255-184-142
Issue 1
Release 4.0

BNS-2000
System Description

Multimegabit Switching for the 1990s

ACCUMASTER, ACCUNET, Acculink, Billdats, Billdats II, CommKit, Comshere, *Datakit*, Dataphone, Definity, Paradyne, *StarKeeper*, *StarGROUP*, Systimax, and Teletype are registered trademarks of AT&T.
Amdahl is a registered trademark of Amdahl Corporation.
Comten is a registered trademark of NCR-Comten, Inc.
DataSMART is a registered trademark of Kentrox Industries, Inc.
IBM and Token Ring are registered trademarks of International Business Machines Corporation.
D/I MUX is a trademark of COASTCOM.
INFORMIX is a registered trademark of Informix Software, Inc.
Microcom is a trademark of Microcom, Inc.
OPEN LOOK and UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.
Penril and Datalink 2400 are registered trademarks of Penril Corp.
Pyramid is a trademark of Pyramid Technology Corporation.
SecurID is a registered trademark of Security Dynamics Technologies, Inc.
Sprintnet and Telenet are registered trademarks of GTE Telenet Communications Corporation.
Stratus is a registered trademark of Stratus Computer, Inc.
Sun is a registered trademark of Sun Microsystems, Inc.
Tandem is a registered trademark of Tandem Computer.
Uniscope is a registered trademark of Unisys Corporation.
Verilink is a registered trademark of Verilink Corporation.

Contents

Figures

Tables

Preface

This issue of the *BNS-2000 System Description* describes the features, capabilities, and operating characteristics of AT&T's BNS-2000 broadband switching product, Release 4.0. The *System Description* also includes information on related products that work in various applications and configurations of a BNS-2000 network.

Previous issues of the *System Description* contain information about earlier releases. The table below identifies existing issues of the manual and the software release each issue supports.

System Description Releases

BNS-2000 Release	System Description
R4.0	255-184-142, Issue 1
R3.0	255-184-136, Issue 1
R2.0	255-184-102, Issue 1
R1.2	255-183-110, Issue 1
R1.1	255-182-110, Issue 1
R1.0	255-181-110, Issue 1

Document Organization

This *System Description* includes seven chapters:

Product Overview — describes how BNS-2000 networks can be used in a variety of data networking and data services applications. Product architecture and data services are also discussed.

Networking Applications — describes typical user applications in which BNS-2000 is a recommended data networking solution.

Data Services and Features — describes BNS-2000 data services and the component combinations that provide these services. The chapter discusses features provided by the system software available to both network users and network administrators.

Hardware	describes BNS-2000 equipment: the node, cabinetry, concentrators, interface modules, and trunk modules.
Software Packaging and Configuration	focuses on the packaging and distribution of BNS-2000 software, the contents of feature packages, and the mechanics of feature selection. It discusses how the system software operates for each Control Computer System configuration, and describes upgrading capabilities.
Related Products	contains information about equipment and software products that operate with BNS-2000 networks.
Support and Services	contains information about training, documentation, customer assistance, and maintenance and support services.

Product Overview

Product Overview

The evolution in corporate computing has produced new requirements and definitions for networking services. To help companies link their computing resources, embedded terminal-to-host applications are being replaced by applications for distributed local area network (LAN) computing environments. During this transition, networks must support both the traditional host-oriented applications and the platforms needed by distributed LAN architectures. The resulting networks must include access, architecture, and service features to support both types of network traffic. Wide area products, built on open standards, protect existing applications and provide a network environment for future expansion and services.

AT&T's BNS-2000 product is designed to provide high-speed services in public and private wide area networking (WAN) applications. The BNS-2000 is a high-performance cell relay switch that supports broadband services including Switched Multimegabit Data Service (SMDS), frame relay, and embedded terminal-to-host environments. It offers key features for access, networking, security, administration, maintenance, redundancy, and reliability — based on industry standards.

The BNS-2000 switch interworks with and is part of the family of AT&T data networking products that includes the *Datakit*® II Virtual Circuit Switch (VCS), LCS60 access server, CommKit® Host Interface Software and associated equipment for host access flexibility, and the *StarKeeper*® II Network Management System (NMS).

The full range of BNS-2000 services can be delivered from one multiservice platform, promoting savings in equipment, facility, and operations costs for public service providers and private network owners. The 200 Mbps bandwidth capacity supports a large number of access lines that allow service providers to minimize the number of nodes and associated costs, and network complexity. Support for multiple interfaces permits a mix of traditional host-centered terminal access applications and LAN access services on the same platform.

Product Architecture

The BNS-2000 supports standards for cell relay and broadband technologies. Architecture based on SMDS and frame relay standards provides a clear path to emerging cell-based broadband services — services that are positioned to dominate network applications in the near future. The BNS-2000 nodes can be seamlessly connected via these standards to higher speed cell-relay nodes to create broadband switching systems that will support true multimedia communications.

BNS-2000 architecture supports switching and transport services for both connection-oriented and connectionless network traffic. The data services available through BNS-2000 simultaneously support addressing and routing for both types of data traffic.

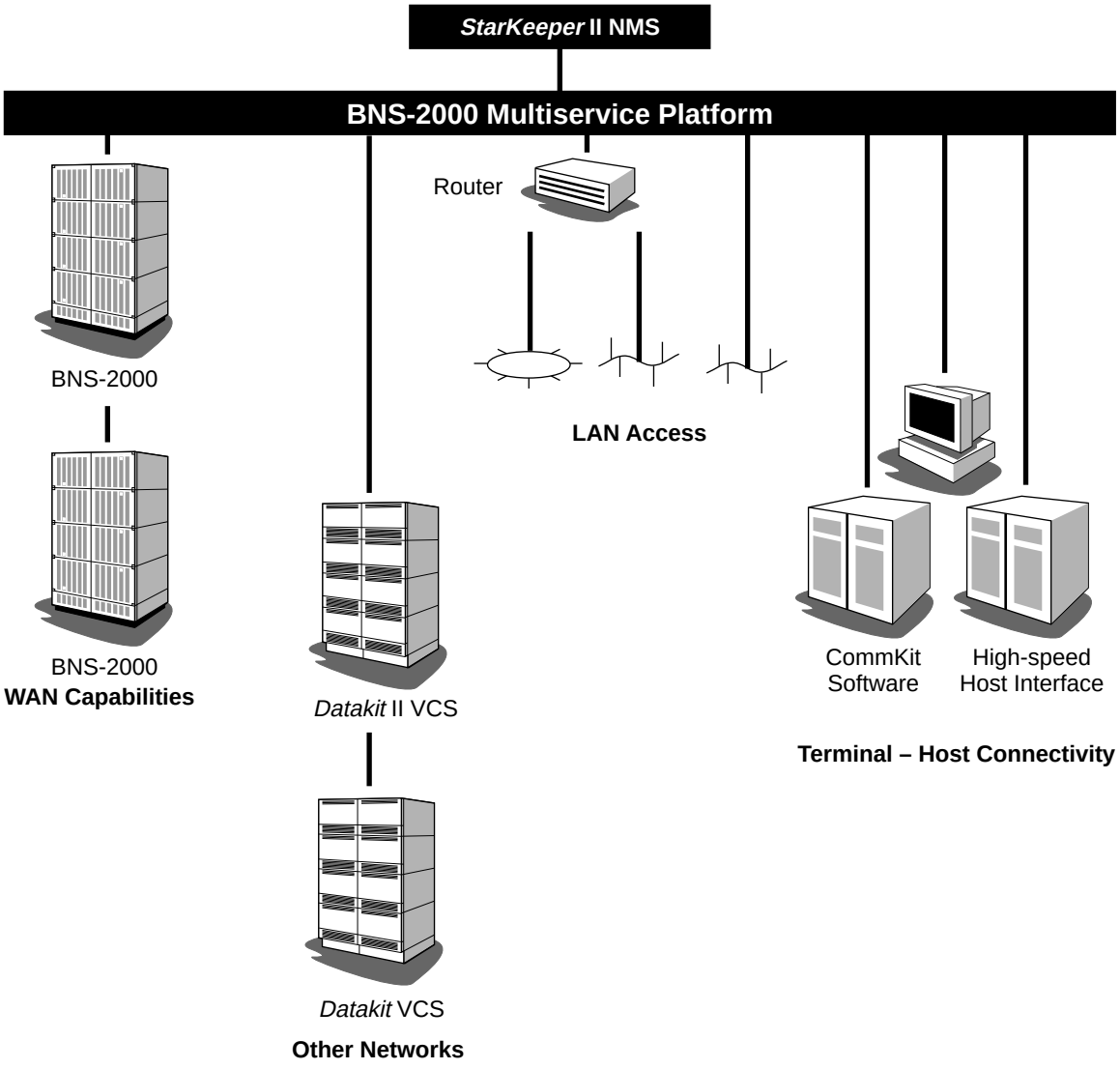

FIGURE 1-1. BNS-2000 Product Architecture

BNS-2000 architecture is modular, which promotes efficiency for growing network applications and future standardization. Node hardware can accommodate any network's current size and projected growth. Every interface type is provided on a separate module within the node, with one function per module or, sometimes, per port. Modules can be installed as needed, allowing for easy network growth. As new services or protocols are defined, additional interface module types can be integrated into the existing architecture. Moreover, additional modules and nodes can be deployed in the network and additional data centers can be supported without disrupting

service to existing network users.

