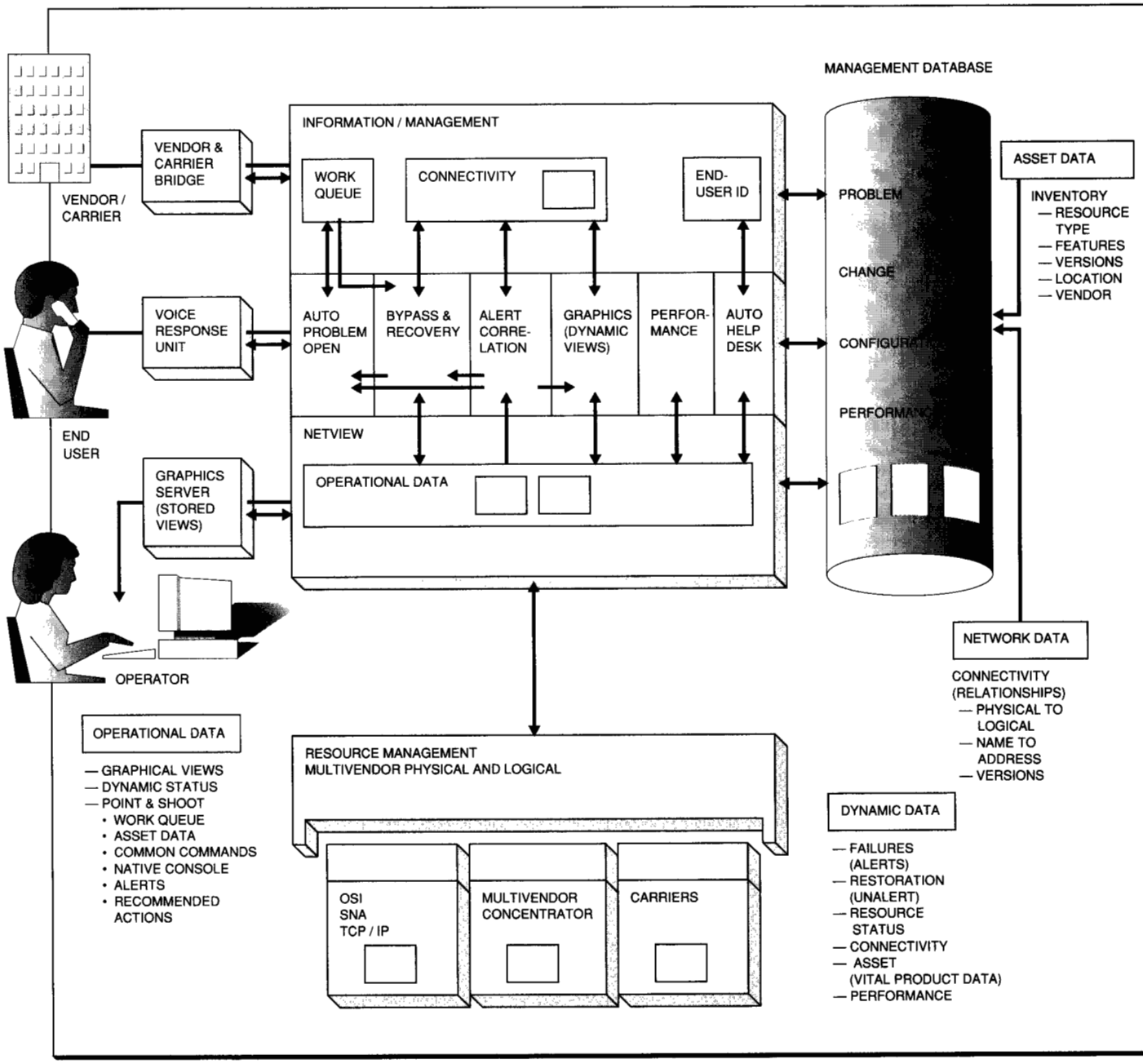
The key functions needed to satisfy the customer's multivendor operational problem management requirements are shown in Figure 3. The offering should provide a seamless view of multivendor management and consist of enhancements to existing products. Available products cannot satisfy all requirements by themselves because considerable tailoring and customization is needed to meet each environment. Products alone cannot provide the total solution.

Some basic function placement assumptions were made during the design of the product offerings. The overall goal is automatic, electronic handling of problems from start to finish, including failure detection, bypass and recovery, vendor notification, and restoration of repaired components. Next, enhancements needed to satisfy the customer's multivendor requirements should support open network management[3] and be built on existing products. The offerings must be developed in a way that will allow easy migration to SystemView*[4] products as they become available. Failures should be detected, bypassed, and recovered as close to the failure as possible. Finally, for those failures for which products are unable to perform bypass and recovery, notification must be passed to a higher automation level that understands the total environment and how to perform bypass and recovery by communicating with multiple products.

The multivendor management platform depicted in Figure 3 shows four different types of data that must be supported.

- Asset data—Inventory data that define each resource of the environment, i.e., resource type, serial number, features, versions, location, and vendor
- Network data—Connectivity data that define the relationships between products, such as physical to logical or name to address

Figure 3 Multivendor management platform



- Dynamic data—Live data that come from the different products that make up the environment, such as event notification, status changes, connectivity, asset, and performance
- Operational data—Data that provide access to all the asset, network, and dynamic data from the administration, automation, and operation applications, including data direct from the different resources

Asset data are manually entered into the database when the product is initially ordered. *Network*

data are manually added when it has been determined how the product will be connected to the environment. Once the product is installed and made operational, it will pass *dynamic data* about its current status and changes that were made since the last time it was connected. These data will be used in the operation and automation applications. The data are also passed to the administration application so the database can be updated with the latest information. The operator accesses the *operational data* from a graphical intelligent workstation to more effectively manage the environment.

