NBBS network management

by S. A. Owen

Network management for Networking BroadBand Services (NBBS), a general-purpose, multiprotocol, high-speed transport backbone is discussed. The paper begins with the objectives and the key choices made in the development of the network management solution. The managed environment for high-speed transport networks and some features of the NBBS architecture that have influenced the network management solution are described, along with the relationship between the network manager and the managed target system agent, the actual communication environment for the Nways™ Switch Manager. The relationship between the Network Management Workstation and an NBBS node acting as a network management agent is presented. The use of managed object classes to provide a Management Information Base (MIB) that may be accessed by a manager using the Common Management Information Protocol (CMIP) to manage NBBS networks is then discussed. Management application models for accounting, configuration, topology, performance, and fault management for NBBS are illustrated, showing how they relate to the NBBS managed objects. The paper concludes with a look at future directions for the NBBS management solution.

Network managers are concerned with various aspects of networks, including initialization, operational characteristics and health, usage, and asset and data security. Over the last ten years, network management services have broadened the original focus on fault management for reporting and working around network problems to offer customers expanded applications in the areas of topology, configuration, performance, and usage accounting. Specific topics such as log control and scheduling have even found their way into network management definitions promulgated by standards bodies. Networking BroadBand Services (NBBS) network management has been defined to support these diverse functions, while embracing standards and incorporating innovations. This paper describes this support.

The sections that follow begin with background: past management concepts paving the way for NBBS management, major objectives that influenced its basic direction, some fundamental choices made in the overall NBBS management approach, and NBBS control characteristics that ease network management. Next there is a discussion of the NBBS network environment that is to be managed, and the effect the unique NBBS technology characteristics have had on the management solution. The paper then covers the enumeration of, and the rationale behind, the key managed objects and their categories defined at "agent" NBBS nodes. Next there is a discussion of management applications at the NBBS network manager and their use of the managed objects. The paper concludes with a brief discussion of possible future enhancements and directions.

The NBBS network management architecture has drawn upon existing IBM network management ideas. First, the concept of a *focal point*[1] responsible for the management of a large number of distributed network components and supporting many different management applications was seen as crucial to a complete management solution for NBBS.

Second, the appeal of a network management solution that concentrates on the hardware and technology aspects of the NBBS subnetwork, much as was done for management of local area networks (LANs),[2] was also fundamental. The focal point management model allowed a manager to bring a rich set of centralized network application programs to apply across multiple subnetworks, while the LAN management model introduced the concept of controlling a wide range of specific components—protocol, logical, and physical—from a single manager platform. Combining these two notions into NBBS network management has resulted in a system that supports the configuration of the network elements, or nodes, at a logical level, while allowing the physical component level to be managed directly by the manager applications.

Both CMIP and SNMP use the concept of a MIB to represent the managed resources.

Three major objectives—network scalability, dynamic end-to-end network connection setup, and generic transport support over wide area networks—also influenced the network management direction for NBBS networks.

The requirement to be able to scale NBBS, not just as a networking transport architecture, but as a realization of a product family—with low-end systems used to interconnect campus applications and high-end systems used for wide-area interconnection—meant that stand-alone management functions were needed that could be deployed for any size network. Network size, however, was not to be the criterion for determining the management function offering. Common applications were needed to span all network configurations, such that the integration of a campus NBBS cluster and a wide-area NBBS cluster would require no new application definition. In short, the seamless, "plug-and-play" characteristics of NBBS were to apply to the network management environment as well.

The nature of the NBBS architecture also played a role in requirements placed on the management of transport connection establishment. The NBBS connection setup process is based on connection origin information. It does not require direct intervention by management in intermediate network elements for setting up a connection path, as is the case in subnetwork architectures[3,4] that rely on route selection through static physical link designation and require explicit operation triggers for path activation. Using NBBS network management, there is no need for intermediate node definition for each connection being set up. The origin path selection component is able to use the connection request parameters, such as the quality-of-service parameters specifying connection cell loss, end-to-end delay, nondisruptive path rerouting, and connection preemption and holding priorities, and the initial bandwidth parameters for peak rate, mean rate, and mean burst duration as they are configured by the network administrator in the origin connection request for route selection—again without management intervention. The only requirement for network management is to be able to define the initial input values at the connection origin, with NBBS processing taking care of the connection setup and path selection.[5] A benefit of using this type of model for connection definition is that the procedures for defining permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) are similar. Detailed aspects of the connection setup model are presented later.

The central purpose of NBBS is to serve as a general-purpose, multiprotocol, transport backbone for wide area networks (WANs). Although different protocol and traffic types all have special characteristics, NBBS developed a generic treatment for traffic transport that avoids special-case processing for each different protocol that attaches to the NBBS network. A corresponding generic network management solution has also been developed. The NBBS network management model accommodates the generic WAN transport architecture as well as, on a case-by-case basis, the specific access protocol or traffic. This approach permits the management of NBBS networks of homogeneous access protocols totally dedicated to a single type of access protocol, such as a frame-relay or asynchronous transfer mode (ATM) WAN, or a network of heterogeneous access protocols serving the transport needs of LAN, frame relay, ATM, and voice users, using the same network management model and applications.

Another fundamental consideration was the selection of the network management technology for NBBS node management and manager-agent interactions. The choice was basically between the two open industry standards, Common Management Information Protocol (CMIP)[6] and Simple Network Management Protocol (SNMP).[7] CMIP was developed and supported by advocates of Open Systems Interconnection, with most Service Provider Environments (SPEs) making it part of their Telecommunications Management Network.[8] SNMP is supported universally by the LAN and router community.

Each technology has points of merit. Both technologies use the concept of a management information base (MIB)[9] to represent the managed resources in a target system. A MIB is a repository of management information that can be accessed and used to control resources of a system. The NBBS network management solution uses a MIB to define the managed resources of the NBBS node.

Both technologies also use the manager-agent paradigm. In this management model, the agent is the repository for the MIB for the system. The manager is the application center that extracts MIB information from agents and modifies agent MIB information to effect status and configuration changes in the target agent resources. As a general rule, using SNMP, the agent remains silent unless queried for information. Using CMIP, the agent may actively inform the manager of events that are considered significant.

Each management technology can claim a large base of standard MIBs that are already available or being developed. For SNMP, the Internetwork Engineering Task Force is the major focus for this activity.[10] For CMIP, in addition to the efforts by the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU) in defining base standards, the Network Management Forum has been developing ensembles to demonstrate interoperability scenarios with CMIP MIBs.

Because of the prevalence of CMIP in the wide area network SPE context, and the various technical benefits CMIP offers—discussed further later in this paper—NBBS network management uses CMIP for its manager-agent interactions. NBBS network management uses defined standards from both the SNMP and CMIP models to define components for the NBBS agent MIB. The detailed reasons for this are also discussed later.

Thus, the model for the management of NBBS draws on several standards as sources for its constituent elements, with standards used in two basic ways: as a technology base for manager-agent interactions and as a source of MIB contents to be further refined to fit the NBBS environment.

NBBS uses CMIP for manager-agent interactions, and both CMIP and SNMP for a source of MIB contents.

The standards of CMIP and Guidelines for the Definition of Managed Objects (GDMO)[11] are used in the definition of the base management platforms for both the manager and the agents. Managed object classes are defined for management purposes in order to emit notifications from resources and to provide operational access to resources. The managed resources may be physical or logical resources. Access to the states or characteristics of the resources is possible only by the methods defined for the managed object class, and access is common to all members of the managed object class. CMIP defines a standard message format for manager-agent messages involving basic operations, such as GET, SET, ACTION, and NOTIFICATION. GDMO defines the structure of the information contained in the MIB. It defines managed object classes and their attributes, parameters, actions, and notifications, and provides packages for grouping and accessing attributes. Therefore, the manager and agents both define management information according to the same principles, using the GDMO structure for the MIB, and communicate using CMIP standard exchanges.

Various standards have also been used in developing the semantic contents of the NBBS MIB. MIBs defined by standards bodies were examined to determine whether they fit the management requirements of NBBS. In particular, the ISO/IEC 10165-2,[12]

which contains rudimentary definitions in the form of managed object classes for managing communication protocol connections, was used. Additional attributes were added to the standard managed object classes to form the particular managed object class used in the NBBS MIB. For example, the ISO/IEC 10165-5[13] defined managed object class, simpleConnection, was refined by the addition of bandwidth and connection path attributes to become the abConnection managed object used by NBBS.

The source of definition for the NBBS MIB relies also on non-CMIP standards. Until recently, no CMIP standard MIBs were defined for certain protocols. For example, network management protocol standards for frame relay and ATM have been defined predominantly for SNMP technology. But the interoperability of CMIP and SNMP has not yet been standardized,[14] so, in these cases, the CMIP managed object class definition used for NBBS for frame relay and ATM was built by refining the protocol components derived from the SNMP MIB standards. The result was a CMIP MIB having components identical to the SNMP definitions, thereby creating a form of semantic equivalence to the SNMP MIBs.

The management of high-speed networks typically entails setting up paths for permanent virtual circuit (PVC) connections by selecting and manipulating the nodes of the network and their resources, a time-consuming and human-intensive network management operation. However, NBBS technology advances in the automation and packaging of the control functions used by the high-speed WAN relieved network management from the tedium of node and path selection,[15] allowing the network management focus to be on the treatment of the access user and network connection endpoint.

Three particular features of NBBS control-point and directory services—the use of a spanning tree, distributed topology information, and built-in search capability—relieved network management of the need to intervene in operational aspects of WAN control for network connection setup.

The NBBS spanning tree control functions[16] permit the automatic creation of a spanning tree for the dissemination of control information throughout the NBBS network. The spanning tree is refined by algorithmic computation each time a [tree] trunk is connected to a node in the network. Tree rebalancing occurs if needed. Moreover, failures of trunks on the spanning tree, or complete node failures, cause an automatic restructuring of the spanning tree.

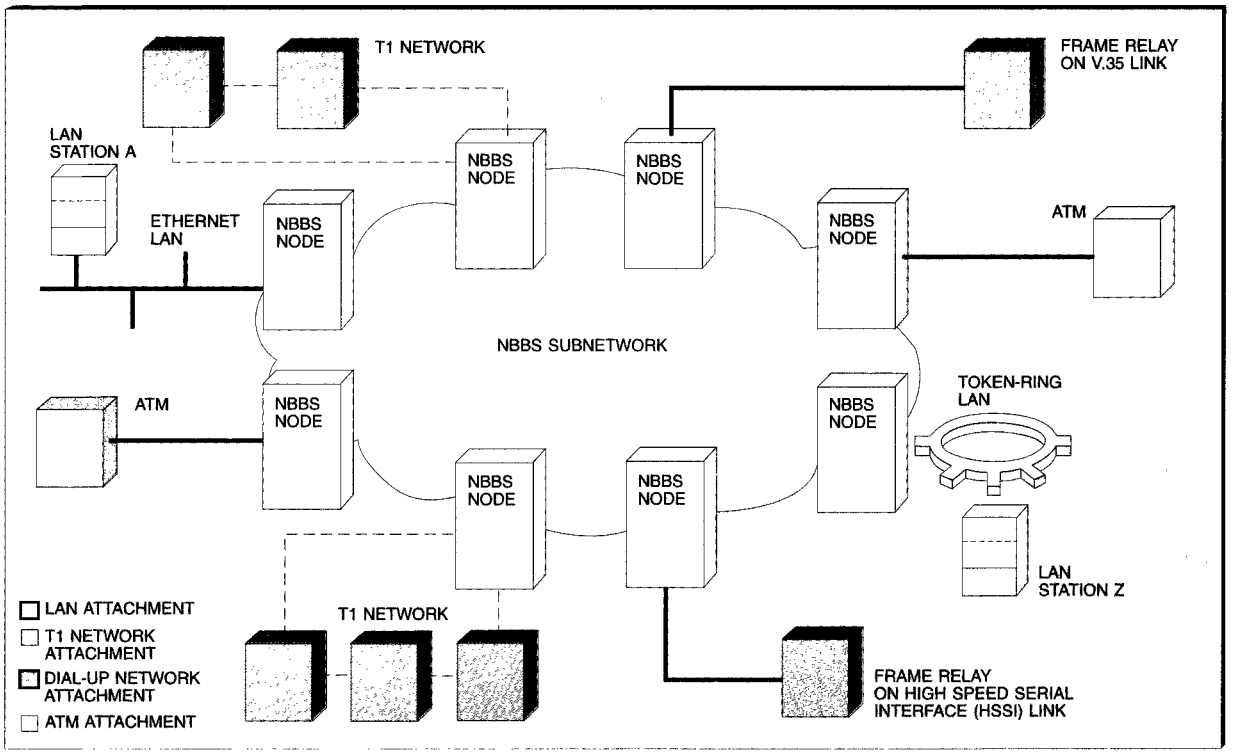
This capability to select and set up the spanning tree means that network management is not involved in selecting the spanning-tree root or its path through the network by explicitly selecting trunks for the tree topology. Automated spanning-tree repair relieves network management of the burden of constantly monitoring the spanning tree to accommodate new nodes or changes due to trunk or node failure. Network management is not involved in deciding how to build the route and in what order to connect the network nodes.