The modular physical architecture also underlies a key strategy of BNS-2000 — hardware redundancy. Nodes can be equipped with backup power modules, control components, switch modules, trunks, and interfaces to create hardware redundancy that improves overall network reliability, making BNS-2000 a good choice for public service applications.

Physical design complies with the standards established for telephone company central office (CO) frame construction, power requirements, alarm notification, and earthquake testing, giving the product an economic edge for CO applications.

Cell Relay

In cell relay technology, data is switched in packets called *cells.* Cell relay technology is capable of providing very high transmission rates across WANs. With cell relay, fixed-length cells of data are relayed — switched — over the network at high transmission rates. This network transport and switching technology allows all forms of information (data, voice, image, and video) to be carried efficiently through the same network infrastructure.

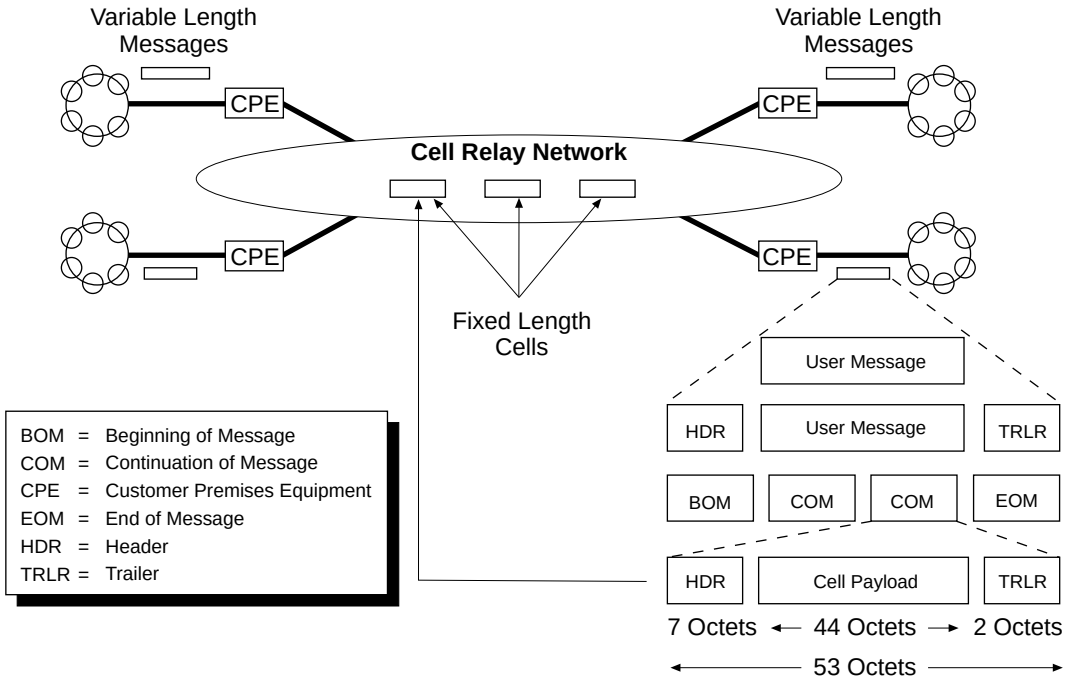

FIGURE 1-2. Cell Relay Network

Network Traffic

Services on BNS-2000 networks support switching and transport for two fundamentally different types of traffic:

- connectionless network service (CLNS)
- connection-oriented network service (CONS).

The two types of service differ in their routing and addressing handling. Each service includes its own special benefits and distinct networking capabilities.

Connectionless Network Service (CLNS) Traffic

Messages in connectionless service are broken into individual segments at the source, and the segments are routed independently through the network. The basic principle of CLNS routing is that each data segment is broadcast on the backplane bus to all connectionless modules. Each module responds only to segments that are addressed to endpoints within its jurisdiction, forwarding such segments through the network. Establishing or maintaining connections between source and destination endpoints is unnecessary, so a virtual circuit is never required.

Eliminating the need for a virtual circuit between the source and destination endpoints provides an additional advantage because data may be transferred over different facilities. Since the data do not necessarily have to follow the same path, additional route diversity is built in, allowing data to arrive at the destination despite a facility interruption.

In practice, when a trunk module accepts a data message segment for transport, it will accept all subsequent segments of the same message. If that trunk facility is inoperative, a different trunk module will accept the remaining segments, using the same routing criteria, and transport them to the destination. Since connectionless data may follow different paths, data segments do not necessarily arrive in the same order in which they are sent. Message re-assembly is the responsibility of the customer premises equipment (CPE), such as routers.

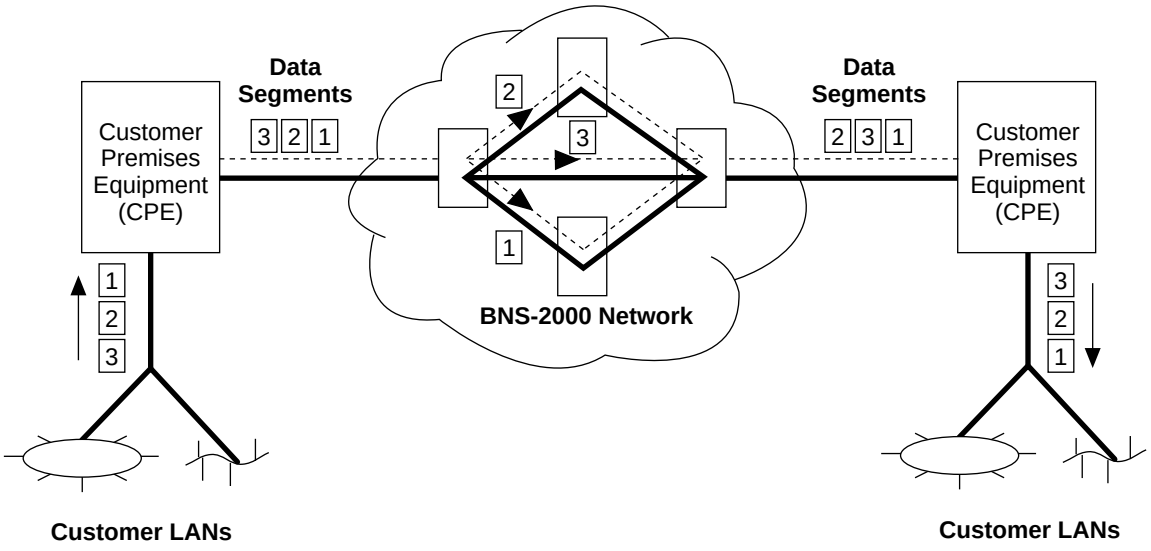

FIGURE 1-3. Connectionless Network Service (CLNS)

The various types of paper mail service represent an analogy of CLNS routing. Mailing a number of envelopes at the same mailbox is similar to the method used by BNS-2000 to switch connectionless traffic. Even if several of the envelopes have the same destination, they may take different routes and use different carriers to that address. They may arrive at the destination in random order, but their successful delivery does not depend on the operation of a single carrier.

CLNS is a standard method of transporting LAN traffic, and BNS-2000 connectionless service permits very high-speed LAN interconnection across a WAN.

Connection-oriented Network Service (CONS) Traffic

To route connection-oriented traffic, the network first establishes a virtual circuit between the source and destination endpoints. When a circuit is established, a series of messages can be exchanged between the source and the destination endpoints. Circuit establishment for connection-oriented traffic is performed by a Control Computer.