Each product that attaches to the network must support event notification, two-way commands, remote console, and configuration and performance data. There are multiple ways for a product to send management data, shown at the bottom of Figure 3:

1. OSI, SNA, and TCP/IP. OSI[5] uses the Common Management Information Protocol (CMIP) to pass dynamic data. TCP/IP[6] uses the Simple Network Management Protocol (SNMP) to pass dynamic data. SNA[7] uses SNA Management Services to pass dynamic data. The architectures for OSI, TCP/IP, and SNA are published to allow multivendor support.
2. Multivendor concentrator. These are resources that provide support for other products that currently have not implemented a way to communicate with the multivendor management platform. A concentrator, such as NetView/PC*,[8] with customer or vendor applications, is used to pass dynamic data.
3. Carriers. The resources that make up the local exchange and interexchange carriers can either implement one of the architectures in category 1 or use a category 2 concentrator.

As errors are detected by each product, the unimportant ones have to be filtered out. Some errors need thresholding because a single error by itself is unimportant, but if the error is occurring at a fast rate, then action is needed. A product should also perform correlation of the cause and effect of errors. Once this is completed, bypass and recovery should be attempted. The results of these actions should be converted into meaningful alerts. Meaningful alerts break down the cause of the error into the following categories:

- User causes—Physical actions on the part of the user that result in an error, for example, powering off a modem
- Install causes—Conditions that may have been caused by activities surrounding the installation of new or updated hardware or software, for example, using the wrong terminal address
- Failure causes—Conditions that identify the most likely cause(s) of the error, for example, a communications adapter card failure

The alert also identifies the actions the automation function or operator should take to resolve the problem.

The alert should also include a failure categorization that will assist with routing the alert to the proper automation function and help prioritize which alerts should be worked on first. The following categories have been identified:

- Category 1 failure—The end user is down, the error data identify the specific cause of the failure, e.g., communications adapter card failure, and there is no automation available to attempt bypass and recovery
- Category 2 failure—The end user is down, the error data do not identify the specific cause of the failure, e.g., timeout, and there is no automation available to attempt bypass and recovery
- Category 3 failure—The end user is down, the error data identify a failure for which automation can restore service or threshold, and automation will attempt bypass and recovery
- Category 4 failure—The end user is not down, the error data identify a failure that has been bypassed or a threshold that has been exceeded

The NetView[9] product is being used as the base of our multivendor management platform (Figure 3). As dynamic data are received from the different types of resources, the data have to be converted into a format that can be used by the management applications. On top of this base are automation enhancements required to perform the different functions needed to effectively handle operational problems. The automation applications have to perform many of the same functions, such as thresholding, alert correlation, and bypass and recovery, that were performed by each product. The difference is that the automation applications have knowledge about the entire environment. Failures that were not recoverable by the products can now be bypassed and recov-

ered by communicating with multiple products. For example, a port failure may not be recoverable by a product, but by performing a port swap or reroute on two adjacent products, the failure can be successfully bypassed.

Once the alert is received, it has to be routed to the proper function. The following are descriptions of the various functions that are supported.

Alert Correlation isolates the cause and effect of failures. It is needed because most failures in a multivendor environment cause many event notifications to be sent from the different products affected by the error. Depending on the category of the failure, the alert will also be routed to the Bypass & Recovery automation or Auto Problem Open functions.

Bypass & Recovery automation takes category 3 failures and determines the connectivity of the path; a rules-based expert system executes the bypass and recovery for each specific failure, maintains the status of spare resources, and automates restoration of repaired components.

Auto Problem Open takes alerts, opens a problem record for new failures, and updates the status of existing problems. This eliminates duplicate problem records and allows for the use of prioritized work queues.

Graphics (dynamic views) provides the dynamic building of graphical views that show the relationship of the different products and their current status.

Performance provides the dynamic gathering of performance data from the different products.

Auto Help Desk allows end users to automatically determine the status of the system and to take actions, such as to reset a terminal or log off without the assistance of other individuals.

The Information/Management[10] product is being used as the base for the administration application. The problem, change, and configuration applications are being enhanced to meet the customer's multivendor requirements. Work Queue, Connectivity, and End-User ID, discussed next, are some of the supported functions.

The *Work Queue* allows the operator to see all of the open problems, in priority order, that the operator is responsible to correct. It includes the automated entry of problems that have or have not been successfully recovered, in a prioritized work queue. Duplicate problems update the problem record, but do not create new problem records. The operator, using Graphics and the Point & Shoot capabilities, can now work from one screen, rather than from multiple screens that are flooded with more messages than an operator can reasonably handle.

The configuration application has been enhanced to support *Connectivity* data for the multivendor environment. Connectivity data are also used to load the physical and logical views, and to provide path information for alert correlation and bypass and recovery.

End-User ID provides the end-user information needed to reset a terminal or log the user off the system.

The application interface is broken down into three major areas: Vendor & Carrier Bridge, Voice Response Unit, and Graphics Server. These functions are described next.