NBBS topology control functions[16] automatically exchange network topology information to provide each network node with up-to-date information about the availability and utilization of paths between nodes in the NBBS network. Since this updated status of the transport network resources is distributed to every node in the network, the path selection required for network setup can be computed at the origins and verified "in-flight" during connection setup. Successful connection setups create updates to the topology information, which is then periodically distributed to the WAN nodes as updates.

This capability to distribute and update network topology data means that network management is free of the burden of configuring, for each PVC or SVC, a particular node in the way a traditional channel-bank or cross-connection switch has been configured in the past. That is, there is no need to supply each switch in a path with explicit details of which ingress channel or port, for example, is to be connected to which egress channel or port for a network connection. The tedious setting of intermediate switches in a path is done automatically by NBBS control functions. Network management is not involved in the actual setting of intermediate switches but learns and records the path configuration for each network connection after the connection has been set up.

The access function of directory services[17] enables the administration of WAN users to be done at local facilities rather than a central location. Directory searches at network connection setup time locate the node and port for each target resource in the network, meaning that users can migrate throughout the network and the directory mech-

Figure 1 Attachments to the NBBS subnetwork



anism will locate their current home. Therefore, while configuring a user to a particular port on a particular node is a network management activity, knowledge of the target node or port for connection setup is not required by network management because of the directory services capabilities.

The managed network environment

The NBBS architecture defines a collection of nodes with knowledge of one another that provides transport services for various traffic types. For the purpose of network management, the major functions that define the manageable operations of NBBS are attachment to NBBS nodes and transport services provided by NBBS nodes.

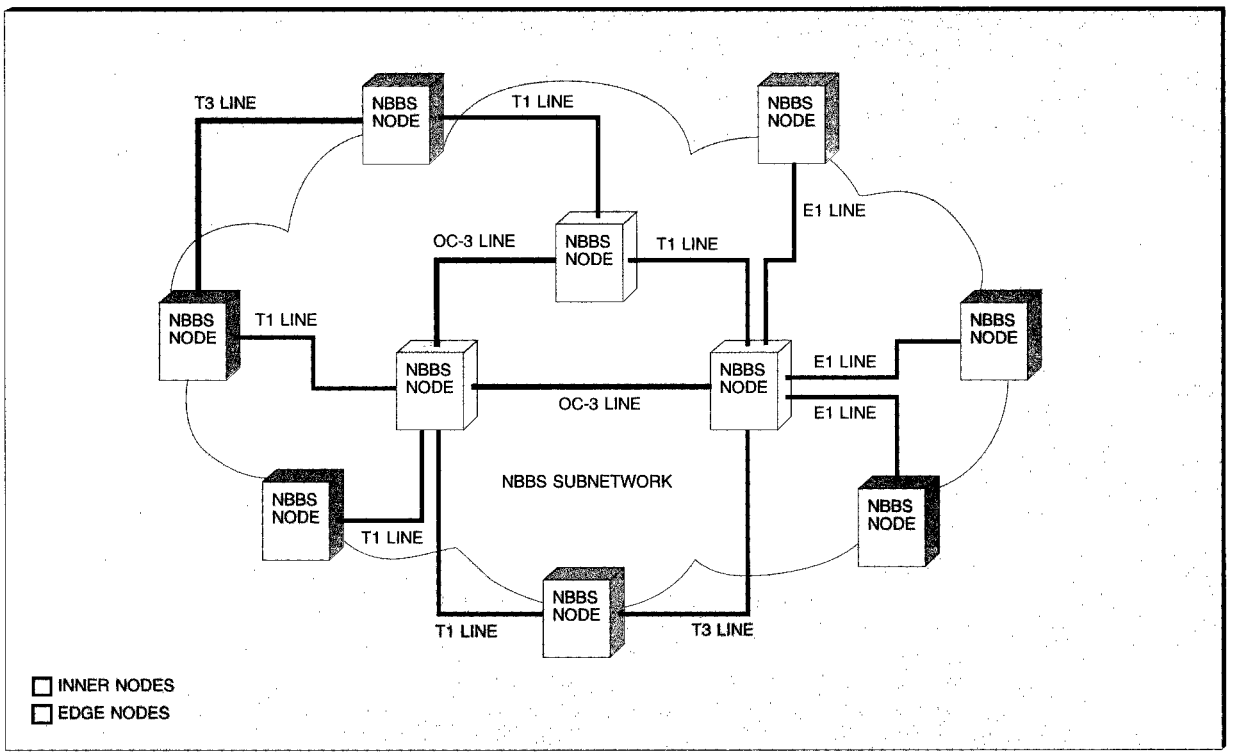
Attachment to NBBS nodes. Figure 1 shows a variety of attachments to NBBS nodes. Since these nodes are organized around a common Networking BroadBand Services architecture, they may be considered a network. But when NBBS nodes are combined with other networking technologies, the NBBS network may be considered a subnetwork.

All attachments to NBBS nodes that do not support NBBS-only protocols can be considered *external*, that is, non-NBBS in protocol. Four attachment scenarios are shown in Figure 1:

- LAN attachment
- T1 network attachment
- Dial-up network attachment
- ATM attachment

This physical communication attachment is independent of the protocol that is used in the traffic arriving at the NBBS node for transport. For example, a T1 network could carry voice, video, or data. T1 is a transmission facility that operates at the digital signal rate of 1.544 megabits per second. If data are used, the protocol might well be frame relay. In the dial-up network, links could support such protocols as X.25, ISDN (integrated services

Figure 2 The NBBS backbone network



digital network), HDLC (high-level data link control), and frame relay.

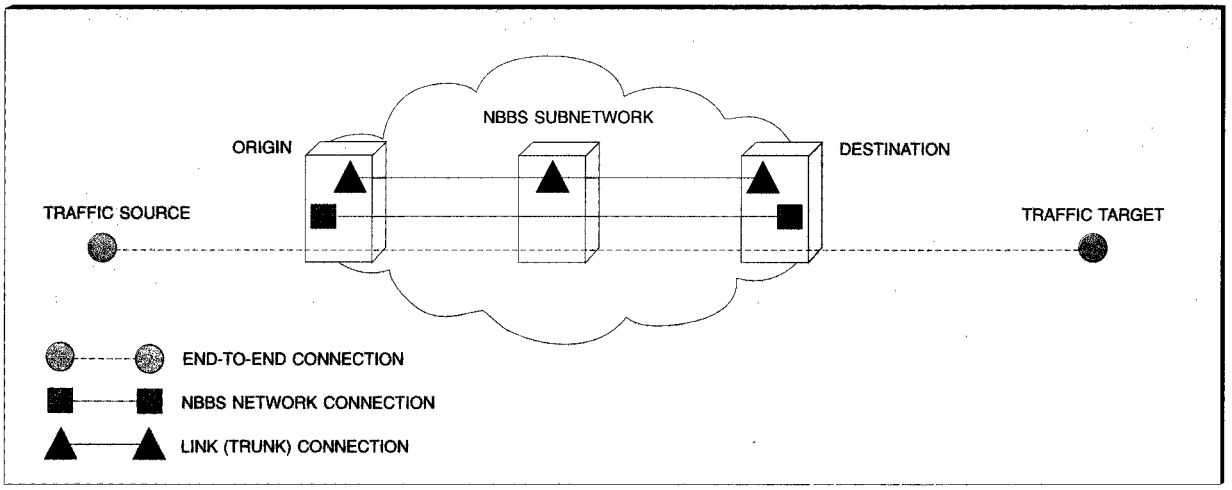
Conceived originally as a transport network for interconnecting homogeneous access users, the NBBS architecture has evolved to support interconnection between those using heterogeneous protocols. An example of such heterogeneous user interconnection across an NBBS network might be between a frame-relay station and an ATM station. Moreover, the NBBS architecture does not preclude the interconnection of low-speed and high-speed access links. For example, several low-speed V.35 links could be connected across the NBBS network to a T1 access link.

Not all the examples above are possible in the first implementation of the NBBS architecture, but the *architecture* itself allows every connection mentioned, provided an access agent is implemented to support a specific protocol combination.

The NBBS transport backbone network. The inner working of the NBBS network relies on a defined architecture for the flows to set up connections and to transport traffic at a given quality of service for a specified bandwidth. In order to meet the high-performance objectives of NBBS transport services, the backbone will be composed typically of high-speed telecommunication lines, for example T1 and T3 lines, or OC-3 to OC-24 lines. T3 is a transmission facility that operates at the digital signal rate of 44.736 megabits per second, and OC-3 and OC-24 are optical transmission facilities that operate at 155.520 megabits per second and 1.24 gigabits per second, respectively. These lines are interconnected in such a manner that they meet the expected traffic loads between geographic areas of the NBBS network.

Figure 2 shows an NBBS backbone network configuration consisting of intermediate (or inner) nodes and nodes at the edge of the NBBS network. The links between nodes represent the transport highway that comprises the WAN backbone. The different speed transmission facilities represent the capability for different routes to accommodate traffic. The links are characterized in terms of traffic

Figure 3 NBBS connection terminology



and queuing metrics in the topology database for the NBBS network. Inner nodes do not have access services components, but from a network management perspective any node may provide NBBS access services as well as transport services. E1 lines in the figure are European Digital Signaling Hierarchy lines at a rate of 2048 Mbps.

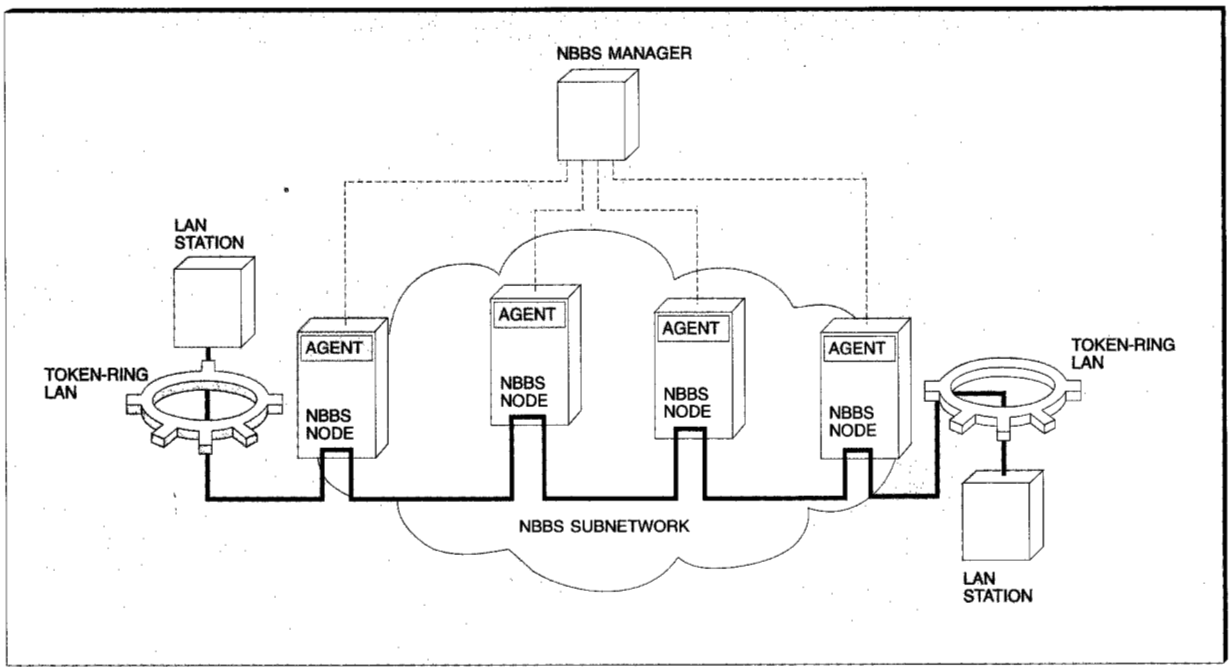
The NBBS network connection model. Because NBBS is defined as a transport network service, particular attention is devoted in NBBS network management to the configuration and selection of resources used for the transport of external traffic. Figure 3 illustrates how traffic from an external source is carried through the NBBS network to an external target. Access to NBBS facilities is provided at an NBBS origin and the exit from the NBBS network is provided at an NBBS destination. A sequence of link connections (trunks) that connect adjacent nodes are the transfer segments that provide the transport service.