After the virtual circuit is set up, all data sent from the source to destination endpoints traverse the same path. The data arrive in the same order in which they are sent. When the data transfer is complete, the node Control Computer disconnects the endpoints and takes the circuit down.

Telephone service represents an analogy of CONS routing. The method used by BNS-2000 to switch connection-oriented traffic has similarities to dialing, talking, and hanging up a telephone call. Asynchronous service is an example of a data service that routes data via CONS.

Wide area networking capabilities with CONS offer a variety of trunk options, including T1/E1,

T3/E3, and fiber optic trunks. Services also include automatic alternate internodal routing on call setup and automatic rerouting of active trunk traffic affected by facility disruptions. T3 trunk options provide additional shared trunking solutions for data traffic as networks grow. The high bandwidth minimizes service degradation resulting from network congestion.

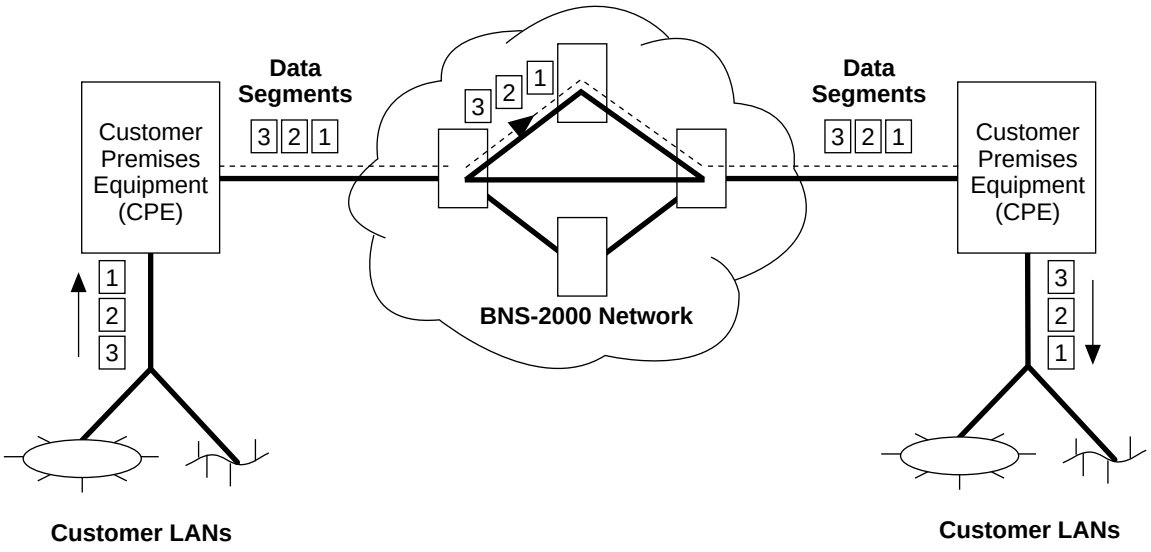

FIGURE 1-4. Connection-oriented Network Service (CONS)

Additional Data Services

BNS-2000 networks also support the following data services:

- Switched Multimegabit Data Service (SMDS), a high-speed, connectionless, public packet switching service that can extend local area network (LAN)-like performance across a wide area
- switched or non-switched connections for asynchronous communications, at speeds up to 115.2 Kbps, including remote access to devices on local area networks (LANs) and dial-in/dial-out modem pools
- switched or non-switched, point-to-point and multipoint connections for bisynchronous communications and synchronous transport between terminals, terminal clusters, and hosts, using a variety of synchronous protocols
- high-speed multiplexed host interfaces for access to asynchronous hosts, including devices functioning as local area network (LAN) servers

- interconnection and interoperability between LANs, including routers and bridges between LANs that use either common or different protocols
- connectivity for Ethernet LAN users to Transmission Control Protocol/Internet Protocol (TCP/IP) applications on remote hosts connected to the network
- routing and communications services between LAN-based clients and multiprotocol devices on the network
- frame relay interface transport across the network for commercial routers
- direct Ethernet access without the need for routers
- switched, two-way communications for BNS-2000-connected asynchronous terminals and X.25 hosts to multiple X.25 hosts on BNS-2000, or on a packet-switched public data network (PSPDN)
- switched two-way communication with X.75 National and International Gateways
- interworking with AT&T's *Datakit* II VCS and Information Systems Network (ISN)
- interworking with AT&T's Definity® 75/85 Communications System
- connectivity and feature support for local common carrier traffic management Operations Systems (OS)
- support for a variety of data communications and networking standards and product line component compliance that permits international use

Reliability

BNS-2000 reliability can be expressed as availability of the network. Availability can be calculated for the BNS-2000 network using the following two performance measurements.

- *Mean Time Between Failures (MTBF)* — MTBF is the average time that a system can provide data transport between two endpoints before a hardware failure occurs. For a BNS-2000 node with a simplex configuration (one that contains a single Control Computer and switch module), the MTBF is about seven months.
- *Mean Time To Repair (MTTR)* — MTTR is the time it takes an operator to repair a service-disrupting failure. For a BNS-2000 node, the time required to replace the backplane bus is two and one-half hours. All other common and interface modules can be replaced in one-half hour.

Availability is based on the MTBF and MTTR figures, and is a function of the rate of occurrence of failure and the duration of repair time. A simplex BNS-2000 node is available 99.97% of the time, or has an average downtime of 2.76 hours per year.

Overall reliability and availability can be increased by adding optional redundant hardware components that can be placed in service if hardware failure occurs in the primary components.

BNS-2000 nodes can be configured with optional redundant Control Computers (with redundant switch modules), and can also include a redundant switch module in the single Control Computer configuration. Manual and automatic recovery options are available both for redundant Control Computers and redundant switch modules. For redundant Control Computers, these options are described below.

- *Manual recovery option* — The manual recovery option uses a warm spare Control Computer. The spare Control Computer contains the basic system configuration database. The spare Control Computer can be manually placed in service if the primary Control Computer fails. Its database can also be manually updated.
- *Automatic recovery option* — The automatic recovery option uses active and standby Control Computers monitored and controlled by a Maintenance and Redundancy Control (MRC) function. The standby Control Computer contains a backup copy of the configuration database. The MRC function monitors the two Control Computers for sanity, and determines whether their status is active or standby. The MRC function can detect a problem in the active Control Computer in 15 seconds or less. When a problem is detected and the recovery option is set to on, the MRC function initiates the automatic recovery. It switches the status of the active and standby Control Computers and resets them, resulting in a warm reboot of the node. During the warm reboot, calls in progress are not affected; new calls can be placed and existing calls can be taken down after the warm reboot is completed.

In a single Control Computer configuration, an optional redundant switch module provides network reliability through a capability to recover from a failure of the active switch module. Both switch modules are in the single control cabinet. The Control Computer issues commands to both switch modules collectively over a common command channel, or individually over separate command channels. During normal operation, one switch module is recognized by the Control Computer as the in-service active switch module. It functions as the node's switching mechanism, forwarding packets between addresses stored in its memory. The other switch module is recognized by the Control Computer as the in-service standby switch module. The standby switch module shadows the active switch, so that during normal operation the routing memory in both switch modules is identical. If the in-service active switch module fails, a quick switchover with no data loss occurs.

The manual and automatic recovery options available for the redundant switch modules are described below.

- *Manual recovery option* — As long as the standby switch module responds to status and sanity polling and is in service, the network administrator can initiate a command to make it the active switch.
- *Automatic recovery option* — The Control Computer monitors the health of both switch modules to ensure that a successful recovery can be initiated if needed. Polling establishes the status and the existence of any detected errors for each switch module, while also checking that the memory for both switch modules is synchronized. Irregular conditions reported in the status packets of the active switch will cause the Control Computer to deactivate the active switch module and automatically initiate a command to bring the standby switch module to active status if the standby switch module is in service. Unless there is a simultaneous

problem with the standby switch that prevents it from participating in the switchover, the switchover is completed and a message is generated to indicate the success of the recovery.

Maintenance

Another aspect of BNS-2000 reliability is the comprehensive set of system tools that place maintenance within the capabilities of most customer support organizations.

The maintenance strategy for BNS-2000 relies heavily on internal diagnostic routines. With hardware faults, these diagnostic routines can usually isolate faults to the module level, and recovery can be performed by replacing the faulty module with a spare.

The basic strategy is to identify and report faults, isolating them to field-replaceable units, and to take advantage of the available tools to troubleshoot problems.