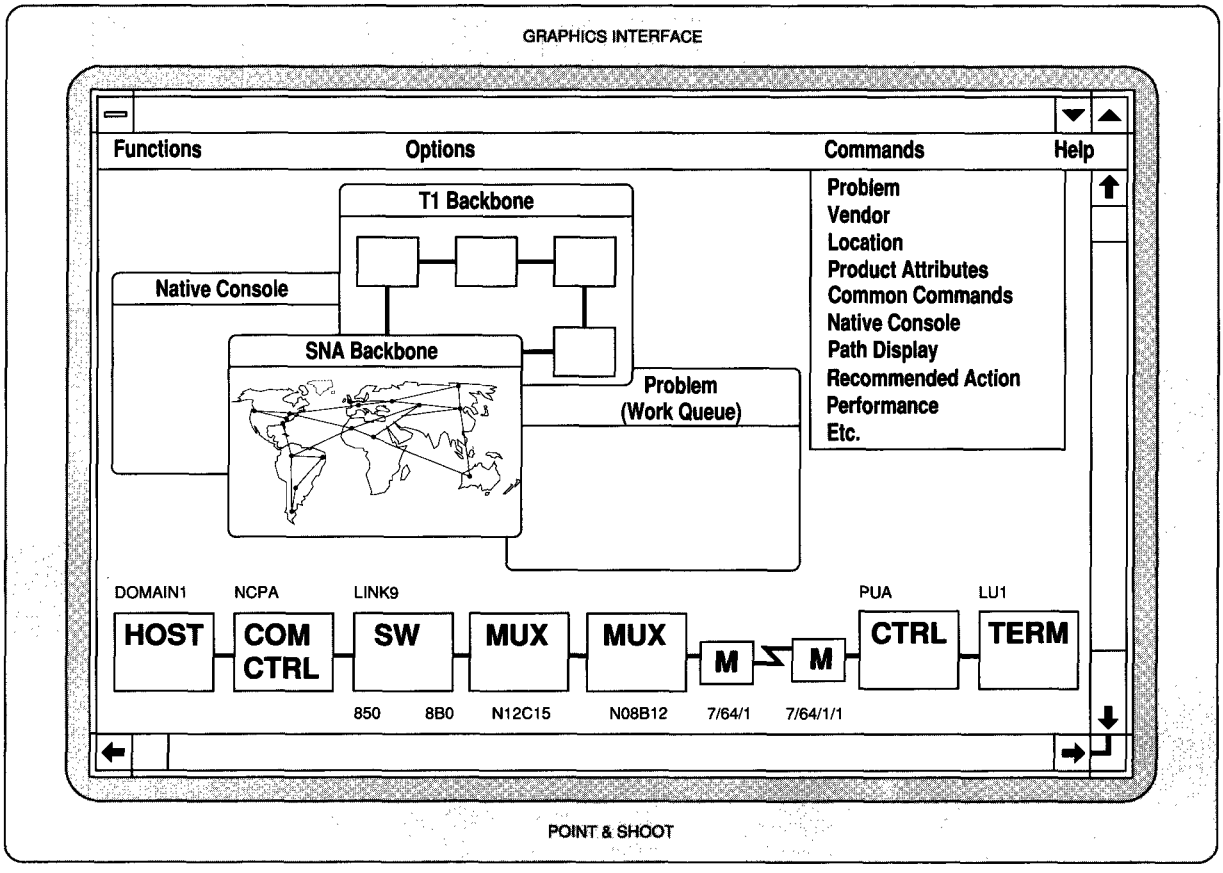
The *Vendor & Carrier Bridge* provides an electronic interface between the problem record and the vendor or carrier that allows notification of problems and update of vendor status when the problem is repaired.

The *Voice Response Unit* provides an electronic interface between the end-user's telephone and the management system. This allows the end user to determine the status of the system and to take predetermined actions.

The *Graphics Server* consolidates all the information and control for multivendor products onto one graphical intelligent workstation screen that will allow access to all data needed to effectively manage the environment. This includes a Point & Shoot capability that allows the operator to click on a graphical icon and pull down a menu that provides easy access to the different management applications.

The operator access to the management applications is illustrated in Figure 4. The operator can look at different types of views depending on the

Figure 4 Operator access to management applications



operator's responsibility. The T1 Backbone shows a physical view, the SNA Backbone shows a logical view, and at the bottom of the screen is a path view that shows both physical and logical resources. The path view is very important if you are trying to visually correlate alerts from multiple products about the same failure. For example, if a failure of modem 7/64/1 was reported by a NetView/PC application, the path view would also show that PUA and LU1 were affected by this failure. The path view function allows the operator to understand the relationship between the cause of the failure, modem 7/64/1, and the affected resources, PUA and LU1.

The Point & Shoot capability allows the operator at an intelligent workstation to easily communicate with the different management applications without having to re-enter data. The operator can select an icon and pull down a menu of functions that may be desired. For example, if the operator clicked on the modem 7/64/1 and selected the function Native Console from the menu, a window would be displayed that would allow the operator to control the modem as if directly connected to a modem control terminal. Unknown to the operator, the graphics application would determine the appropriate Native Console function to invoke for the selected resource. If this modem was being managed by a NetView/PC application, then it would probably invoke the NetView/PC Multi-Terminal ASCII Emulator/2 (MTAE/2) program. Another example could be clicking on the icon for PUA and selecting Problem. The graphics application would search the Information/Management problem application for a problem for resource PUA and display the results in a window. These are just a few examples of how user-friendly the graphics interface is.

Different individuals can use the multivendor management platform to more effectively handle operational problems.

The network operator uses the intelligent workstation graphical interface to monitor the multivendor environment. When the status of resources changes, the operator sees the color change on the graphical display. The Point & Shoot capability allows the operator to click on an icon and pull down a command menu that provides easy access to the different management applications. The goal is to automate as many of the operator tasks as possible. Ideally, the automation platform should eliminate the need for the operator to perform repetitive mundane tasks. The network operator may also use the problem work queue to determine the next highest priority problem to work on. If the operator is flooded with problems, the work queue helps put them in the proper priority.