The external traffic is carried by network connections from the point of entry or *origin* to the point of exit or *destination* of the NBBS network. The network connections provide paths through the NBBS network at specific quality-of-service levels. The network connections are created by the selection of a series of connected links between NBBS nodes.

The NBBS management communication model. The NBBS model for management follows the manager and agent paradigm, with the NBBS nodes acting as agents and one or more managers responsible for management applications. More than one manager could be used in order to have a backup in case of a node failure, to spread the management load to separate manager applications, or simply to reflect the organization of responsibilities in a network. Figure 4 shows an NBBS subnetwork serving as the transport for two token rings. In this case, the network management agents in the NBBS subnetwork are managed by a single NBBS manager that resides in an external node and accesses the NBBS subnetwork through an NBBS node. Each manager sets up management application associations with the NBBS management agents that it is going to manage.

Several communication models could have been adopted for manager-to-agent message transport. The model chosen in the first implementation of NBBS architecture in the IBM 2220 Nways* BroadBand Network Switch uses an Internet Protocol (IP) communication model. For the most part, this model was chosen because of the support offered by the Netview/AIX* platform and the communication stack it offered. In this IP model, the NBBS manager accesses the NBBS subnetwork by an IP subnetwork through one or more designated NBBS nodes that act as management gateways for management information. Figure 5 illustrates this model.

Figure 4 Manager-agent interaction



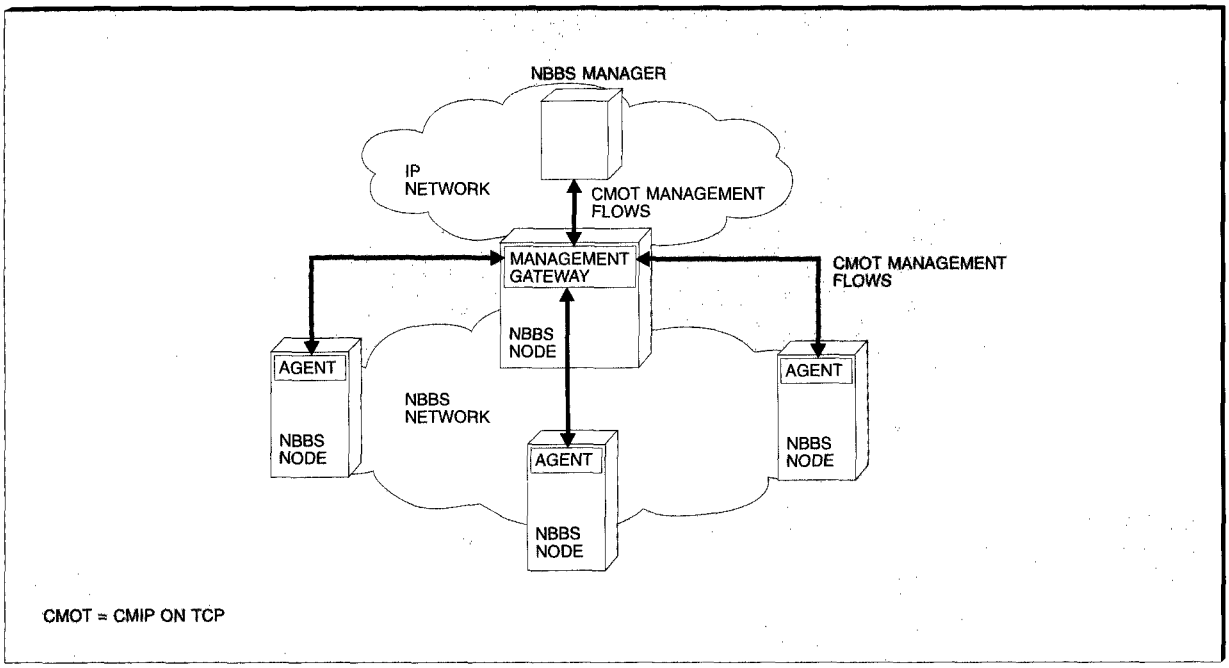
Because NBBS manager-agent interactions are based on CMIP, CMIP management information is carried between the manager and the agent in Transaction Control Protocol/Internet Protocol (TCP/IP) packets. The protocol used is thus called CMIP on TCP, or CMOT. All management-related communication also uses IP addresses for the routing of messages inside the NBBS subnetwork between the management gateway and the management agents, and even inside an NBBS node between the agent and the different components providing management information. Of course, the CMOT traffic is carried over NBBS network connections inside the NBBS subnetwork. The IP address in the IP header for a CMOT message selects the network connection to the destination node or component.

With the announcement of SystemView* for AIX with the TNM/Workbench application, the Nways Switch Manager applications may be placed on a platform that supports additional communications protocols for management communication between the manager and the agent. With this platform, support for the Telecommunications Management Network (TMN) "Q3" interface is possible. Q3 is a standard widely supported by the service provider environment (SPE), that specifies the X.25 network layer and the OSI transport and session layers, for manager-agent communication. Of course both the manager and the agent or a "mediation device" that represents the target agent are required to support the same management communication protocols. The Nways agent can support the Q3 communications protocols because the IBM Portable CMIP Platform*[18] used by the agent to process CMIP messages and interface to management applications is independent of the protocols used for communication.

Benefits of CMIP for NBBS network management

While there can be much debate about the relative merits of CMIP versus SNMP, certain technical features of CMIP were key in selecting CMIP over SNMP, or indeed over any previously defined Systems Network Architecture (SNA) Management Services technology. Foremost among these were the following features offered by CMIP: support for object-oriented principles in MIB development, a global naming convention for access to managed objects, the dynamic creation and deletion of managed ob-

Figure 5 Manager-agent communication using CMOT



jects, an abstract syntax for representing complex structures, support for reporting events in an asynchronous manner with filtering of the notifications at the sender, the ability to extend operational control for MIB enhancements, the ability to perform scoped operations, and a long management message length. The following subsections expand on these features.

Use of object-oriented principles. Managed object modeling in the GDMO approach permits the principles of object-oriented programming to be followed. The principles of inheritance are incorporated into the GDMO specification for managed object classes. Reusability comes into play when the attributes defined in a managed object class are refined into subclasses, with the addition of new attributes unique to the new managed object class. The principle of encapsulation is supported for GDMO. All communication to and from the managed object is controlled by the CMIP methods defined for operations on the managed object class attributes or through actions directed at the managed object class.

As with any management definition, changes in the definition or evolution of a MIB require careful planning. An advantage of CMIP and GDMO is that changes in the agent MIBs do not require a lockstep upgrade of management applications. This is because management applications written for a specific managed object class will also work with a new refined subclass that inherits the properties of the original class for which the application was written; this capability of the refined subclass to be managed as an instance of the original class for which an application was written is called *allomorphism*. As new features are needed and subclasses are refined from the original definitions, coexistence of old and new definitions becomes a reality. Therefore, management applications can treat agents that support different subclasses of the same inherited managed object class the same way, because certain of their components are the same. Moreover, manager applications can develop a routine test by using allomorphism for determining if any agent MIB conforms to the managed object classes understood by its applications. Thus, managers can operate on different MIBs without requiring management application rewrites for new subclasses.

Global naming. With CMIP, manager applications can work directly with the target managed object

of an agent MIB. This is due to the way in which managed object classes are named and how the names are combined in a containment tree for a particular MIB. One attribute of each managed object class is selected as the naming attribute to be used in name binding. Name bindings define the relationship between the managed object classes when managed object classes are combined together into a MIB. These name bindings are formal rules that permit the construction of unique identifiers for all managed objects within an agent MIB by the concatenation of naming attribute values.[19] This emphasis on naming results in three benefits. First, a manager does not need to have a predefined list of names, but can learn the naming convention by a query to the MIB. Second, within a MIB, managed objects may be addressed directly by CMIP for management activity. Third, the managed object class may be reused in a subclass or in another MIB without the need to redefine the naming component, because the name binding can be reused for subclasses.

The collection of managed objects forming the NBBS MIB is replicated in every NBBS node.

Dynamic create and delete. CMIP provides the ability to actively manipulate the agent MIB in a standardized manner. CMIP has defined create and delete operations that permit managed objects to be added or removed from an agent by a manager. The creation and deletion of managed objects allows dynamic representation of a network environment by adding or removing instances of classes defined for the MIB as the operational needs of the network require it. For example, the addition of a new telecommunications adapter to a node configuration can easily be accommodated by creating a new instance of the adapter class to represent the resource.

Abstract syntax. Abstract syntax notation 1 (ASN.1)[20] is supported by GDMO and permits a general definition of management structures. ASN.1 allows the definitions for the managed object classes to closely parallel the constructs found in many programming languages. ASN.1 supports simple data types, such as integer, Boolean, and octet string. It also supports complex constructor types, such as sets and sequences and their combination. Virtually anything can be represented by this syntax.

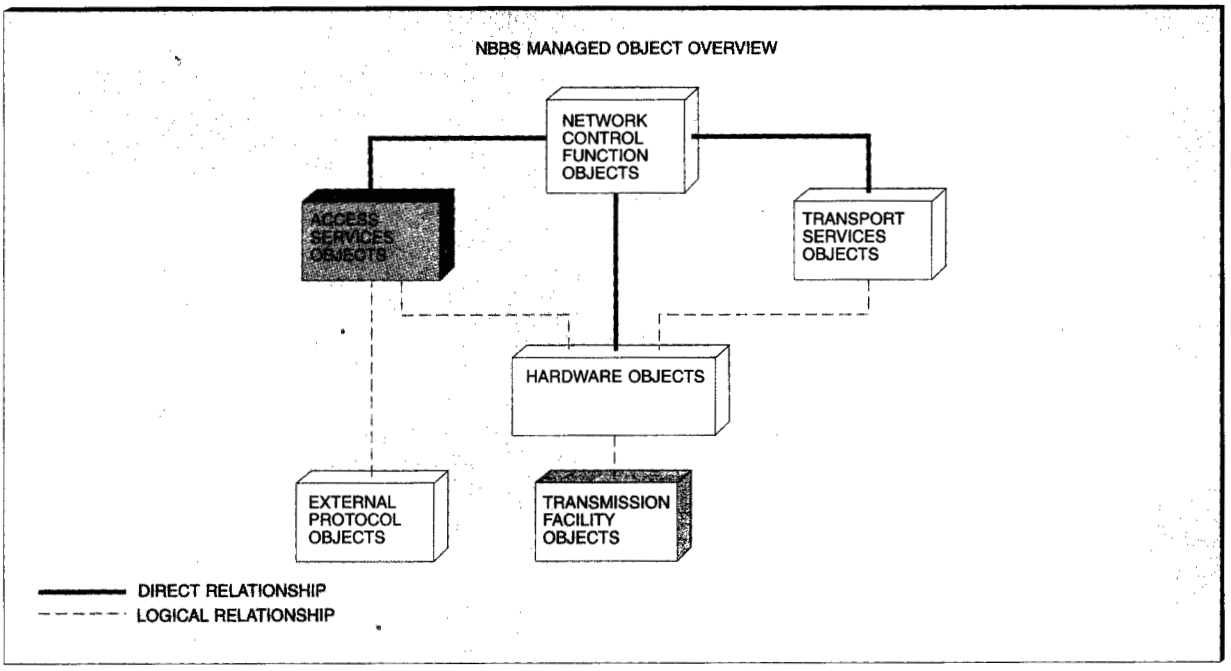
Asynchronous communication. Another strong point for CMIP is the extensive standardized definition for notifications. The structure and definition of asynchronous notifications, such as attributeValueChange notification, stateChange notification, and equipment, environmental, quality of service, and communication alarms,[12] are well defined and rich in scope.[21] Furthermore, the CMIP model permits the manager to create agent structures called event forwarding discriminators (EFDs), which designate the network manager interested in a given notification issued by an agent. This facility provides a form of source filtering of notifications, where the agent determines after the creation of a notification if it is to be logged and sent to a manager, or just logged.