- *Status LEDs* — Status light-emitting diodes (LEDs) on BNS-2000 components monitor the state of the component. A visual check of the LEDs can supply information needed to make a maintenance decision.
- *Self-tests* — The system administers self-tests at regular intervals that monitor the node, concentrators, and their components for evidence of failure:
  - *Status polling*. Status polling is a means of detecting module faults and hardware states by sequentially testing all modules. The Control Computer instructs the Clock module to poll all slots regularly for their status. Status packets report the poll results to the Control Computer. If the information reports a module in an alarm state or the module fails to report any status, the Control Computer generates the appropriate alarm. The switch module enhances this strategy by capturing the source module and channel numbers of packets that cause errors. This source address allows the administrator to isolate any module generating bad packets.
  - *Transient failures*. Transient failures are reported after the number of errors exceeds the predetermined threshold within a set period of time.
  - *Sanity tests*. In sanity tests, firmware diagnostics exercise the hardware components to ensure that the module is operating logically and to detect and report faults.
  - *Automatic loopback tests*. Automatic loopback tests are provided for all trunk, concentrator link, and multiplexed host connections to ensure that the connection is up.
  - *Watchdog timer*. A watchdog timer activates an audible alarm that signals a Control Computer crash when keep-alive signals sent from the Control Computer to the timer do not appear within a given period of time.
- *Diagnostic tests* — Diagnostic tests, which are sometimes service-disruptive, locate and isolate defective modules or bad transmission paths and are available for all control modules (including the MRCM), interface modules, trunks, and concentrators.
- *Alarms* — Alarms are generated by the system to show errors of three magnitudes: critical,

major, and minor. The system reports identical errors at intervals specific to the alarm type.

- *Reports* — The system provides four types of reports that are useful in determining the appropriate maintenance procedures to take:
  - *Verification reports*. These reports show static information about a component as it is entered in the database.
  - *Display reports*. These reports provide dynamic information on the actual hardware and software states of various components.
  - *Status display reports*. These reports provide useful information that reflects greater detail than the alarm system reports.
  - *Measurement reports*. These reports help locate and identify problems because the traffic and performance information they contain can be analyzed to deduce reasons for potential errors. Measurement reports can be generated manually, by system routines, or by *StarKeeper* II NMS.

In addition to system tools, BNS-2000 provides an extensive set of commands that can be entered by operators at the console. The commands are supported by on-line help screens. The *Data Networking Products Commands Reference* as well as interface module and concentrator reference documents describe these commands.

Session Maintenance

Session maintenance is a feature that provides data transport reliability over internodal trunks in BNS-2000 networks. The feature provides the capability to maintain user sessions by automatically rerouting active sessions from the failed facility over spare capacity on other trunks within the network.

The session maintenance feature is designed to take advantage of several capabilities and strategies of BNS-2000 networks:

- Session maintenance is supported on all BNS-2000 trunk types except connectionless-only trunks. This support allows network-wide administration to provide recovery from facility failures, and adds fault tolerance for trunks that complements node and concentrator high availability features.
- Most existing networks with sufficient bandwidth and internodal connectivity can support failure recovery via session maintenance without physical modification. Administrators can configure previously unused trunk capacity in the network for use as standby trunk capacity that supports the alternate reroute paths required for session maintenance activities.
- Session maintenance eliminates the need to back up regular trunks with spare trunks that are used only when the regular trunks fail. It allows administrators to make optimal use of the bandwidth capacity available in the network by allowing normally routed and rerouted traffic to share the same trunks.
- Integration between BNS-2000 and *StarKeeper* II NMS provides a means of administering the

session maintenance feature in BNS-2000 networks. Configuration and monitoring activities for session maintenance are centralized in *StarKeeper* II NMS Network Builder. The Network Builder also provides a simulator tool that models trunk failure and recovery events throughout the network, allowing administrators to preview the expected performance of trunks set up for session maintenance without putting actual traffic at risk.

Session maintenance is especially useful for network applications that require high availability and end-to-end reliability. Session maintenance complements BNS-2000 hardware redundancy features by increasing internodal trunk availability to avoid active call disconnections from errors that result in trunk failure.

Session maintenance administration includes characteristic BNS-2000 flexibility. Networks with alternate internodal connectivity over trunks that support session maintenance can rely on automatic rerouting controlled in part by configurable parameters. Although the parameters supplied by the system when the feature is configured are generally sufficient, most parameter values as well as the order in which the system selects alternate trunk paths can be changed by administrators. This option allows administrators to direct calls over a certain trunk, maintaining necessary throughput or isolating call traffic to specific paths appropriately for their networks.

The centralized administration services provided by *StarKeeper* II NMS Network Builder simplify ongoing session maintenance management as the network grows or as network services and traffic patterns change. Network administrators can make use of capabilities that permit snapshots of network behavior during selective simulated trunk failures and rerouting events. These capabilities permit administrators to model a variety of trunk failure scenarios, using the output to make reliable decisions about tuning trunks throughout the network for optimal performance.

Administration and Network Management

BNS-2000 administration and network management is performed using the *StarKeeper* II Network Management System (NMS). The BNS-2000 administration workstation provides limited functionality local console access for node administration.

StarKeeper II NMS Overview

StarKeeper II NMS is a multifunction, UNIX®-based operations system that manages the complete line of BNS-2000 nodes, concentrators, gateways, and other network elements in geographically dispersed networks from one central location. It provides a full range of network management functions, and can be used for network configuration; node administration and maintenance; centralized collection, analysis, and reporting of traffic, performance, and billing data; and fault monitoring.

StarKeeper II NMS, built on the OSF/Motif™ Graphical User Interface, provides leading-edge network management features that enhance BNS-2000 usability. *StarKeeper* II NMS architecture consists of a Core System and a Graphics System. The Core System maintains connectivity to the BNS-2000 network, collects alarm, statistics, and measurements data from the network,

maintains the network configuration database, and performs basic (non-graphics) network management. The Graphics System includes a graphics platform and several optional graphics applications which provide graphics support of fault management, configuration management, and performance management.

StarKeeper II NMS maintains either a direct or virtual circuit connection to each node in the network. For a direct physical connection, cables connect the *StarKeeper* II NMS host to an administration port on the node. The virtual circuit connections are set up through the network. Redundant links to the network are possible.

Figure 1-5 is a functional diagram of the system components.

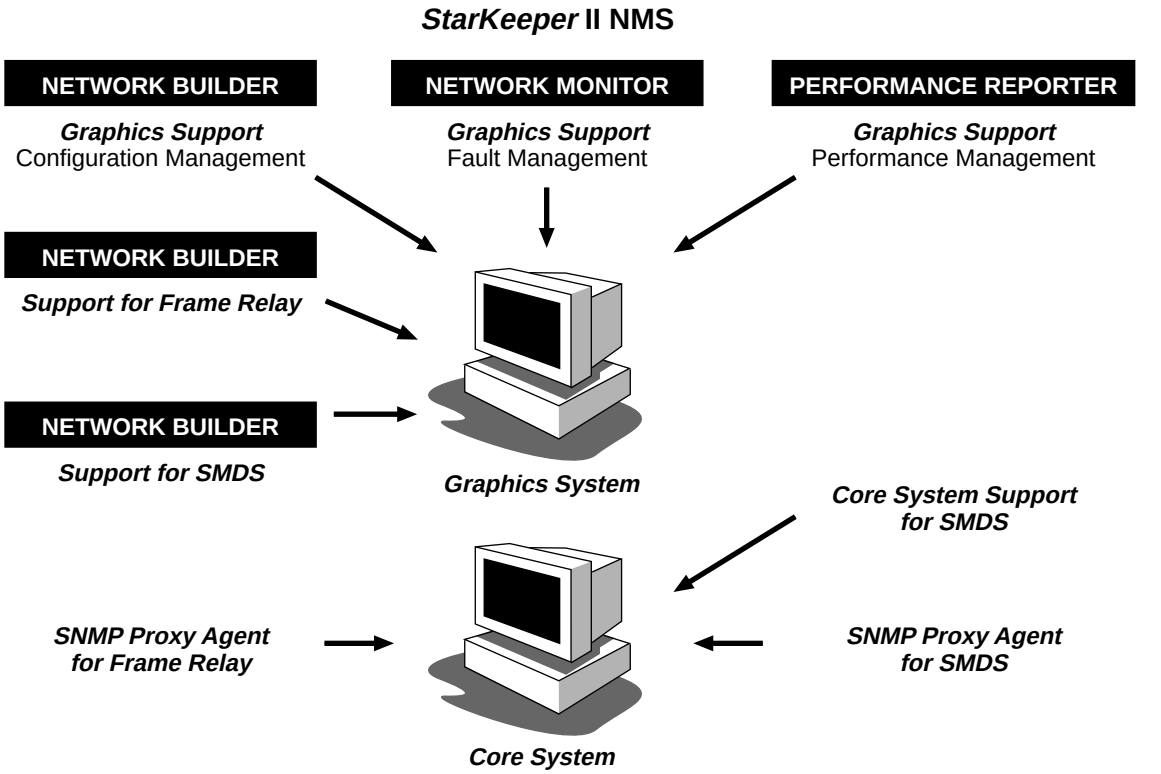

FIGURE 1-5. ***StarKeeper*** **II NMS Architecture Components**

Core System

Every *StarKeeper* II NMS needs at least one Core System, which runs on a *StarKeeper* II NMS host processor. A single Core System can manage multiple nodes or support several applications, or it can be assigned to perform one specialized function, such as billing or performance. As a network grows, the workload can be distributed to multiple Core Systems.