The technical support group is usually busy working on problems. They want to be able to work out of a work queue on the next-highest priority problem that they are responsible to resolve. This usually takes place after automation has attempted to perform bypass and recovery for the failure.

The help desk uses the graphical interface to determine the status of resources. An end user may call the help desk to complain about a problem, such as "No system response for PC LU1." The help desk operator can use the path display to determine the status of LU1 and all the other resources in the path to the host.

Operational examples

This section describes how NetView, the automation applications, and Information/Management will be used to simplify multivendor management. Scenarios are included for different failures, which show how the multivendor management offerings automate the handling of enterprise problems, how the network operator, technical support group, and help desk can use this capability, and how the different functions work together.

T1 multiplexer port failure. A T1 multiplexer port failure is detected by T1 MUX, shown by a large "X" in Figure 5. This type of error cannot be bypassed and recovered by the product. The error message is captured by the service point SP and sent as an Alert Port Failure H12C15, which identifies port C15 on T1 MUX H12. The error was also detected by Com CTRL, which was trying to communicate with PUA. After the retries are exhausted for this error, it also sends an Alert Timeout PUA.

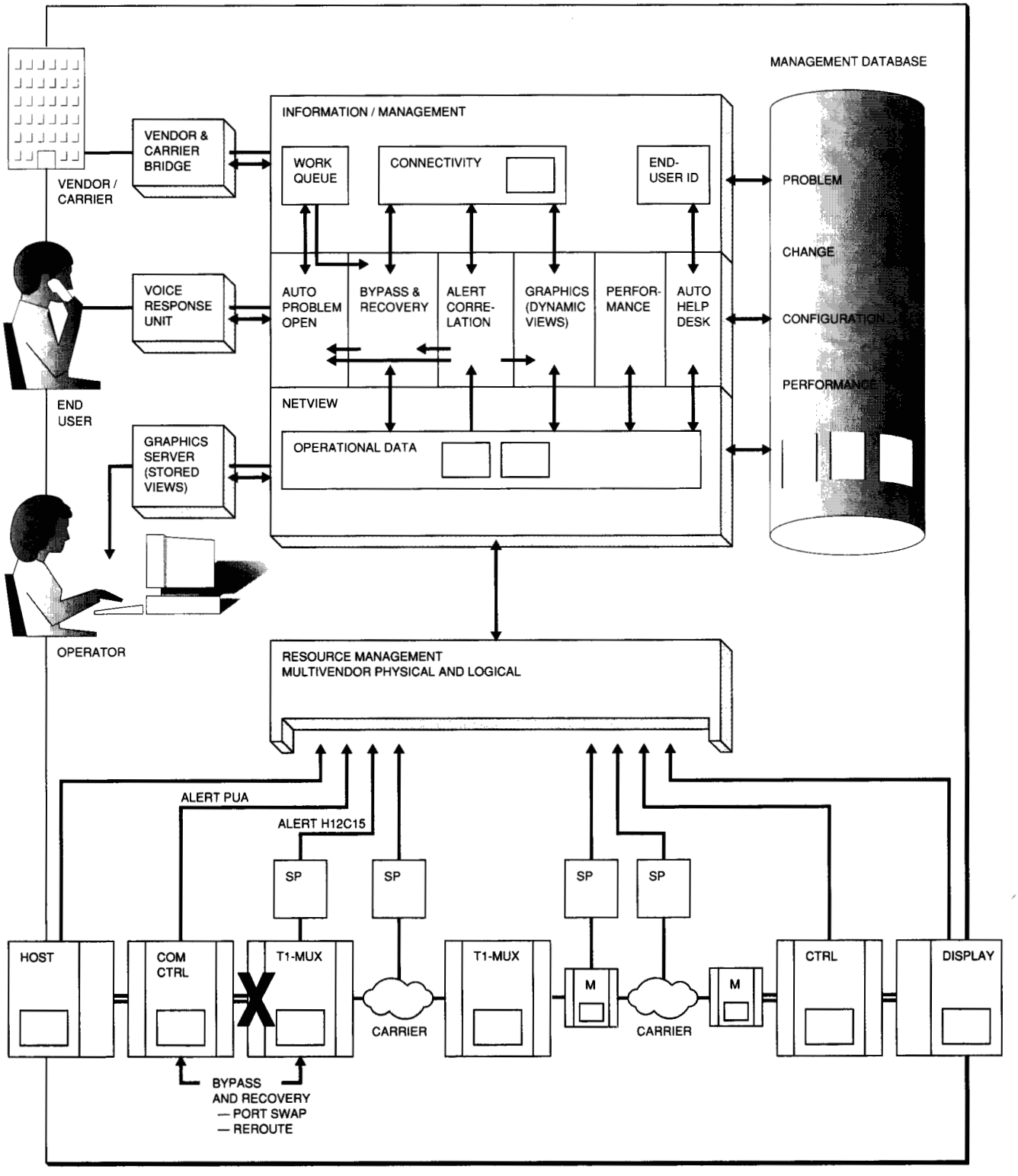
The help desk, network operator, and technical support group can use the multivendor offerings.

As these two alerts are received at the Alert Correlation function, they are first logged on an events database. Next, they are passed to the Graphics function for display. The alerts are then put into a buffer and a timer is started, which allows for the network delay that may be associated with multiple notifications arriving at different times. Once the timer has expired, path connectivity information is obtained to see if there are any other resources in the buffer for this path. This process eliminates the cause and effect for each failure. In this scenario, the resource that caused the failure is H12C15, and the affected resource is PUA. The Graphics function is updated to show that PUA is now an affected resource and not the cause of the failure.