CMIP provides two methods for operation control that were considered distinct technology advantages: the action operation and scoped request for operations.

Flexible operations control. The action operation permits the manager to send a special type of CMIP message, an *ACTION*, to a managed object. ACTIONs may be developed to perform a class-specified operation not covered by standard Get and Set operations.[22] In addition, within the ACTION syntax, special parameters may be added to ACTIONs that carry application-specific information.

The scoping of requests for operations. CMIP permits a manager to issue complex queries to an agent that require processing of agent MIB data. While a straightforward manager-issued Get function targeted to a specific attribute is supported, a scoped request for information may also be issued to an agent. In this case, the manager does not precisely specify a target managed object. Instead, a base managed object is given for the request and specified subordinate instances contained under the base object are considered as candidates for the request.

Figure 6 Managed object model categories



CMIP provides the scoped request on any CMIP retrieval operation the ability to apply tests, called *filters*, to the target MIB candidate responses. In addition, CMIP permits the use of access control to allow an agent to certify that the requester of an operation is authorized for that operation.

The management message length. CMIP conformance[23] limits the maximum CMIP message length to a maximum protocol data unit (PDU) size of 10K octets. While this is sufficient for most network management messages, there are cases where the MIB values will exceed this message limit—for example, in the case of attributes having complex syntax consisting of sets of items. In such cases, the number of items in the set may become very large and even exceed a single message PDU. For the NBBS MIB, the potential for these large-message cases was recognized and special CMIP actions with linked replies were defined to handle the large PDU. The link reply capability used in this way allows potentially very large messages to be sent to the manager as a series of smaller PDUs, thereby ensuring no loss of MIB information because of message truncation.

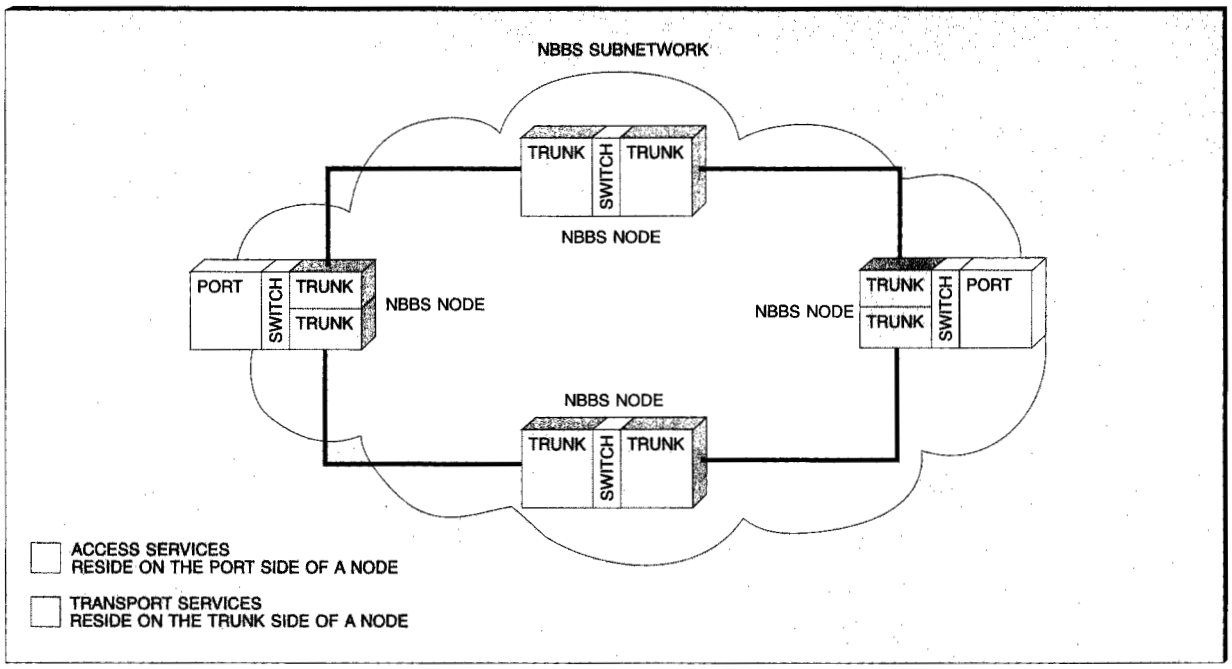
NBBS managed objects

The NBBS model for management relies upon the SystemView Managed Resource Model[24] for the definition of abstract superclasses for fundamental object characteristics. To reflect the specifics of the NBBS implementation, attributes had to be added to the basic SystemView model. The managed objects are grouped into six categories:

- Network control function objects
- Access services objects
- Transport services objects
- Transmission facility objects
- External protocol objects
- Hardware objects

Figure 6 illustrates the linkage between the object categories found in agents used to manage NBBS nodes. This collection of managed objects forming the NBBS MIB is replicated in every NBBS node that provides services to attached non-NBBS networks (including directly attached, single non-NBBS nodes). However, NBBS nodes inside the NBBS network that do not provide access services

Figure 7 NBBS function placement model



to external networks or nodes will not maintain access services or foreign protocol objects.

Figure 7 illustrates in a network context the relationship between managed object groups for access services, which are represented as a port, and the transport services, which are represented as a trunk, in NBBS nodes.

Network control objects. Network control objects are managed objects needed to manage the specific protocols and structures of the network control services. These objects represent the nodes and their control points and the way network control services use directories and exchange, process, and maintain network topology information in the NBBS network. The network control objects define common characteristics across all NBBS nodes and allow for management extensions as new NBBS features require management.

Currently, two network control managed objects are defined:

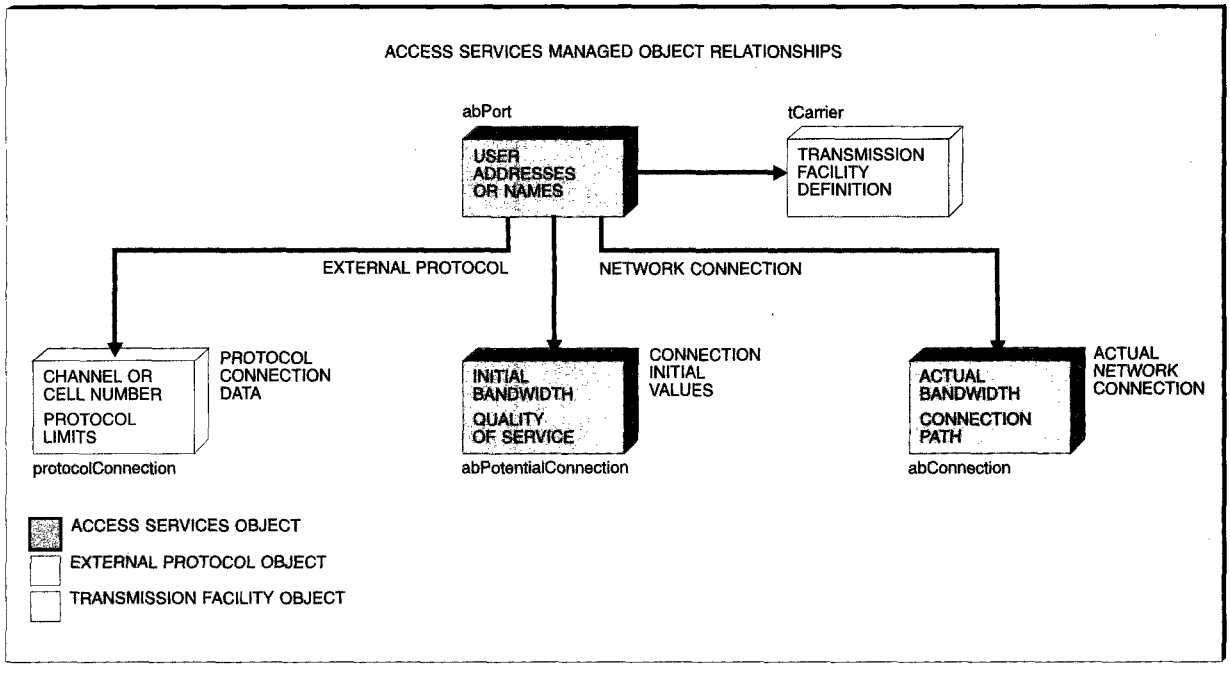
- The abNode[25] represents the box realization of an NBBS node. It is the highest naming level for a node, which means all other managed object classes are contained beneath the abNode object class.
- The abCP represents the control point as the summary of all network control services in a node.

Access services objects. Access services objects are needed to define the logical relationship between the external traffic requests made by users of the NBBS network and the NBBS method of providing the traffic transport service. These objects relate the interfaces provided by non-NBBS protocols to services provided by NBBS networks. The functions provided by access services are target address resolution, path selection and maintenance, and access protocol control.

The access services managed objects include, but are not restricted to, the following:

- The abPort managed object represents a link (port) to an adjacent non-NBBS node that is served by an access agent.
- The abPotentialConnection managed object represents the initial values for network connection that may be activated through time-of-day trig-

Figure 8 Relating external traffic to network connection definitions



gers or operator actions for permanent virtual circuit type connections.

- The abQOS managed object represents a set of quality-of-service parameters.
- The abConnection managed object represents the network connection bandwidth and path used to carry user traffic through the NBBS network.
- The abConnectionScheduler managed object permits automated coordination of connection activation and termination.
- The abConnectionCounters managed object contains the counters that allow performance measurement and accounting for traffic flow.

Transport services objects. The transport services objects are used to define the logical relationship between adjacent NBBS-node link partners. The NBBS links represent the logical view of the NBBS backbone network that carries all user and network control traffic. The transport services objects are dependent on the actual physical backbone that is represented by objects that monitor the physical facilities (such as T1 or T3 links).

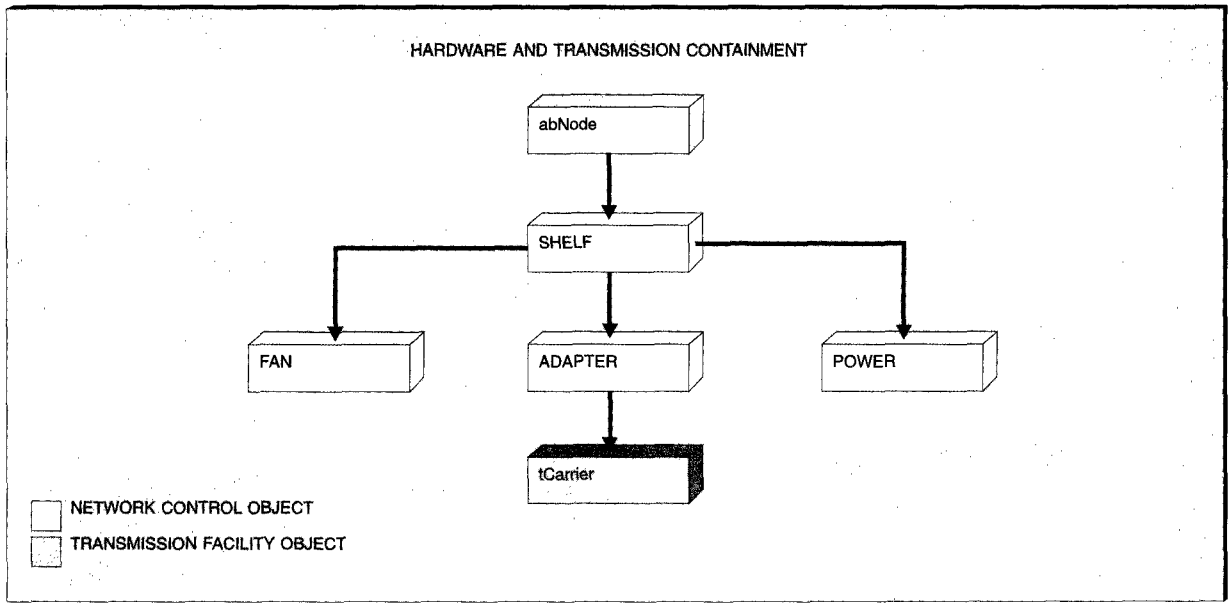
Objects in this class include, but are not restricted to, the following:

- The abTrunkConnection managed object represents a (unidirectional) link to an adjacent NBBS node. It contains the view of this link as seen by the node maintaining this object. A complete view of the status of the link is possible only when combining information from the two objects representing the link in the nodes connected by this link.
- The abTrunkCircuit provides a view and control of the state of the link defined by the interaction of the abTrunkConnection objects at each end of the link.
- The abTrunkConnectionCounters object contains counters that allow the measurement of traffic flows and total link performance.