Multiple Core Systems can be used to divide the network workload either geographically or functionally. From a single workstation, a centrally located administrator can communicate with multiple Core Systems and manage equipment at many locations. This gives the administrator a consolidated network view even for very large networks. Centralized management significantly lowers network management costs.

Optional application packages that provide Core Systems with enhanced functionality for high-level network management tasks include the following:

- ***StarKeeper II NMS Simple Network Management Protocol (SNMP) Proxy Agent*** is an optional application for a *StarKeeper* II NMS Core System, allowing network management stations to interface with *StarKeeper* II NMS via SNMP. SNMP is a widely used protocol for managing TCP/IP based internets.

  The SNMP Proxy Agent supports SMDS and frame relay interfaces on BNS-2000, and will enable end-users to monitor the service provider's end of their SMDS and frame relay interfaces using the SNMP network management system on their own premises; that is, the Customer Network Management (CNM).

  The SNMP Proxy Agent initially allows customers to monitor the current status of their interfaces, retrieve performance measurements and error counts, and receive alarms on changes in the status of their interfaces

- ***StarKeeper II NMS Core System Support for SMDS*** is an optional application for a *StarKeeper* II NMS Core System. The Core SMDS package must be used when using SMDS. The Core SMDS package provides Core support for on-demand displays of SMDS measurements and statistics.

Graphics System

A *StarKeeper* II NMS Graphics System can reside on the same processor as the Core System or on a separate processor that interacts with the Core System. A Graphics System uses the databases on one or more specified Core Systems. A Graphics System consists of the Graphics System Platform and one or more optional graphics applications. Many Graphics Systems can co-exist in the network and one Graphics System can be connected to multiple Core Systems.

Graphics System components include the following:

- ***StarKeeper II NMS Graphics System Platform*** must be installed on a Graphics System before any other graphics applications are installed. The Graphics System Platform provides graphics capabilities for the installed application packages. The platform provides the following capabilities:

- ***Cut-Through Application*** allows window access to one or more StarKeeper II NMSs or other systems for additional interaction. The Cut-Through Application allows you to emulate an asynchronous terminal within the graphics environment and connect to a StarKeeper II NMS Core System or a network element console.
- ***Bulletin Board*** posts messages to the user. When an application sends a message, a glyph (icon picture and label) is displayed in the Bulletin Board area. There may be multiple glyphs displayed simultaneously. The topic of the Bulletin Board can be determined from the design of the glyph. There are four types of glyphs that may appear in the Bulletin Board area: file system, database, communications, and computer resources.
- ***Workstation Administration*** allows the user to establish connections to remote StarKeeper II NMS machines, to specify files and directories for automatic cleaning, and to have access, simultaneously, to several different computers in a network from a single Graphics System via the Cut-Through application.

The Graphics System Platform also introduces a user-friendly graphic interface, based on the OSF/Motif and HP Visual User Environment (VUE), that makes the other StarKeeper II NMS Graphics System software easy to use. This state-of-the-art user interface offers windows that display data and commands, menus for user choices, mouse point-and-click selection, color network maps (Network Monitor application), color-coordinated application packages, and help screens. As a result, novices can quickly become productive network managers.

- ***StarKeeper II NMS Network Monitor*** is an optional Graphics System application used for fault management by providing alarms and diagnostics capabilities on geographic network maps. Network Monitor provides an easy-to-use map editor and the ability to generate maps automatically. You can also display real-time alarms in network maps and alarm lists.
- ***StarKeeper II NMS Network Builder*** is an optional Graphics System application used for configuration management and analysis. Network Builder provides a Forms Interface to configure nodes, groups, trunks, and service addresses. Network Builder also allows for configuration of routing information and databases. Network Builder use is required when using SMDS or session maintenance (a node optional trunk recovery feature) and is highly recommended when using Frame Relay.
- ***Performance Reporter*** is an optional Graphics System application used for routine performance assurance and long-term traffic engineering. Performance reports for resource utilization and error counts are provided as well as thresholding of error counts and performance measurement indicators. Measurements available from StarKeeper II NMS help the network administrator observe areas of network usage to anticipate network needs.

StarKeeper II NMS Features

StarKeeper II NMS supports the following basic set of features:

- ***System operations and maintenance functions*** — Most operations performed at the local BNS-2000 administration workstation can be performed via *StarKeeper* II NMS. These include full configuration capabilities (**enter**, **change**, **delete**), running available on-line

diagnostics, requesting available status displays, rebooting a node, removing/restoring a module from/to service, and controlling measurements collection and scheduling.

- ***Network graphics displays*** — *StarKeeper* II NMS supports color bit-mapped graphics. Different views of the network are possible through user-defined network maps. Alarms are color-coded on the display by severity level. The graphics interface includes a forms interface for configuration and other tasks.
- ***Logging of all command entries and responses*** — Command entries and system responses are logged in a file and are available for browsing.
- ***Logging of all error/alarm messages*** — *StarKeeper* II NMS maintains a log of all error/alarm messages generated at the nodes. This log file is available for browsing, with search capabilities supported by UNIX or INFORMIX® features.
- ***Alarm alerts*** — Alarms are delivered to *StarKeeper* II NMS as they occur. The severity of the alarm, full alarm message, and time of delivery are logged in the alarm database, and are available for display.
- ***Alarm handling*** — Alarms can have a status of active, deferred, or cleared; most alarms are active when first received.
- ***Alarm consolidation*** — A *StarKeeper* II NMS, configured as a master console, can receive and display alarms from other *StarKeeper* II NMSs and Dataphone® II System Controllers.
- ***Network configuration*** — *StarKeeper* II NMS maintains a configuration file of network-level information on nodes, trunks, and network connections. Configuration provides the capabilities to enter, delete, change, and display this information.
- ***Software download*** — *StarKeeper* II NMS can store the generic and maintenance software, download it to geographically dispersed nodes while the nodes are operational, and manage its installation remotely. The cutover of each node to the network can be done remotely from the *StarKeeper* II NMS console.
- ***Upload/download*** — *StarKeeper* II Network Management System (NMS) can act as the UNIX host providing transfer of the configuration database to and from a node.
- ***Data collection/reporting scheduling*** — The performance measurements subsystem collects, stores, and formats measurements data, which can be scheduled for generation on a daily, weekly, or monthly basis.
- ***Billing*** — The billing subsystem collects, stores, formats, and outputs billing data generated by the nodes. Reports can be generated daily, weekly, or monthly for all services.
- ***Archiving*** — The logs and databases collected by *StarKeeper* II NMS can be archived. Reports can be generated and output from the archived data at any time.
- ***On-line help*** — *StarKeeper* II NMS has help facilities that provide the operator with on-line documentation for the following:
  - all system alarms and error messages, including recommended actions to take

  - all commands, including help for specific BNS-2000 or *StarKeeper* II NMS commands (in both a full-screen display and a convenient one-line format)

- ***INFORMIX support*** — *StarKeeper* II NMS databases use the INFORMIX Database Management System, which provides data storage and data manipulation facilities.
- ***A programmer's interface*** — *StarKeeper* II NMS has a user-programmable interface for incorporating UNIX shells or C programs. This interface permits further automation and customization of network management tasks.
- ***Network Management Protocol (NMP) support*** — *StarKeeper* II NMS supports NMP, which is used to transmit messages between ACCUMASTER® and various network management systems and is a key element in AT&T Network Management Architecture.