Category 1 failures are passed to the Auto Problem Open function, which will determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

Category 2 failures are eliminated if a category 1 failure can be found in the same path. In this scenario, Alert Timeout PUA is a category 2 failure. If a category 1 failure cannot be found and the cause of the problem cannot be determined by testing, then the alert is passed to the Auto Problem Open function, which will determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

Figure 5 Multiplexer port failure



Category 3 failures are passed to the Bypass & Recovery function. In this scenario, Alert Port Failure H12C15 is a category 3 failure. The first step in the bypass and recovery process is to update the Graphics function that the automation function is working on this problem, and to test the failing component to see if it is still failing. If it is still failing, path connectivity information is obtained to see how it should be bypassed. For this failure, a spare port on the Com CTRL and a spare port on T1-MUX will be used to perform the bypass. These spare components are maintained by the Bypass & Recovery function. The appropriate commands are sent to the Com CTRL to perform a port swap, and a reroute command is sent to the T1-MUX to reroute the output port to the new input port. Once this is completed and tested, recovery of the path would be performed by restarting the resources that were affected by this failure.

The Graphics function is updated, indicating that the resources are now operational again, and a category 4 failure is generated and passed to the Auto Problem Open function to determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

The next major function is the Work Queue function, which allows the operator to work from one screen to view a problem list that is in priority order. When the operator selects the problem it can be assigned to the vendor responsible for service of the T1 MUX. The operator can determine the vendor by clicking on the problem record and using the pull-down menu to select a vendor. Once the vendor's name is entered into the problem record, it will be sent to the vendor electronically. When the vendor fixes the port failure in H12C15, an electronic notification will be received and entered into the problem record.

To restore the system, the operator can select the common commands, allowing the operator to send a command to the Bypass & Recovery function. All the operator has to enter is "restore H12C15." The restore function will determine the original path and the components that were used for bypass. It will first test the H12C15 port to see if it was really fixed, before moving everything back to the original path and restoring the spare components to the spare pool, so they can be used for the next failure.

Modem failure. A modem failure is detected by M, shown in Figure 6 by a large "X." This type of error cannot be bypassed and recovered by the product. The error message is captured by the service point SP and sent as an Alert Modem Failure 7/64/1, which identifies the modem. The error was also detected by Com CTRL, which was trying to communicate with PUA. After the retries were exhausted for this error, it also sends an Alert Timeout PUA.

As these two alerts are received at the Alert Correlation function, they are logged on an events database. Next, they are passed to the Graphics function for display. Figure 4 illustrates how the graphical interface would look, with three resources highlighted at the bottom of the screen. The terminal LU1 becomes inoperative at the same time that the PUA timeout occurs. The alerts are then put into a buffer and a timer is started, allowing for the network delay that may be associated with multiple notifications arriving at different times. Once the timer has expired, path connectivity information is obtained to see if there are any other resources in the buffer for this path. This process eliminates the cause and effect for each failure. In this scenario, the resource that caused the failure is 7/64/1 and the affected resource is PUA. The Graphics function is updated to show that PUA is now an affected resource and not the cause of the failure.

Category 1 failures are passed to the Auto Problem Open function, which will determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

Category 2 failures are eliminated if a category 1 failure can be found in the same path. In this scenario, Alert Timeout PUA is a category 2 failure. If a category 1 failure cannot be found and the cause of the problem cannot be determined by testing, then the alert is passed to the Auto Problem Open function, which will determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

Category 3 failures are passed to the Bypass & Recovery function. In this scenario, Alert Modem Failure 7/64/1 is a category 3 failure. The first step in the bypass and recovery process is to update the Graphics function that the automation