External protocol objects. External protocol objects manage specific protocols used to attach to the NBBS network. Examples of these protocols are ATM and frame relay. The relationship between the incoming and outgoing protocols and the NBBS network connection transporting them is key to providing a seamless management picture for customers.

Figure 8 illustrates the relationship between the NBBS access services managed objects of the

Figure 9 Typical hardware and transmission relationship in an NBBS node



abPort and the external protocol managed objects and the transmission facility managed objects. The abPort acts as a container object for the many initial-value descriptions for the permanent virtual circuits defined for network connections and their associated external protocol managed objects. Each of these network connections originates on an access link defined by the transmission facility, tCarrier.

Transmission facility objects. Transmission facility objects are defined to manage specific physical-layer protocols that attach to or are used in the backbone of the NBBS subnetwork. For example, T1 or T3 transmission facilities are monitored by managed objects that describe the configuration of the physical layer and report state and error conditions. The access services and transport services objects are linked to the transmission facility objects.

Hardware objects. Hardware managed objects are needed to manage the specific implementation of an NBBS node. The hardware objects provide a logical view of the hardware organization and the hardware features that may be managed. The hardware objects include the physical transmission protocol components used for both access services and topology services.

The networking approach of NBBS relies on physical components to provide an efficient platform for network control flows. The integration of hardware object definitions into the management architecture of access and network control services is thus critical to successful NBBS network management. For example, while the operation and status of a cooling fan or of an internal bus may not be important to NBBS protocols, the failure of such a hardware component could drastically affect the ability of a node to process traffic. The ability to relate a failed hardware component, such as an adapter, to the traffic being carried is critical to the rapid isolation of problems and possible corrective reconfiguration of the hardware to support the traffic load of the failed component.

Hardware managed object class definition and integration of the hardware status into the NBBS network topology permits the manager to learn quickly about network problems.

Figure 9 illustrates the relationship between the NBBS node and the hardware and transmission facilities being used by a node. This relationship is key to the way in which the condition of a node is represented in the NBBS manager topology. Because of the hierarchical relationship, a dependency structure between the managed objects and

their resources can be established. Changes in state of any subordinate managed object, for example a tCarrier outage, can be represented and the effects on the superior managed objects, for example a logical trunk and the node, can be propagated up the hierarchy to a visual display in a topology map which will indicate the loss of connectivity between two NBBS nodes.

NBBS management applications

NBBS management covers the six network management categories required for the management of any network:

- Topology management
- Accounting management
- Performance management
- Problem or fault management
- Configuration management
- Hardware management

The NBBS architectural objective for network management was to provide a small set of powerful managed objects to enable the network management applications listed above. The Nways Switch Manager network application[26] objective was to provide a graphical user interface (GUI) that permits consistency of presentation from one management application to another.

Network management models form an "ensemble" to provide a foundation for the information flow and the management activity needed to accomplish a management application objective. Therefore, the network management model abstracts what the network management application provides. The model deals with what management information or capability the agent can make available to the manager. The application deals with the manipulation of management information for a specific objective, that is, whether creating, deleting, retrieving, setting, displaying, or processing the information is required.

Currently, no network-wide management activities are defined. All management functions are focused on the NBBS node and its components. The management applications that use the GUI are all based on the NBBS network topology. Using the topology, NBBS nodes may be selected and managed according to management activity menu selection.

Managed object classes are not specific to any of the six management categories, but comprise attributes (which may be shared between categories) that are generally defined. Each management category uses a model that defines how managed object classes and their attributes are related and how the management activity is achieved.

Because of the significance of topology and the emphasis on manipulation of hardware components by the management applications, the topology and hardware areas, which normally fall under the rubric of configuration management, are treated separately in this paper.

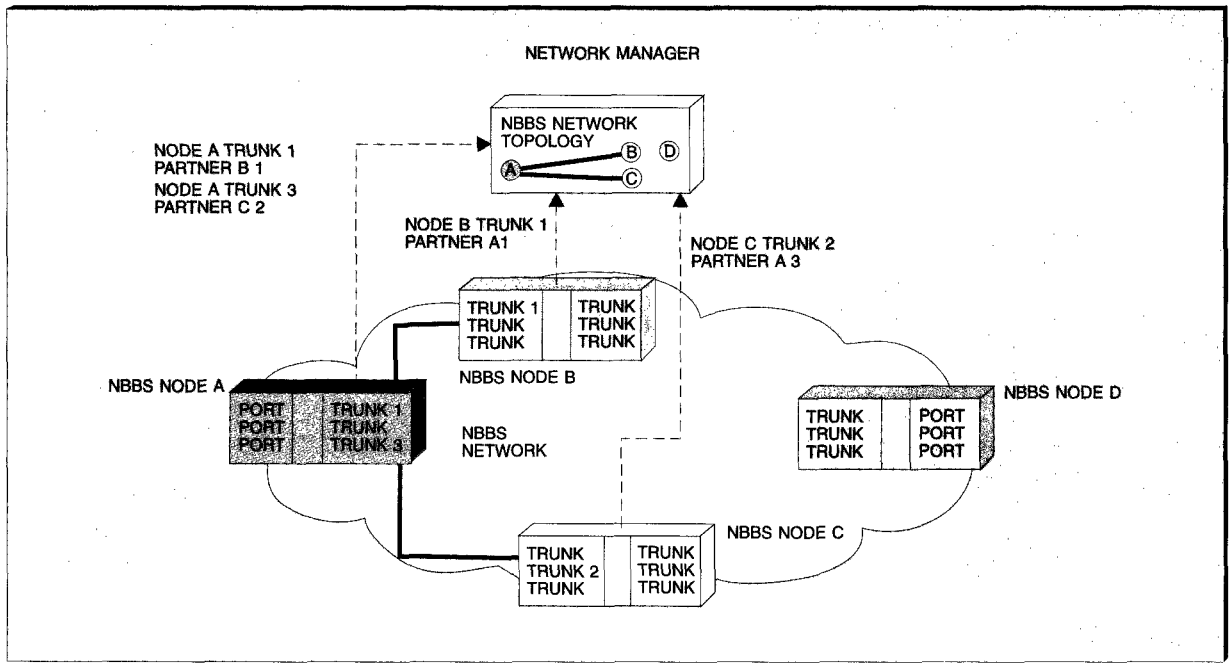
The topology model. The goal of the topology model is to permit the network management station to present a graphical view of all nodes in an NBBS network and how these nodes are interconnected. In a displayed view, the actual status of nodes and links is shown based on notifications sent by the management agents when a change occurs in the status of a node or link.

Of particular importance to the network management operation of NBBS is the ability to accurately show the relationship among nodes of the network. For a given NBBS network, the Nways Switch Manager knows what nodes comprise the network prior to the activation of any of the NBBS nodes. However, the topology application in the manager has no way of knowing how these nodes are connected until node activation has completed and the nodes have been linked.

After a node has successfully been started and initialized, NBBS-defined message flows between partner trunk endpoints permit the exchange and negotiation of link data. Examples of the information exchanged in these flows are the bandwidth allotted to a particular traffic category, for example nonreal-time or packet traffic; the delay characteristics of the link, such as propagation delay; and loss characteristics, measured as a function of the trunk buffer size.[15]

Once successful link initialization has occurred, each abTrunkConnection involved in the link setup prepares an unsolicited notification called a CMIP stateChange notification, which is sent to the manager. This notification contains the current state of the link and the trunk partner name.[27] As part of the CMIP convention, the NBBS node identifier

Figure 10 The NBBS node topology model



of the sending trunk is always included in the management naming hierarchy.

The stateChange notification reaches the topology application in the manager with the sender's node name and trunk name, its current trunk state, and the trunk partner's node name and trunk name in the message. Therefore, the topology application can begin to associate a node and trunk with another node. Confirmation of this association occurs once the trunk partner's state change notification has been received at the topology application. With both parts of the link identifying the partner, the topology application can be sure of the relationship between the nodes.

Figure 10 shows the network manager using notifications from the abNode and abTrunkConnection to construct a topology view that includes the states of the endpoints and the partner names. In Figure 10 the solid lines indicate the actual NBBS links connecting two NBBS nodes. Notice that not the whole network topology is connected. The dashed lines indicate the network management messages being sent to the manager from the abTrunkConnection managed object instances at each NBBS node giving topology information about neighbor node and trunk partner names.

The topology model is also used to display how connection traffic is transferred from node to node through the network. This display normally will indicate two different physical paths, one for each direction of transmission. The abPort managed object contains a list of all abConnection managed objects representing network connections that have been created to transport user traffic from an origin port to a destination port. The particular path that a connection uses as it traverses the NBBS network can then be determined by accessing the associated abConnection instance of the port containing the list of abTrunkConnection names that comprise the path in the direction of transmission from the port to the destination.

The accounting model. The accounting model permits the NBBS service provider to show how much of the network service a particular connection used. The entry and exit from the NBBS network is defined in terms of access to specific ports to which the NBBS user attaches. Network connections can be established dynamically by an access

agent on request of the served user if the external protocol supports signaling of connection requests. If the external protocol does not support this, connections have to be predefined; this is done by defining specific connection request profiles, called *potential connections*. By requesting specific abPotentialConnection instances to be activated through time-of-day triggers or operator action, NBBS ports are then connected (as in the dynamic case) at selected quality-of-service and bandwidth levels. The requested quality of service does not change during the connection, but the bandwidth requested may be adjusted, if this option is chosen, to reflect the actual traffic usage.

The use of NBBS network services by the user is accounted for by the specification of an accounting set composed of:

- The quality of service of the connection
- The bandwidth parameters
- A meter consisting of a set of traffic counters

Periodic reports are issued by the abConnection instances to account for the changes in traffic use or network activity, such as rerouting of the connection.

For the benefit of the NBBS network provider, usage counts of internode links are kept with each abTrunkConnection instance. These usage counts are not reported by the accounting application for network connections; however, these counters make it possible to assess how much each link has contributed to total network traffic.

The architectural model used for accounting follows the definitions of the accounting model for APPN and subarea management.[28] In the NBBS adaptation of this model, the agent system collects accounting event information as it is issued from the abConnection instances and keeps it until the manager application requests the information.

The performance model. The NBBS performance model permits an estimate to be made of the activity level of the NBBS network. Since the NBBS architecture defines a self-regulating network process, little outside intervention by operator control is needed in tuning the NBBS network. However, the monitoring of network facilities is important and can be used to indicate to the operator that intervention may be required in the control of connection and port activity.

The abPort instances keep counters of the number of successful and blocked or failed connection setup requests, thereby giving a measure of the ability of users to access NBBS services.

Once a user has been awarded a connection, the measures of bandwidth used, path selected (number of hops), setup time to create the path, and end-to-end delay are gathered in the abConnection instances. Counts of traffic offered and traffic passed are also kept according to the priority level for the connection. It is possible to determine at any time during the life of a connection how much of the traffic offered to the NBBS network for transport has exceeded requested bandwidth levels, how much has been passed, and how much has been discarded.