Local Administration

The BNS-2000 administration workstation provides limited functionality local console access for node administration. The workstation consists of a logical CRT/printer combination. Messages and alarms can be directed to a printer connected to one of the two administrative console ports.

The workstation can be optionally configured to ask for an access password. Anyone attempting to log on via the workstation is given three tries to enter the password correctly. After three unsuccessful tries, an alarm is generated.

Workstations can be either located on-site or deployed remotely, as a BNS-2000 workstation located at a remote site.

Node administration is performed through a set of commands that support all administration tasks. The commands, which can be input at an administration workstation, adhere to a verb-object format. This format specifies the action to be performed and the target of the action. The commands may be entered either as command lines, with extra positional arguments following the verb-object pair, or in a prompted mode, in which the workstation operator is queried for missing or invalid parameter values. Basic administration tasks such as database configuration, node initialization, and service provisioning are performed via command input.

Output directed to the administration workstation includes reports and alarms. The output consists of alphanumeric displays composed of ASCII characters (with delimiting control characters) compatible with any ASCII terminal.

Administration reports provide support for maintenance tasks performed by the network administrator. Reports are provided on the configuration database, user profiles, automatic report output schedules, hardware status, and measurement data for specified entities. Many reports are generated automatically with administrative control over the frequency of reporting. Other reports can be manually requested and routed to the administration console.

An extension to the standard configuration database report facility permits searching the database (through pattern matching) for text-string comments associated with a variety of node entities.

Module hardware fault conditions are signaled by audible alarms and by outputs to the administration console. Each of the severity levels is characterized by its own distinctive audible

output and printed code. Audible alarms are available only for the Central Office (CO) models of BNS-2000. The audible alarms are provided through a connection to the Alarm Relay Unit (ARU) offered in the Central Office Frame.

Software-related problems are reported in printed form. Alarm output is automatic and the method used to retire alarms varies by severity level.

Security

BNS-2000 provides a variety of security methods that may be implemented independently or in unison, allowing administrators to set security measures consistent with their specific network application.

- *Network access restrictions* can be applied to every device attached to the network, requiring a network access password before granting network access.
- *Originating group security* is based on the identity of a call originator. BNS-2000 allows the network administrator to restrict access to network resources by associating an endpoint device with one or more originating groups. A call setup request succeeds or is denied based on the name of the originating group to which the device belongs. This name is matched against the destination's security pattern. The administrator can also give a user the ability to select a group identity when making a call request, and thus gain access to more than one set of restricted resources.
- *Console password security* is available for both the "A" and "B" console ports to prevent unauthorized access to the administrative console ports. The syntax of the password requires at least 6 characters, with at least 2 alphabetics and at least 1 special character. In a dual controller configuration, with a Maintenance and Redundancy Control (MRC) function arbitrating between the administrative user and the console ports, there is an additional "M" port password available.
- *Permanent virtual circuits (PVCs)* can be used to connect one compatible endpoint to another via an administrator-provisioned circuit, also known as a predefined destination (PDD). PVCs/PDDs are used in a switched environment to limit one source to a single destination. This same mechanism also provides the security and connection definition for Frame Relay services.
- *Closed user group security* enables an administrator to define groups of endpoints that restrict access to or from endpoints outside the group. It is available for endpoints placing calls to an X.25 host, packet assembler/disassembler (PAD), PSPDN, or 5ESS Switch endpoint, or for endpoints receiving calls from an X.25 PSPDN, X.25 host, or 5ESS Switch endpoint. It is implemented as a set of X.25 facilities and X.75 utilities that are based on the 1988 CCITT X.25, X.75, and X.3 Recommendations.
- *Call screening for CPM-connected hosts* allows the network administrator to prevent unauthorized host-to-host calls from a CPM-connected host.

- *Trunk call screening* ensures security management for large, shared, or interconnected networks by providing network administrators with a security method for screening incoming call setup attempts arriving over each trunk the node shares with the network. The administrator defines trunk call screening profiles containing sets of security patterns that must be matched by an incoming dialstring. Any mismatch blocks the call at the network interconnection.
- *X.25 incoming/outgoing calls barred* uses X.25 facilities to prevent an endpoint connected to an X.25 port from originating or receiving calls. Administrators can use these facilities to restrict calls into or out of X.25 endpoints. Similar facilities allow administrators to define a range of SVC logical channels on a two-way X.25 port that can only receive calls or only originate calls.
- *X.75 gateway utilities* include several that provide security mechanisms. These utilities are supported on both national and international gateways:
  - *Check of traffic agreements (CTA) for incoming calls*. Screens incoming calls based on Country Code (CC), Telephone Country Code (TCC), or Data Network Identification Code (DNIC) at an international gateway
  - *Disallowing of new calls over a gateway module*. Provides manual congestion control by allowing an X.75 gateway port to reject any new call attempts in both incoming and outgoing directions
  - *X.75 closed user group indication*
  - *X.75 closed user group with outgoing access*
- *The Network Access Control System* can be used with BNS-2000 to provide a security mechanism that complements security features of the system software. The system provides effective network access control for dial-in modem users, and also offers the convenience of centralized security administration.
- *Various vertical services* are provided through software applications running on the DKAP module. Calls can be routed to the DKAP-resident application for user authentication before splicing the call to the destination.
- *SMDS security features* including the individual addressing, group addressing, source address validation, source address screening, and destination address screening. For more information, see Chapter 3, **Data Services and Features**.

Networking Applications

Networking Applications

The BNS-2000 product line addresses both service provider and end customer data networking applications. A common, expansive set of operational features performs equally well in all wide area network configurations. Additional options can provide diverse data services required for different network applications. Various network configurations efficiently deliver feature subsets that are carefully aimed at defined data network applications.

Wide Area Network (WAN), International, and High Reliability applications highlight BNS-2000 versatility and reliability, and show how a network can easily expand in applications where changing needs continually redefine the plan for network data services.

In a Central Office Local Area Network (CO-LAN) or an Operations Systems Network (OSN) application, BNS-2000 data services provide benefits to both the common carrier and their clients who desire the economy of integrated voice and data services.

The following list points out BNS-2000 versatility:

- Node hardware of various physical sizes is available to accommodate a network's current size and future growth.
- Concentration and distribution devices provide a variety of economical network access solutions for physically distributed locations.
- Feature packages that range from a set of basic features to a comprehensive set that combines support for multiple data services and user features provide options appropriate for a variety of network applications.
- User services that enhance basic switching and transport services, such as call hold and directory assistance, are available, as are multiple security mechanisms that provide various levels of security.
- Operations, administration, and maintenance (OA&M) capabilities are fully integrated on the node, and network management is further centralized by the *StarKeeper* II Network Management System (NMS), which extends centralized OA&M to the edge of the network.
- Networking capabilities include a variety of trunking options, including low-speed analog or Digital Data Service (DDS) private line, T1, T3, E1, E3, and fiber trunks. Networking services provide automatic alternate call routing on call setup between nodes and automatic rerouting of active calls adversely affected by trunk facility failures.

Public High-speed WAN Application

BNS-2000 is designed with the SMDS/frame relay public data network (PDN) in mind. The network provides efficient interconnections among nodes with T1/E1 or T3/E3 trunks that permit clusters of users, personal computers (PCs), workstations, and data centers to be linked over wide geographic areas. The number of nodes that can be linked together is unlimited. The low delay through a BNS-2000 switch allows many switches to be interconnected without any appreciable impact on network performance.

Node physical architecture is designed to meet CO requirements, and hardware redundancies guarantee reliability and overall availability of BNS-2000 networks. Alternate routing and default routing, plus a variety of trunking options, provide for the design of flexible, economical, reliable WANs. Trunking between BNS-2000 and *Datakit* II VCS or BNS-1000 nodes is supported, making BNS-2000 an excellent choice for a backbone network that connects existing *Datakit* II VCS networks. BNS-2000 is well-suited for deploying wide area networks. WANs typify the need for interconnect and information transfer services that LANs require beyond their own geographic boundaries. As LANs proliferate, WAN capabilities must keep pace. And as the geographic radius of the service area increases from LAN to WAN size, service demands increase as well.