Figure 6 Modem failure

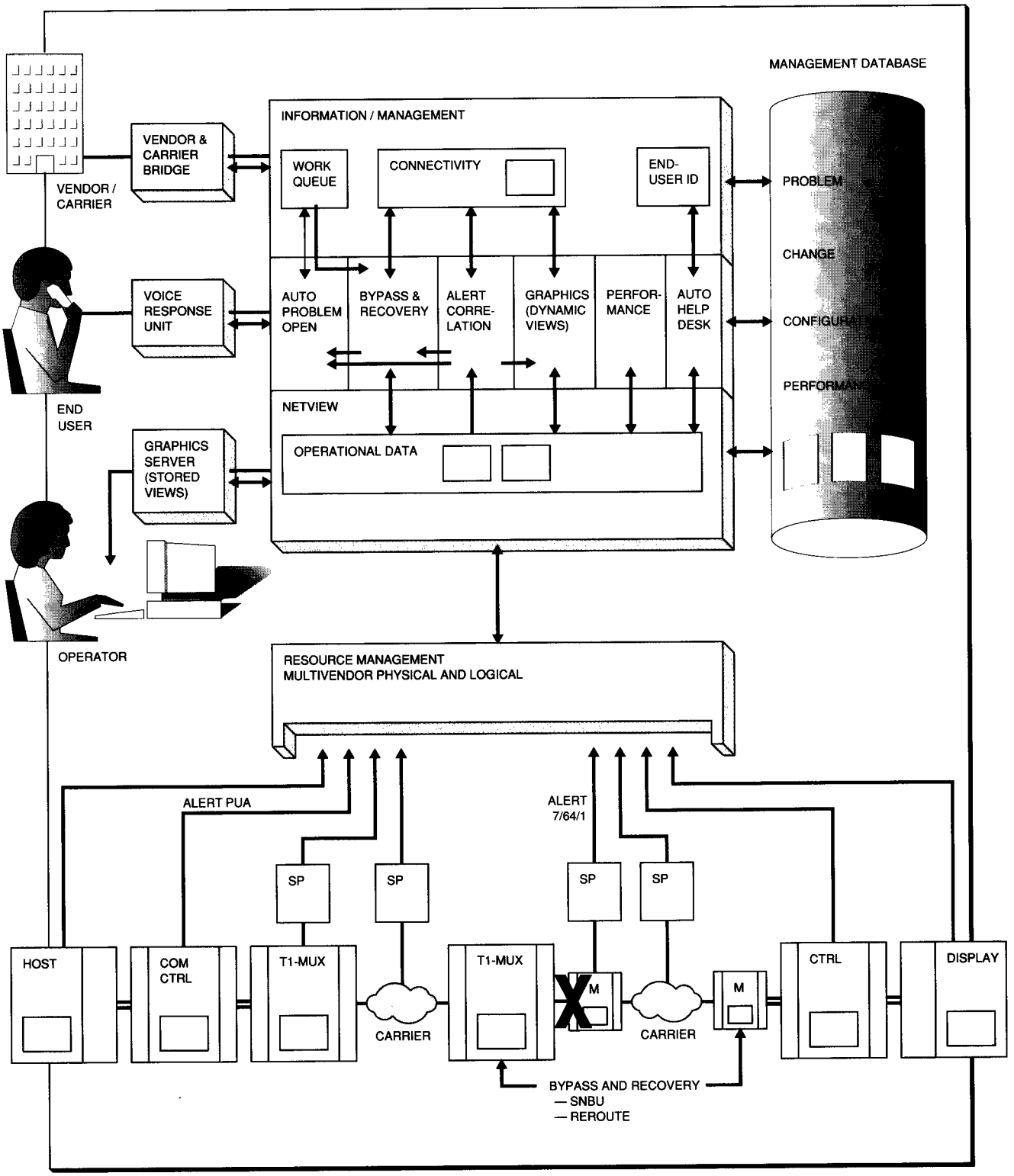
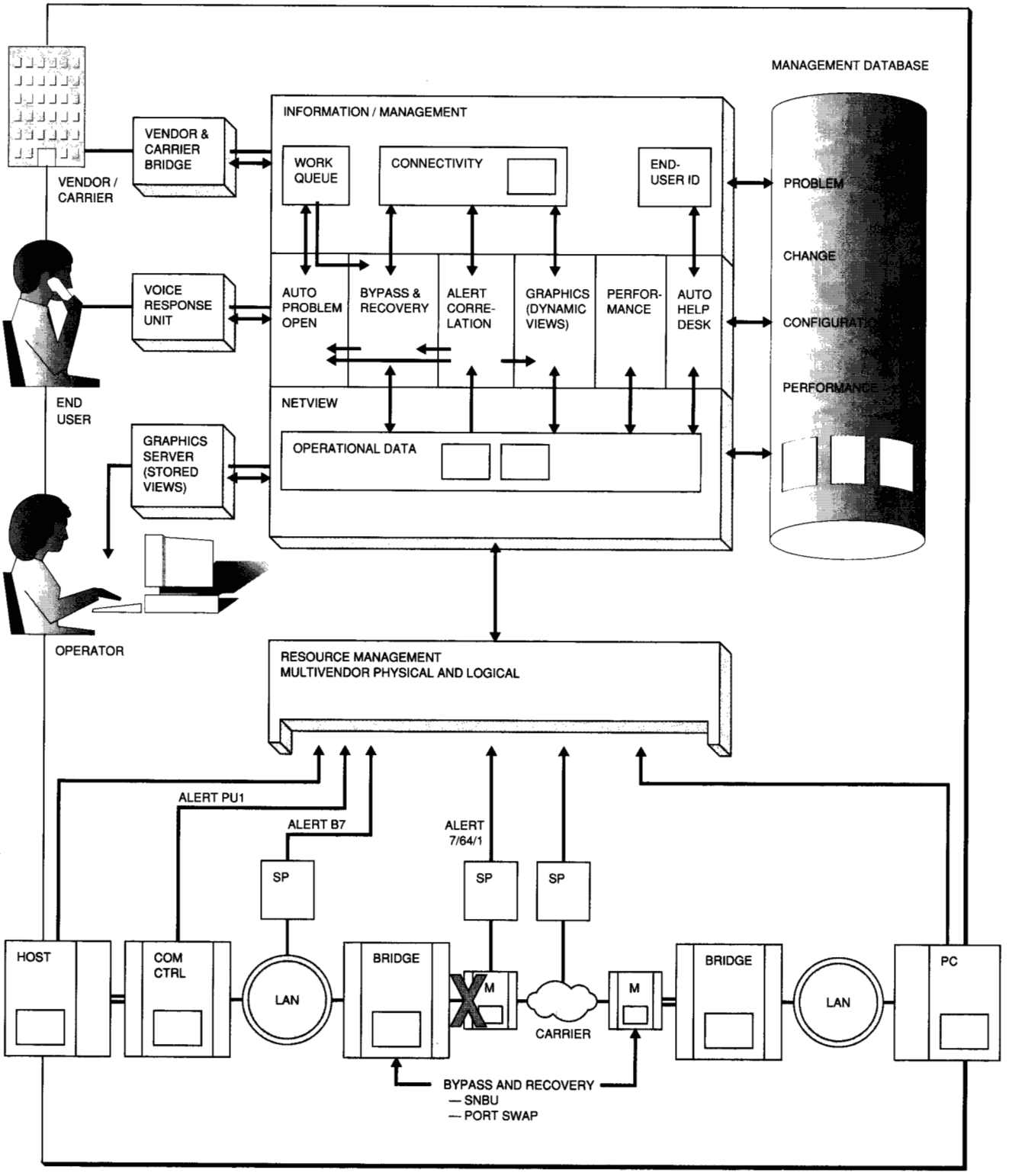