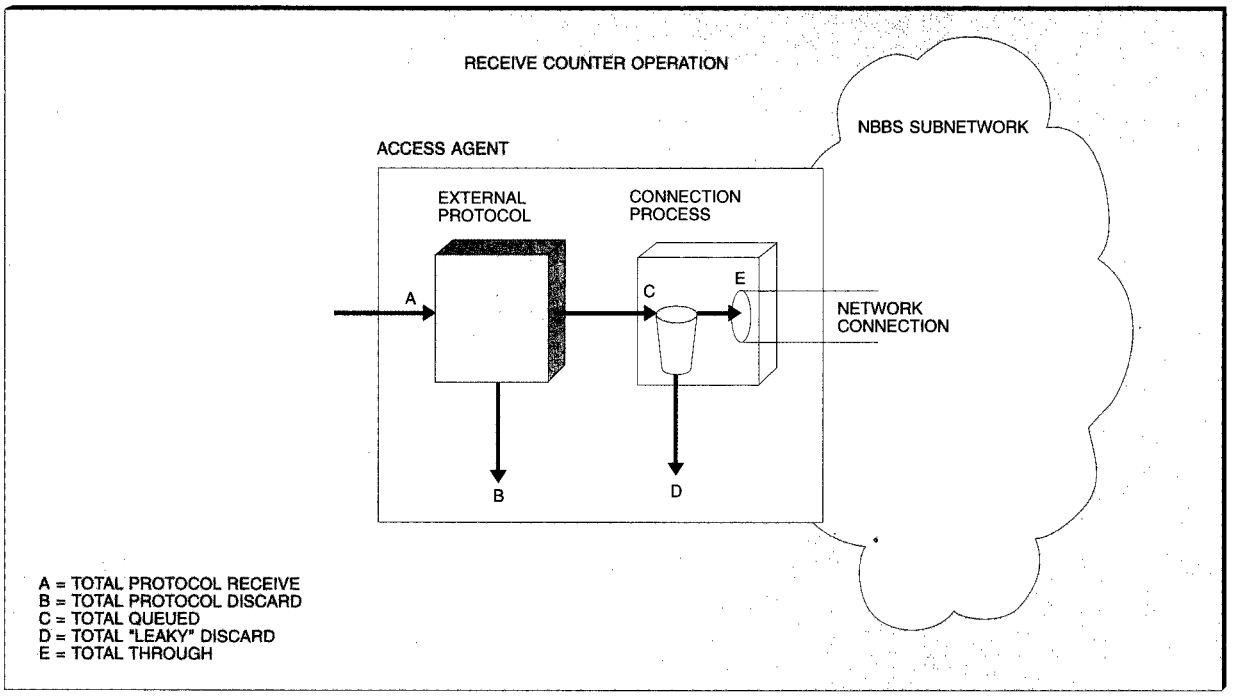
The trunk traffic counters for the different delay priorities maintain statistics of total traffic processed, good and bad, as it arrives and exits at the link endpoints. This gives a detailed measure of the traffic processed by a particular link at a node. In addition, the abTrunkConnection instance keeps track of all the bandwidth reservation requests for network connections using the link. For example, a manager performance application can access managed objects for performance information related to the network connection at the NBBS link by accessing each abTrunkConnection, at the network connection level by accessing the abConnection, and at the external protocol sources by accessing the protocol connection endpoint.

This ability to derive a performance profile for a connection, a port, or a link is provided by the performance management application, which relies on the IBM SystemView for AIX performance platform for basic function. The platform permits the definition of counters to be related through mathematical expressions and the results graphed via the GUI. The NBBS performance application has added a predefined set of counter relationships that graph the performance of NBBS links. As part of the application, the raw counter data are retrieved on a periodic basis from the target abTrunkConnection instance and summarized graphically.

This same application technique may be applied to external traffic measured as it relates to network connection traffic.

Figure 11 illustrates how the receive operation at an NBBS access agent captures counter informa-

Figure 11 Generic receive counting operation for a network connection



tion related to the network connection and external traffic source. Counter information for access services is kept in two managed objects: one specific to the counters for the external protocol, and one containing counters for the network connection. Here the amount of received traffic can be compared to the amount of traffic that was actually queued for network connection transmission according to the policing[29] criterion for the network connection. Ratios of total traffic to excess or marked discard-eligible traffic can be derived to monitor the behavior of network connections.

Use of details of the parts to characterize the whole is also true at the network level. There is no single network metric for utilization, just as there is none for each node. It is possible, however, to characterize the utilization of each link connection between two nodes and then to develop an overall path utilization summary measure for the connections to a specific node. Repeating this process for every node creates a network view of utilizations.

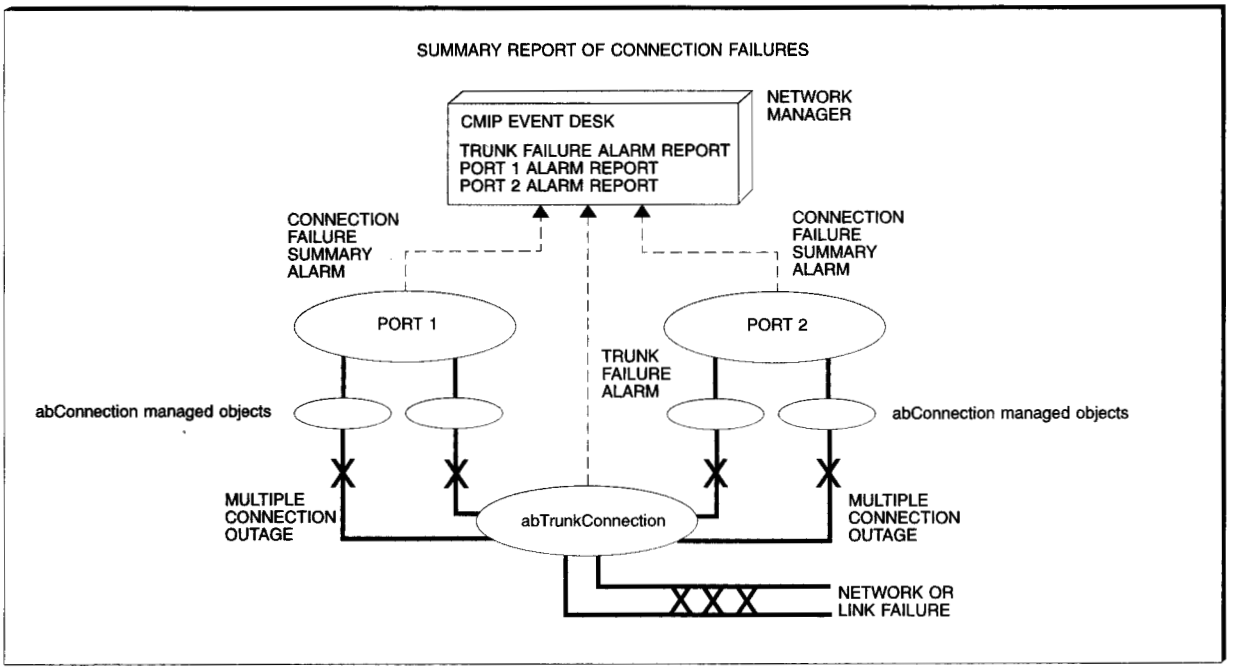
The fault model. The fault model for NBBS management consists of reporting failures or abnormal operational events in such a way as to isolate the problem component and to direct corrective actions. State change reports and alarms are used as the two forms of notification for fault reporting.

The agent routes the notification information to an Event Desk application, which logs the event and converts the notification information from a standardized encoded message format into human-readable fault management activity descriptions for display.

Notifications may be selectively filtered by the agent. In what is known as *source filtering*, one or more managers set "filters" in the agent by selecting which notifications they are interested in receiving. These filters may be dynamically altered during the operation of a node, thereby permitting flexibility in the type of fault-reporting message and the managers receiving it.

NBBS logical components, such as instances of abPort, abConnection, and abTrunkConnection, report communication failure events; these events can be, for example, failure to establish a network connection, connection failure, and loss of connectivity. The abCP and abNode instances report processing

Figure 12 A summary report for multiple connection failures



failures. The instances of hardware-managed object classes report equipment failure events in logical or system-wide functions.

In addition to these notifications to report specific failures or degradation in performance and availability, status change notifications are sent by instances of the abCP, abNode, abPort, abTrunkConnection, and hardware objects to indicate a change in the operational and availability status of a component.

At the hardware level, when the failure of a low-level component is reported, the hierarchy of state information permits detecting the effect of the failure on related or logically dependent components. Relating problems from a base component to a higher-level component makes failures and their impacts on a node's system structure visible in the management of the hardware.

Figure 12 illustrates how, when each port in a node, upon detecting multiple connection failures (for example as a result of a trunk failure), sends a single alarm notification to the manager as a summary of failed connections, instead of sending separate alarm reports for each failed connection, thereby optimizing the notification traffic. In addition, a single problem list permits a manager application to use the list of failed connection names to check their respective initial value managed object for the "permanent" value in the connectionStartupMode attribute and issue a command to the port to restart the connections.

The configuration model. The configuration model is the most significant in terms of proactive operator intervention within the NBBS network. Configuration activities for NBBS can be either static or dynamic.

Static activities establish network characteristics in preparation for network activities. The creation of new objects to manage the addition of hardware, ports, trunks, or new nodes to the network are such examples.

For network connection configuration, the operator creates new abPotentialConnection instances in response to changes in user requests for new network connections. Typically associated with this task is the selection of an external protocol source, the specification of bandwidth and quality-of-ser-

vice information for the network connection and any value-added features for the network connection, such as nondisruptive path switch or automatic bandwidth adjustment.

Once established, the abPotentialConnection may be modified to reflect changing network conditions. For example, if upgrades or changes to the quality of service (QOS) required for a connection are needed, the abPotentialConnection instance can be modified to refer to a different abQOS instance.

A human or programmed operator initiates dynamic activities to regulate the NBBS networking processes. Examples of dynamic configuration activities are:

- An operator may change the configuration parameters of a port or trunk through CMIP SET and ACTION commands.
- For the access services objects, an operator may configure an abPort to start or stop initiating or completing network connections. This changes the way a port processes connection requests. By selecting which role to use, the port will either only initiate connections, only complete connections, or permit either initiation or completion of connections.
- An operator may start, shut down, or stop immediately the operation of a port or a trunk through CMIP SET commands directed at the administrativeState attribute.
- An operator may start a particular connection by issuing a start connection command against the port containing the abPotentialConnection instance that has the connection characteristics desired for the connection.
- An operator may stop a particular connection by issuing a stop connection command directly to either the initiating or completing abConnection instance representing the connection.
- An operator may change, create, or delete a schedule for automatic network connection establishment by accessing the abConnectionScheduler instance for a particular port as shown in Figure 13. Here the updated time-of-day trigger for the network connection from Atlanta to Chicago is modified. At the appropriate time (17:30 in Figure 13), the abConnectionScheduler issues the start connection command to the abPort to select the abPotentialConnection named in the schedule entry to start a network connection.
- For trunk objects, the operator may remove or add links to and from service by issuing CMIP SET commands against the abTrunkConnection instance. This will then also cause their state in the NBBS topology database to be changed. Figure 14 shows that a manager can cause a change in the network topology by issuing a management state change through the CMIP SET command locking the administrativeState of a trunk endpoint. The trunk endpoint acknowledges the command and after the state change activity has been completed reports the new trunk status to the manager with a stateChange notification indicating the new state of the resource is *locked*. As a result of the lock management request, the NBBS trunk connection manager directs the trunk to issue an NBBS trunk state change on the link to the partner trunk endpoint. This is done by converting the network management state *lock* to the NBBS trunk state *disable* and sending an NBBS trunk update message to the partner. The partner trunk connection endpoint in turn as a result of the NBBS link state change also issues a stateChange notification to the manager indicating a locked state. Therefore, at this time both endpoints have reported a locked state and the manager topology application changes the connection icon for the link connecting the two nodes indicating the out-of-service condition. Parallel NBBS control activities not shown in Figure 14 are the NBBS topology update flows that are issued by each node as a result of changes in the NBBS link state from enabled to disabled.
- The most significant configuration action an operator can take is to request a restart of the CMIP ACTION directed at an abNode. This action has the effect of causing a node initial program load, which has the side effect of marking it unreachable in the topology database and control point (CP) spanning tree. All previously created managed object instances associated with that node are deleted and new instances are created as the node is initialized. Once the node is operational, it will rejoin the NBBS network and participate in its control processes.