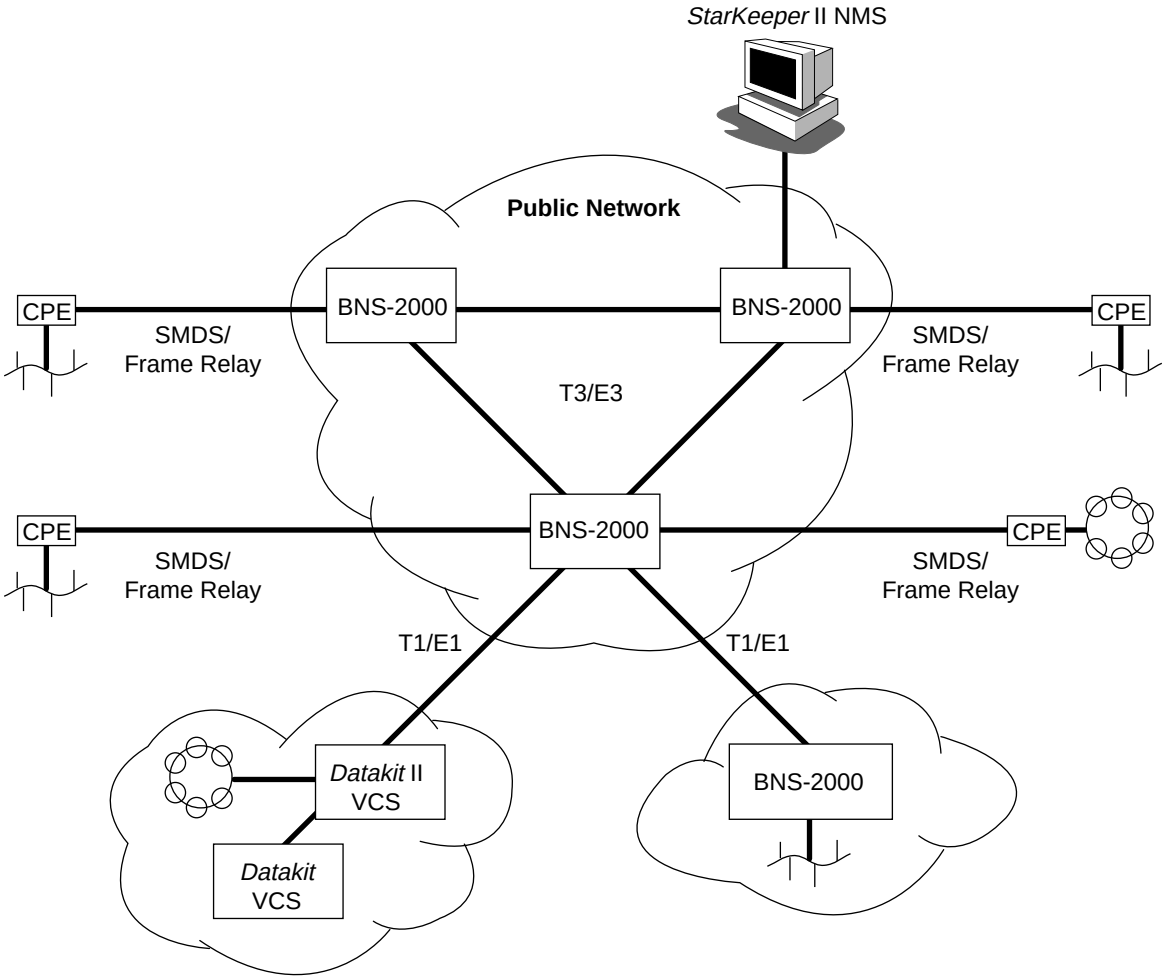

FIGURE 2-1. High-speed Public WAN

Public networks require standards-based equipment and services that are compliant with protocols developed to support the service-diverse demands made on the physically larger WANs. The IEEE developed the 802.6 extension of existing 802 standards to speed widespread introduction of standards-based equipment that allows simple interconnection.

Attributes of a BNS-2000 Network

Applications	Services	Standards	Features
High-speed Public WAN High-speed Backbone Network Private Enterprise Network	SMDS Frame Relay Multiplexed Host Interfaces Asynchronous Synchronous X.25 X.75 Connectionless Routing Connection-oriented Routing LAN Interconnect Wide Area Networking *StarKeeper* II NMS CNM/SNMP Internetworking	SMDS Cell Relay Frame Relay X.25 X.75 ISDN/B-ISDN ANSI IEEE CCITT CEPT EIA	High Capacity High Speed WAN Reliability Hardware Redundancy Modularity Automatic Fault Detection Security Customer Network Management (CNM/Simple Network Management Protocol (SNMP) Local Administration Configuration Diagnostics Customized Billing Training Customer Support/Services Documentation

Connectionless SMDS complies with IEEE 802.6 standards for network access. Together, SMDS and frame relay provide LAN-like performance and features on shared network resources.

Network management is controlled by the service provider through *StarKeeper* II NMS, which has end-to-end management capabilities, including interfaces to other operations systems used by service providers. *StarKeeper* II NMS also provides capabilities for customer network management (CNM) — which allows the end user to manage a subset of the network.

Private WAN Applications

Intelligent WANs become the common thread through which large corporations or enterprises connect their distributed processing resources. In this environment, BNS-2000 connects multiple vendor systems, providing high-speed, highly reliable networks for companies with end users who need their own WAN.

Any network application with the following characteristics can benefit from the BNS-2000 options for private WAN applications:

- large, geographically dispersed networks that need a full-service, high-speed backbone network to support distributed processing of LAN interconnect and traditional terminal-to-host applications

- a multi-vendor hardware environment with multiple operating systems or protocols, requiring support for operational interworking
- a variety of asynchronous and synchronous protocols and a need for asynchronous and synchronous connections between terminals or PCs, host computers, and peripheral devices
- a variety of host interfaces and a need for economical high-speed, multiplexed communications with hosts
- a variety of standard LAN protocols and a need for routing, bridging, and gateway services for existing IEEE 802.3, 802.5, and 802.6 segments
- X.25/X.75 connectivity with Public Data Networks and X.25 hosts.

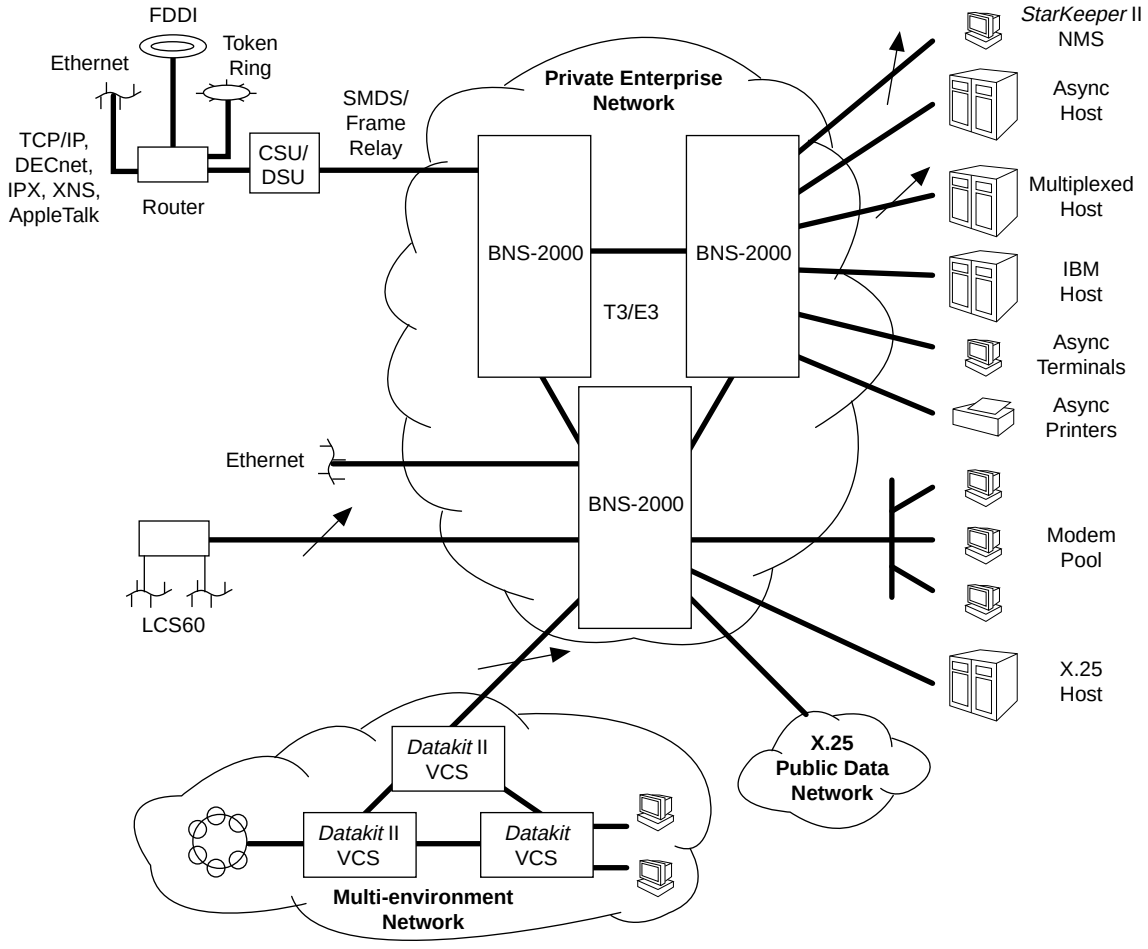

FIGURE 2-2. Private Enterprise Network

The high-speed BNS-2000 network infrastructure supports emerging LAN interconnect applications as well as traditional, embedded-base terminal-to-host applications, and gateways between the two.