Figure 7 LAN split bridge modem failure



function is working on this problem, and to test the failing component to see if it is still failing. If it is still failing, path connectivity information is obtained to see how it should be bypassed. For this failure, a spare modem and a spare port on TI-MUX will be used to perform the bypass. These spare components are maintained by the Bypass & Recovery function. The appropriate commands are sent to the modem SP to perform switched network backup (SNBU), and a reroute command is sent to the TI-MUX to reroute the input port to the new output port. Once this is completed and tested, recovery of the path would be performed by restarting the resources that were affected by this failure.

The Graphics function is updated, indicating that the resources are now operational again, and a category 4 failure is generated and passed to the Auto Problem Open function to determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

The next major function is the Work Queue, which allows the operator to work from one screen to view a problem list that is in priority order. When the operator selects the problem, it can be assigned to the vendor responsible for service of the modem. The operator can determine the vendor by clicking on the problem record and using the pull-down menu to select a vendor. Once the vendor's name is entered into the problem record, it will be sent to the vendor electronically. When the vendor fixes the modem failure in 7/64/1, an electronic notification will be received and entered into the problem record.

To restore the system, the operator can select the common commands, allowing the operator to send a command to the Bypass & Recovery function. All the operator has to enter is "restore 7/64/1." The restore function will determine the original path and the components that were used for bypass. It will first test the 7/64/1 modem to see if it was really fixed, before moving everything back to the original path and restoring the spare components to the spare pool, so they can be used for the next failure.

LAN split bridge modem failure. A LAN split bridge modem failure is detected by M, shown in Figure 7 by a large "X." This type of error cannot be bypassed and recovered by the product. The error message is captured by the service point SP and sent as an Alert Modem Failure 7/64/1, which identifies the modem. The error was also detected by Com CTRL, which was trying to communicate with PU1. After the retries were exhausted for this error, it also sent an Alert Timeout PUA. The service point SP managing the LAN detected a failure; the bridge was congested because of the modem failure. This was sent as an Alert Bridge Congestion B7.

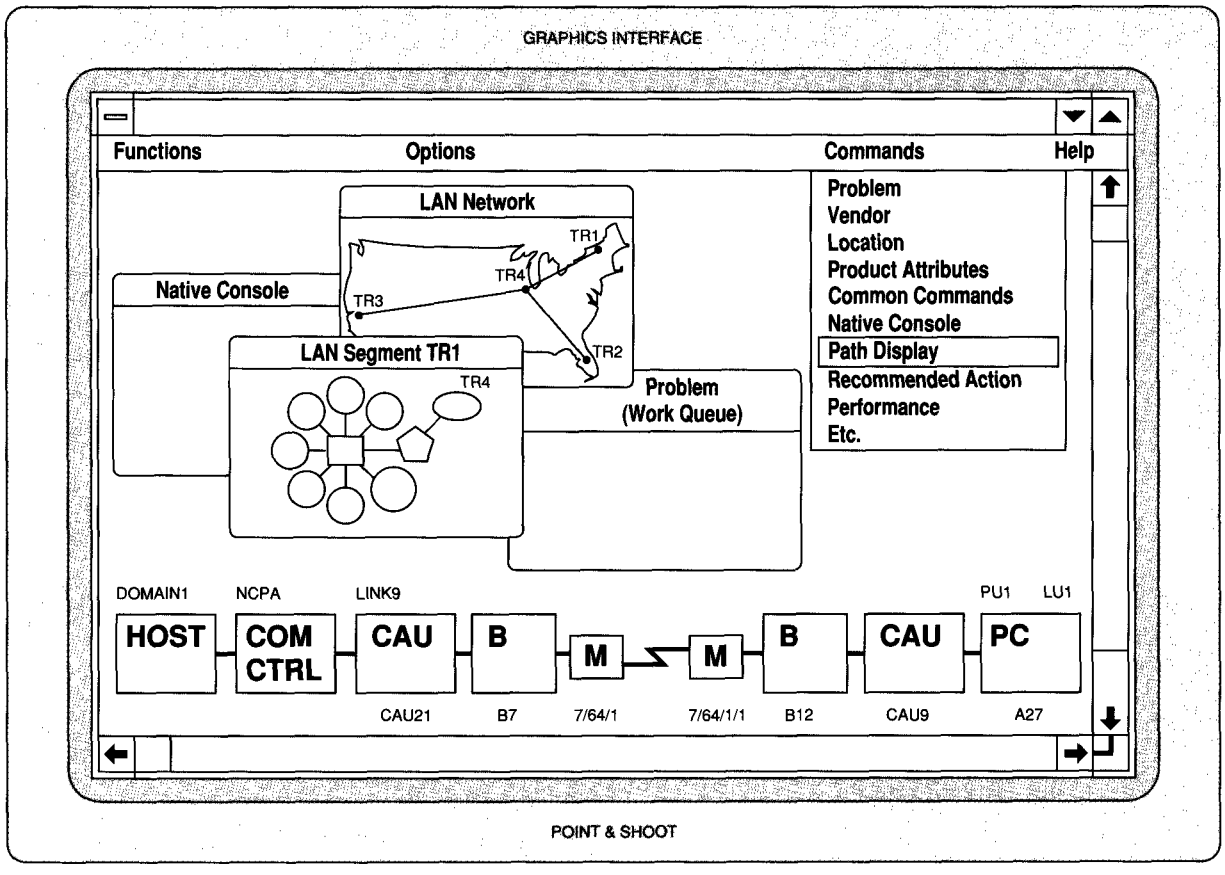
As these three alerts are received at the Alert Correlation function, they are first logged on an events database. Next, they are passed to the Graphics function for display. Figure 8 indicates how the graphical interface would look, showing three resources highlighted at the bottom of the screen. The alerts are then put into a buffer and a timer is started, allowing for the network delay that may be associated with multiple notifications arriving at different times. Once the timer has expired, path connectivity information is obtained to see if there are any other resources in the buffer for this path. This process eliminates the cause and effect for each failure. In this scenario, the resource that caused the failure is 7/64/1 and the affected resources are B7, PU1, and LU1. The Graphics function is updated to show that B7, PU1, and LU1 are now affected resources and not the cause of the failure.