The hardware model. Closely related to the NBBS configuration model for access services and transport services is the hardware configuration model. The hardware configuration model permits the manager application to examine the exact physical makeup of the NBBS node. Information such as the presence or absence of adapters in the node, the kind of function—port, trunk, or switch—the adapter is being used for, and the kind of protocol used in the transmission facility are available to

Figure 13 Updating an access agent time-of-day connection

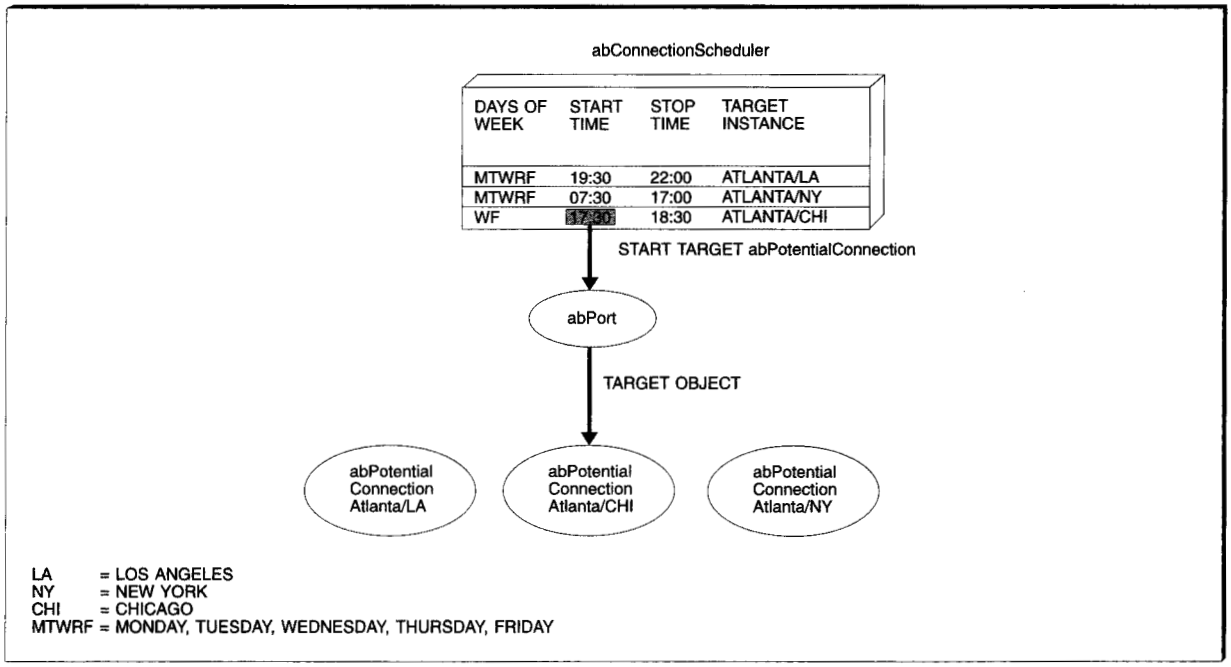
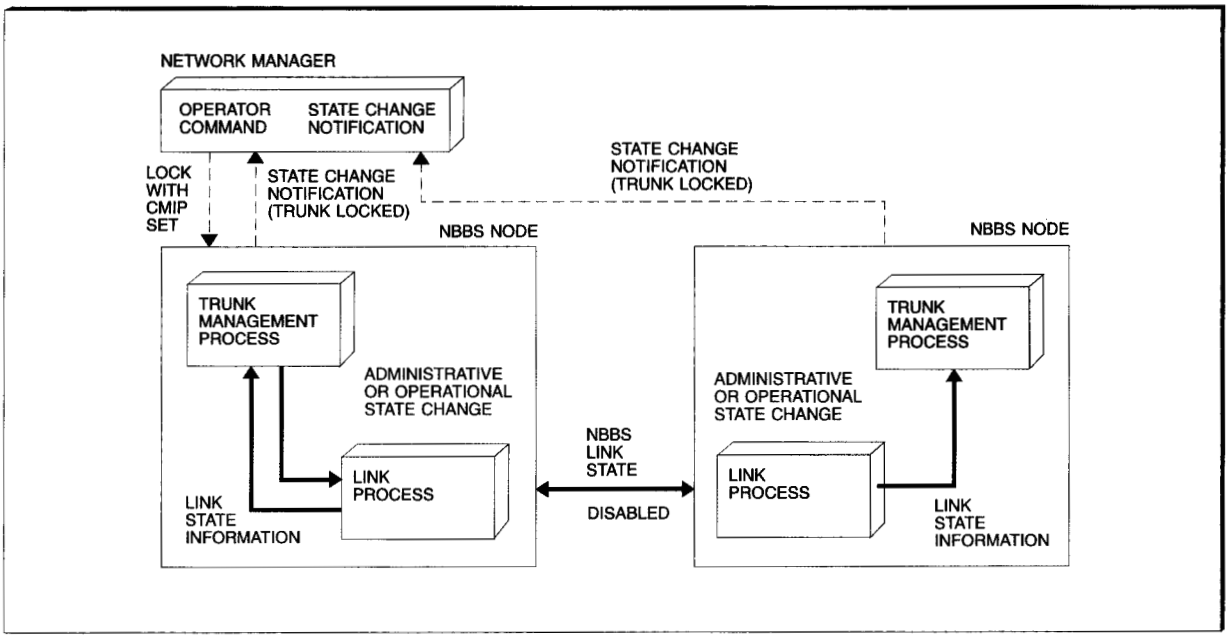


Figure 14 Managing the NBBS link states



the hardware management application. The manager displays visual clues about the operation of the node from a hardware point of view by associating colors with the reported states of the managed objects that represent the hardware and transmission resources of the node.

Future enhancements and directions

The Networking BroadBand Services management solution is planned to grow in two ways: by offering new application interfaces at the manager and by offering new agent MIB support.

The extension of the manager applications "outward" will permit greater reach of control and service of NBBS networks to meet two important requirements. NBBS will be able to be managed as a component subnetwork in a much larger network, such as a global or regional network comprised of many other subnetworks, as in a service provider environment (SPE). It will also permit support of network management services from a customer network management center having logical control of the NBBS resources.[30]

These requirements can be accomplished by offering new management communication interfaces at the Nways Switch Manager.

Manager extension. In the multivendor environment, the network management solution offered by NBBS must be able to integrate with other managers in different ways. First, the Nways Switch Manager must interact as a peer manager with other managers. As shown in Figure 15, peer managers in both the customer premise environment (CPE) and the SPE environments may interact with the Nways Switch Manager; however, the protocols used for manager interaction may be different. In SPE networks using the TMN model,[8] the interface for peer manager communications is called the "X" interface. While an "X" interface using CMIP could also be used for communication between a CPE manager and the Nways Switch Manager, the IP interface preferred by many SPEs and customers is SNMP.

Second, as also shown in Figure 15, the Nways Switch Manager must interact as a submanager for a manager of managers. In this case, the TMN model specifies CMIP with the "Q3" interface[8,31] for communication between the manager of managers and the submanager, or "mediation device."

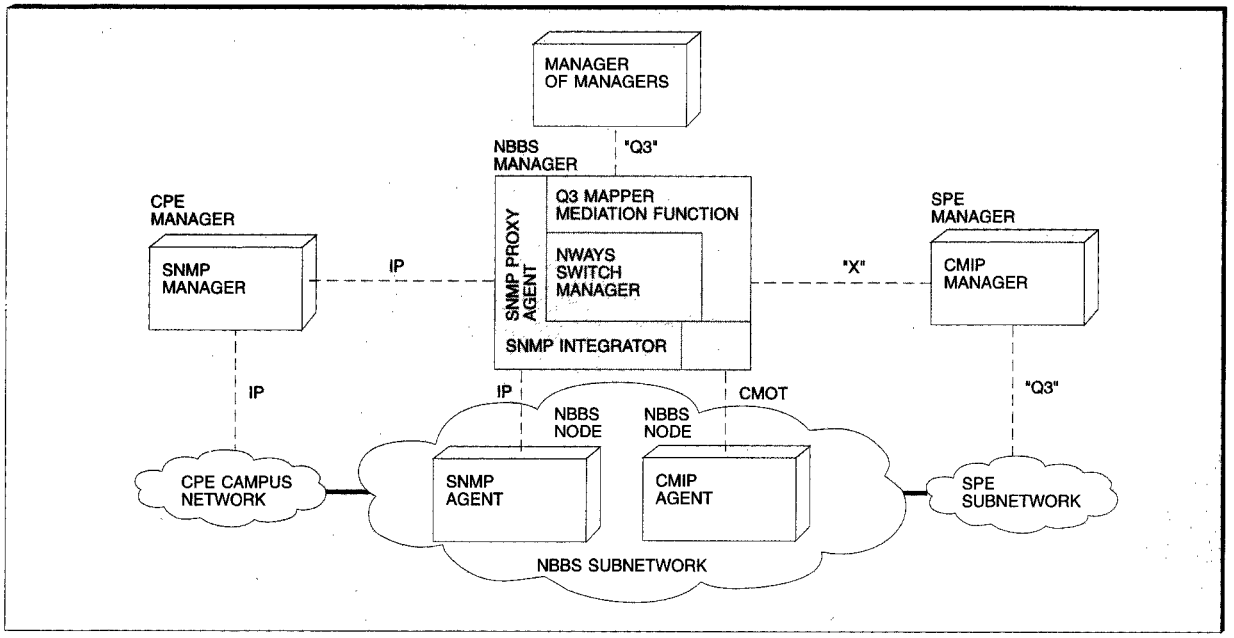
The ability to support network management service interfaces requires the Nways Switch Manager to accommodate new roles as it changes from a manager to a proxy agent in support of these interfaces. The proxy agent acts as if it is the management agent for a resource. For interactions with the customer management center, a proxy agent presents an agent interface to the customer management center, while actually executing NBBS manager applications. As a proxy agent, the Nways Switch Manager accepts commands from the customer manager and translates them to the appropriate application request targeted for the real NBBS agents in the Nways network. Although the protocol stack may be different, the same proxy agent activity occurs in the case of the "Q3" interface, but in this case the activity of the Nways Switch Manager is referred to as a "mediation" function.

This new translation and dispatching role of the Nways Switch Manager as a proxy agent, or mediation function, is made possible by the development of two mirror functions. For an SNMP agent appearance, the "integrator" function[32] permits the translation from SNMP MIB items to NBBS MIB items. For a CMIP agent appearance, the "Q3 mapper" function[33] permits the translation from non-NBBS MIB items to NBBS MIB items. Thus both the proxy agent and the mediation function requirements share the common objectives of being able to map the NBBS MIB to other MIB formats in order to interoperate with other managers.

Agent extension. In order to offer an NBBS node with integrated architecture that is less costly, for both the CPE and the SPE environments, NBBS agent changes are necessary. To accomplish the network management portion of this objective, an SNMP agent definition for the NBBS MIB that is equivalent to the CMIP NBBS MIB has been developed. The SNMP MIB will mirror the GDMO MIB. The Nways Switch Manager applications will continue to operate as if they are targeting a CMIP MIB, but a new network management component, the "integrator" function, will provide a technology conversion between the CMIP operations and the SNMP operations. The IP connection between the NBBS node and the NBBS manager in Figure 15 illustrates the network scenario of this model.

The ability to manage SNMP agents in the Nways Switch Manager means that a manager application—for example, a network connection configuration setup—can begin to have network management

Figure 15 Expanding the NBBS manager role



protocol independence. Complete independence from technology requires the support of a new technology to permit this form of application sharing. The advantage of this approach is that enhancements to existing applications and new manager applications may be developed without concern about the MIB technology of the target agent, bringing the management of high-speed networks from an end-to-end perspective that is much closer to reality.