Category 1 failures are passed to the Auto Problem Open function, which will determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

Category 2 failures are eliminated if a category 1 failure can be found in the same path. In this scenario, Alert Timeout PUA and Alert Bridge Congestion B7 are category 2 failures. If a category 1 failure cannot be found and the cause of the problem cannot be determined by testing, then the alert is passed to the Auto Problem Open function, which will determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

Category 3 failures are passed to the Bypass & Recovery function. In this scenario, Alert Modem Failure 7/64/1 is a category 3 failure. The first step in the bypass and recovery process is to update the Graphics function that the automation function is working on this problem, and to test

Figure 8 Operator access, LAN example



the failing component to see if it is still failing. If it is still failing, path connectivity information is obtained to see how it should be bypassed. For this failure, a spare modem and a spare port on the bridge will be used to perform the bypass. These spare components are maintained by the Bypass & Recovery function. The appropriate commands are sent to the modem SP to perform switched network backup (SNBU), and a port swap command is sent to the bridge. Once this is completed and tested, recovery of the path would be performed by restarting the resources that were affected by this failure.

The Graphics function is updated, indicating that the resources are now operational again, and a category 4 failure is generated and passed to the Auto Problem Open function to determine if this is a new problem and a problem record should be opened, or if an existing problem record needs to be updated.

The next major function is the Work Queue, which allows the operator to work from one screen to view a problem list that is in priority order. When the operator selects the problem, it can be assigned to the vendor responsible for service of the modem. The operator can determine the vendor by clicking on the problem record and using the pull-down menu to select a vendor. Once the vendor's name is entered into the problem record, it will be sent to the vendor electronically. When the vendor fixes the modem failure in 7/64/1, an electronic notification will be received and entered into the problem record.

To restore the system, the operator can select the common commands, allowing the operator to

send a command to the Bypass & Recovery function. All the operator has to enter is "restore 7/64/1." The restore function will determine the original path and the components that were used for bypass. It will first test the 7/64/1 modem to see if it was really fixed, before moving everything back to the original path and restoring the spare components to the spare pool, so they can be used for the next failure.

Conclusion

To provide customers with effective multivendor network management offerings, it is necessary that all products that connect to the network support event notification, two-way commands, remote console, configuration data, and performance data.

Initial NetView Extra offerings provide a new approach to meeting customer requirements. The approach integrates multiple products, and provides on-site services and expanded support. These offerings provide a solid foundation for customers interested in moving to SystemView. The offerings will be enhanced as the SystemView products become available.

*Trademark or registered trademark of International Business Machines Corporation.

**Trademark or registered trademark of Digital Equipment Corporation.

Cited references

1. *NetView Extra Marketing Announcement*, 391-133, and *NetView Graphics and Automation Offering*, G326-0008, IBM Corporation; both available through IBM branch offices.
2. *A Management System for the Information Business, Volume 1, Management Overview*, GE20-0062, IBM Corporation; available through IBM branch offices. This document contains references to related publications.
3. *Introduction to IBM's Open Network Management*, GC30-3431, IBM Corporation; available through IBM branch offices.
4. *IBM Systems Application Architecture: An Introduction to SystemView*, GC23-0578, IBM Corporation; available through IBM branch offices.
5. *Open Systems Interconnection (OSI) Reference Summary*, G221-3025, IBM Corporation; available through IBM branch offices.
6. *Introducing IBM's Transmission Control Protocol/Internet Protocol Products for OS/2, VM, and MVS*, GC31-6080, IBM Corporation; available through IBM branch offices.
7. *SNA Formats*, GA27-3136, IBM Corporation; available through IBM branch offices.
8. *NetView/PC Application Program Interface/Communications Services Reference*, SC30-3313, IBM Corporation; available through IBM branch offices.
9. *NetView at a Glance*, GC31-6114, IBM Corporation; available through IBM branch offices.
10. *Introducing the Information/Family*, GC34-4170, IBM Corporation; available through IBM branch offices.

Accepted for publication December 13, 1991.

John G. Stevenson *IBM Networking Systems, P.O. Box 12195, Research Triangle Park, North Carolina 27709.* Mr. Stevenson joined IBM in 1967 as a customer engineer in Waldwick, New Jersey. Currently he is an IBM Senior Technical Staff Member in the Complex Systems Support organization and is responsible for providing technical direction for customer network solution offerings.

Reprint Order No. G321-5469.