For the time being, however, the Nways Switch Manager applications are to drive both the CMIP MIB and the SNMP MIB for the Networking BroadBand Services nodes. Of course, only one type of agent, CMIP or SNMP, is permitted in a single agent node. But the same manager applications will operate on subnetworks composed of SNMP agents, or subnetworks composed of CMIP agents, or with a subnetwork that combines both network management technologies.

Conclusion

The architecture for the management of NBBS addresses important challenges. It attempts to provide high-level, easy-to-use applications to drive the automated processes for WAN transport services offered by Networking BroadBand Services. For the most part, NBBS automated control functions for the configuration of the network, and the location and selection of network resources during network connection setup has permitted the development of network management solutions to focus on the connection management, where the initial-value specifications for connections and the monitoring of connections are the primary concern of management activity. However, the management of NBBS as it is realized in the Nways switch has also required management of the details of each node at the hardware level. Therefore, the complete management solution offered for Nways integrates the management of the logical transport functions offered by the Nways switches and the Nways hardware configuration details of the nodes that deliver the NBBS function.

The choice of Common Management Information Protocol technology as the basis for NBBS network management has been discussed, and its merits enumerated.

The managed object model used to support the objectives of the management of NBBS and the hard-

ware components of NBBS nodes have been presented. An overview of how the managed objects defined for management activities of topology, accounting, performance, fault, configuration, and hardware correspond to application requirements has been given.

It has been shown that the manager applications can be extended to provide additional services to customer network management centers through SNMP or to an SPE Telecommunications Management Network subnetwork management environment. Thus, the network management solution for NBBS transport can be applied to small campus feeder subnetworks, intermediate enterprise WAN subnetworks, and large SPE transport networks.

The flexibility in the use of the network management solution and its capability to meet very different subnetwork objectives has been discussed. The extension of the Nways Switch Manager applications through a proxy agent has shown the direction of being able to drive both CMIP and SNMP manager interfaces. The extension of the NBBS MIB to its equivalent SNMP MIB has been presented as a way of scaling the management agent part of the network design.

Finally, the development of NBBS network management and its implementing product, the Nways Switch Manager, emphasizes how the combination of architectural vision with innovative product development can contribute to a superior solution—one that can be readily extended to meet the challenges of today's high-speed networks.

Acknowledgments

I thank the following colleagues for their help on this paper: Peter Lenhard, for suggestions on simplifying an early draft for wider audience appeal; Matt Hess, for high-level perspective and management support; and Gary Schultz, for advice on the paper's organization and level of detail, and for his generous editorial assistance.

Cited references and notes

1. M. O. Allen and S. L. Benedict, "SNA Management Services Architecture for APPN Networks," *IBM Systems Journal* **31**, No. 2, 336–352 (1992).
2. M. Willett and R. Martin, "LAN Management in an IBM Framework," *IEEE Network* **2**, No. 2, March 1988.
3. D. Comer, *Internetworking with TCP/IP, Vol. I: Principles, Protocols, and Architecture*, Prentice Hall, Englewood Cliffs, NJ (1988).
4. CCITT Recommendation M.3100 (1992), *Generic Network Information Model*, abbreviated as M.3100. TA-NWT-001114, *Generic Requirements for Operations Interfaces Using OSI Tools: ATM/Broadband Network Management*, Bellcore (October 1992).
5. G. A. Marin, C. P. Immanuel, P. F. Chimento, and I. S. Gopal, "Overview of the NBBS Architecture," *IBM Systems Journal* **34**, No. 4, 564–589 (1995, this issue).
6. ISO/IEC 9596-1:1991, *Information Technology—Open Systems Interconnection—Common Management Information Protocol, Part 1: Specification.*
7. RFC-1157, *Simple Network Management Protocol*, and RFC-1156, *Management Information Base for TCP/IP Based Networks.* These RFCs and others can be obtained by writing to the governing body, which is the Internet Engineering Task Force (IETF). (Electronic mail: ietf-web@cnri.reston.va.us)
8. CCITT Recommendation M.3100 (1992), *Generic Network Information Model*, and CCITT Recommendation M.3010 (1991), *Principles of Telecommunications Management Network.*
9. ITU-T Recommendation X.700 (1992), *Management Framework Definition for Open Systems Interconnection (OSI) for CCITT Applications*, and ISO/IEC 7894-4:1989, *Information Processing Systems—Open Systems Interconnection—Basic Reference Model, Part 4: Management Framework*. For CMIP, the referenced documents define the MIB as the conceptual repository of management information within an open system. SNMP has no formal definition for the term MIB, but refers to a collection of management information definitions.
10. *Frame Relay Service Customer Network Management Implementation Agreement (MIB)*, March 25, 1994 Frame Relay Forum Technical Committee, and *ATM User-Network Interface Specification*, June 1994 ATM Forum. With the increased acceptance of SNMP outside the Internet, forums established to accelerate protocol interoperability, such as the Frame Relay Forum and the ATM Forum, have also been contributing heavily to the development of SNMP MIBs.
11. CCITT Recommendation X.722 (1992)|ISO/IEC 10165-4: 1992, *Information Technology—Open Systems Interconnection—Structure of Management Information—Guidelines for the Definition of Managed Objects*, abbreviated as GDMO.
12. CCITT Recommendation X.721 (1992)|ISO/IEC 10165-2: 1992, *Information Technology—Open Systems Interconnection—Structure of Management Information—Definition of Management Information*, abbreviated as DMI.
13. ITU-T Recommendation X.723 (1993)|ISO/IEC 10165-5: (1993), *Information Technology—Open Systems Interconnection—Structure of Management Information—Generic Management Information*, abbreviated as GMI.
14. *Desktop Management Task Force Interface Specification*, Version 1 (April 29, 1994). The Desktop Management Task Force (DMTF) (electronic mail: dtmf-info@dtmf.org) has defined a standard to permit access to the MIB contents of a desktop resource by any network management protocol. Desktop resource information is stored in a technology-independent manner in a Management Information Facility (MIF). The MIF data can be accessed by a management agent (or directly by a manager with Remote Desk-

top Management Interface [RDMI]) through the use of a service layer that coordinates the MIB specific requirements of the agent and the component specific definitions of the desktop resource. *NetFinity LAN Management Made Easy*, G511-3125, IBM Corporation; available through IBM branch offices.
15. T. E. Tedijanto, R. O. Onvural, D. C. Verma, L. Gün and R. A. Guérin, "NBBS Path Selection Framework" *IBM Systems Journal* **34**, No. 4, 629–639 (1995, this issue).
16. M. Peyravian, R. Bodner, C.-S. Chow, and M. Kaplan, "Efficient Transport and Distribution of Network Control Information in NBBS," *IBM Systems Journal* **34**, No. 4, 640–658 (1995, this issue).
17. C. P. Immanuel, G. M. Kump, H. J. Sandick, D. A. Sinicrope, and K. V. Vu, "Access Services for the Networking BroadBand Services Architecture," *IBM Systems Journal* **34**, No. 4, 659–671 (1995, this issue).
18. IBM Portable CMIP Platform PRPQ HONE number P85481, formerly known as "CMIP Works." The original documentation, P. Reder, "CMIP Works for Agent or Manager Platforms," is available by anonymous FTP from www.raleigh.ibm.com in the directory: pub/protocols/mgmt/cmip/cmipWorks.
19. ISO/IEC 10165-1, *Structure of Management Information Part 2: Management Information Model. Relative Distinguished Name* (RDN) is the term given to the concept that each managed object class will provide a naming attribute whose value permits uniqueness among any members of the managed object class.
20. ISO/IEC 8824, *Specification of Abstract Syntax Notation One (ASN.1).*
21. IBM participated actively in the ISO X3T5/4 in the definition of the CMIP Alarm format in an attempt to align the concepts and components with the already published generic alert architecture. (R. E. Moore, "Utilizing the SNA Alert in the Management of Multivendor Networks," *IBM Systems Journal* **27**, No. 1, 15–31 [1988].) IBM also provides a mapping application from the CMIP alarm format to the generic alert format, thereby extending the fault management reach for problem determination. (*IBM LAN NetView Tie Administration Guide*, S96F-8575, IBM Corporation; available through IBM branch offices.)
22. CMIP defines several standard actions: CREATE and DELETE are examples of actions that establish change MIBs; ACTIVATE and DEACTIVATE are examples of standard actions that allow MIB states to be changed.
23. ISP-11183-1, *International Standards Profile: ACSE, Presentation, and Session Protocols for the Use by ROSE and CMISE* (May 1992).
24. *IBM SystemView for AIX Features and Functions*, GH19-4213, IBM Corporation; available through IBM branch offices, and *IBM SystemView for AIX: An Overview*, GC24-2541, IBM Corporation; available through IBM branch offices.
25. Managed object classes for NBBS are named by starting the object class name with lowercase "ab." By GDMO standard, all names are value identifiers and must start with at least one lowercase alphabetic character. The use of the prefix "ab" derives from the architecture codename for NBBS, which was AutoBahn (for a high-speed data highway).
26. G. Lebizay, C. Galand, D. Chevalier, and F. Barre, "A High-Performance Transport Network Platform" *IBM Systems Journal* **34**, No. 4, 705–724 (1995, this issue).
27. Network management flows are used to convey the network connectivity information from the trunks in the nodes to the Nways Switch Manager topology application. After successful link establishment, the negotiated trunk information is loaded into the topology database and propagated to the other connection nodes in the network. The topology information that flows between nodes in the NBBS network for network control purposes, however, is not comprised of network management flows, but of special flows designed to carry the topology information.[16]
28. R. Bird, C. Brotman, R. Case, G. Dudley, R. Moore, and M. Peters, "Advances in APPN Architecture," *IBM Systems Journal* **34**, No. 3, 430–451 (1995).
29. With the advent of multiplexing medium access control (MAC) protocols that did not share a medium, such as frame relay and asynchronous transfer mode, it becomes necessary to monitor the usage of each individual user of the medium in order to prevent congestion in the switching network. (LAN protocols achieve congestion control by collision detection and back-off, or by using timed or token access to the medium.) Therefore, each connection is policed to determine if the traffic it is presenting to the network conforms to, or is in excess of the requested maximum for the connection. Even if connection traffic is in excess of the requested maximum for a connection, it can still be transmitted to the network. However, excess traffic for a connection is usually treated as discard-eligible while in transit by a type of marking placed in the MAC header.
30. This capability is referred to as Virtual Private Network (VPN). A VPN provides the customer with the capability through network management control to logically partition, allocate, and control the real network resources of a service provider network as if the network resources were owned by the customer.
31. In the Asynchronous Transfer Mode Forum Specifications UNI-3.1, the network management model closely parallels the Telecommunications Management Network (TMN) model. The interface between CPE and SPE manager is called the M3 interface and the interface between SPE managers is called the M5 interface. Both these interfaces for support of asynchronous transfer mode activity can be supported by extensions to the Nways Switch Manager.
32. R. E. Moore and J. Panian, "CMIP/SNMP Integration Prototype," *Network Operations and Management Symposium (NOMS 94) 1994 IEEE Network Operations*, Volume 1 (February 14–17, 1994), pp. 257–267.
33. The "Q3 mapper" is being developed at the IBM Heidelberg Laboratory to support the coexistence between NBBS MIB particulars and the generic requirements of cross-connection style networks described in ATM Forum Specification M4 and ITU-T Recommendation G.atmm.

Accepted for publication July 20, 1995.

Stephen A. Owen *IBM Networking Hardware Division, 800 Park Offices Drive, Research Triangle Park, North Carolina 27709 (electronic mail: sowen@vnet.ibm.com).* Mr. Owen, who received B.A. degrees in economics and philosophy and M.A. and M.S. degrees in French and computer science from the University of Wisconsin–Madison, joined IBM in 1984 and worked on LAN interconnection strategies, particularly the source routing concepts applied to token ring. In 1986 Mr. Owen was named Standards Project Authority for ISDN Network Management and worked on several early CMIP-based MIB definitions for ISDN systems. He has been active in network management standards in the ITU-T and in ANSI-T1, where he was a past chairman of T1M1.2 Internetwork Operations. He has developed the MIBs for frame relay and Networking BroadBand Services network management and is currently working on the management of asynchronous transfer mode. His current interest is applying cognitive models to network control algorithms.

Reprint Order No. G321-5591.