Private networks that link critical applications to dispersed network endpoints need fault-tolerant network availability and routing. Complex private networks that require integrated network management and control can benefit from BNS-2000 and *StarKeeper* II NMS. Planning tools that predict network feasibility and simulate network outages are available to private network engineers and administrators. Vertical services accommodate custom-designed applications. Multiple security mechanisms and administrable security features are available. Operational features provide automatic recovery and automatic database backup.

BNS-2000 and related AT&T products can help organize the overall WAN and provide a flexible way to distribute computing resources throughout company locations, putting network access close to data communications devices.

LAN Interconnect Applications

In the past few years, there has been an explosive growth in the deployment of LAN technology. As LANs are deployed, there is a business need *not* to leave them as disconnected islands of users. Key reasons include the need for sharing of data and resources (disks, software, printers, modem pools), and for distributed processing.

The LAN Interconnect application is characterized by the following traits:

- need for higher bandwidths — from 56 Kbps to T1/E1
- LAN users grow accustomed to high LAN bandwidth and low LAN delay
- bandwidth on demand — to efficiently handle bursty LAN interconnect data
- distinction between LAN and WAN is blurring as users expect LAN-like performance across the WAN
- the need to support standard interfaces for interoperability in multi-vendor environments and to avoid obsolescence
- high availability and fault tolerance, so that mission-critical applications continue to operate even during network failure
- transparency to higher level protocols, so that one common backbone can be used for multiple applications/environments
- growing need for telecommuters with dial-in modems to access LAN resources at the office.

The BNS-2000 solution combines the important elements of the WAN application — high-speed backbone networking, multi-protocol support, fault-tolerant network availability and routing — with the inherent low delay and bandwidth-on-demand architecture of the product line to effectively address the infrastructure required by these applications. In addition, the support of the frame relay protocol as the industry standard, a direct Ethernet TCP/IP interface to the BNS-2000 (obviating the need for a separate router) and the LCS60 for support of off-site access to the LAN help to make the BNS-2000 LAN interconnect solution among the most full-featured available today.

International Applications

BNS-2000 is designed to meet applicable international safety and Electromagnetic Interference (EMI) requirements. BNS-2000 complies with IEC and VDE standards for electrical safety, EMI, and power. It operates at both 110 VAC 60 Hz or 220 VAC 50 Hz (nominal).

BNS-2000 is a worldwide product that service providers from any geographic area can use with confidence to establish OSNs and CO-LANs in their countries. A G.703 input/output (I/O) board is available for internodal trunking via the Standard Wire Trunk (SWT). Internodal trunk interfaces at E1 and E3 rates is supported. If E3 rates are required, BNS-2000 nodes must be used at each end of the trunk.

BNS-2000 is well-positioned in the world of X.25 networking. It provides support for 1988 CCITT Recommendation X.25 and provides two-way switched communications across the X.25 interface. Among the capabilities provided with this service are the following:

- full switched and permanent virtual circuit (PVC) X.25 service, including an integrated asynchronous PAD service and X.25 SVC-to-PVC connectivity
- X.121 addressing consistent with the North American Numbering Plan
- closed user group (CUG) security
- a packet assembler/disassembler (PAD) conforming to CCITT X.3, X.28, and X.29 Recommendations (1988).

BNS-2000 also offers a gateway to the 5ESS Switch using an X.25 interface. This feature can offer international customers a solution to integrated voice and data networking, providing a single backbone ISDN network that handles separate voice and data networks and multiple data protocols for both local and wide area networking.

X.75 National and International Gateway support allows BNS-2000 to serve as a public national and international network that can route calls to other PSPDNs through the X.75 Module. Each port on the X.75 Module can be configured as an international or national gateway. When connected to an international network through the X.75 Module, BNS-2000 can serve both as an originating and as a destination network.

Although the X.75 service supports the 1988 International X.121 Numbering Format, it can escape to the E.164 (ISDN) numbering plan. Calls may thus be routed to a PSPDN through an X.75 Gateway using X.121 and E.164/E.163 addressing. Calls can also be routed to or from a BNS-2000 asynchronous host or an X.25 host endpoint on an X.75 Gateway.

X.75 interfaces conform to the 1988 CCITT X.75 Recommendation.

Frame Relay provides LAN-to-LAN connectivity for international applications and is compliant with CCITT standards.

High Reliability Applications

High reliability applications can be found within the government, with service providers such as telephone companies, and with end users who need their own WAN, such as leaders in the banking industry. Generally, any network application with the following characteristics can benefit by BNS-2000 options for providing high network reliability:

- a large physical network spread out over a large geographic area
- an interest in security, including multiple security mechanisms, and administrable security features
- a vast need for networking to bring data communications to various agencies
- a multi-vendor hardware environment.

The full product line is applicable to high reliability applications. High reliability customers benefit from the following:

- redundant hardware configurations that include automatic reboot of a spare Control Computer, automatic switch recovery with a redundant switch module, and automatic backup of the network database
- the ability to set up redundant trunks throughout the network
- the ability to use spare trunk bandwidth for automatic rerouting of active calls in the event of a trunk facility failure.

Service Provider OSN Applications

BNS-2000 provides the interface modules and networking that support the Operations Systems (OSs) used by service providers to survey, administer, and maintain their voice networks and equipment. Over 100 OSs use *Datakit* II VCS/BNS-2000 networks to provide connectivity between the network elements in the Central Office, the user in the work center or maintenance center, and the OS hosts in the data center. Examples of these OSs are

- Total Network Management (TNM)
- Traffic Data Management System (TDMS)
- Switched Access Remote Test System (SARTS)
- Access Networking System (ANS)
- Network Monitoring and Analysis–Facility (NMA-F)
- Multi-Functional Operations System (MFOS)

A single BNS-2000/*Datakit* II VCS network is shared among the different OSs. The network supports both legacy OS protocols, such as E2A and BX.25, as well as emerging OS protocols, such as TCP/IP, SLIP, and PPP, at speeds from 75 baud to 10 Mbps over a variety of media, such as twisted pair, fiber, and Ethernet.

The BNS-2000 product line continues to grow in order to satisfy the service provider's needs as different interfaces evolve. BNS-2000 networks interwork with *Datakit* II VCS and *Datakit* VCS networks. Migration strategies provide for upgrading from one network to the other with almost total reuse of existing equipment, thus preserving the service provider's capital investment. Additionally, both BNS-2000 and *Datakit* II VCS nodes can be used in one network.

A BNS-2000/*Datakit* II VCS OS network satisfies these OS needs:

- reliable, error-free data transmission
- high throughput with low delay
- connectivity from any terminal to either directly-connected or LAN-based OS hosts for a variety of tasks
- high availability throughout the network, including redundant systems
- levels of security
- –48 VDC power
- support of 1988 CCITT X.25 and X.75 standards
- direct Ethernet connectivity for emerging LAN interfaces in the Central Office.

BNS-2000 can provide a highly reliable infrastructure for the OSN and permits personnel in each operations center to gain access to OSN components in any center on the network.

CO-LAN Applications

In a Central Office LAN (CO-LAN), BNS-2000 is used to provide data communications to telephone company customers over the same facilities that provide voice services. The BNS-2000 equipment is owned and operated by the telephone company and is located in a telephone company central office.

The star network topology used by BNS-2000, in which the node is the central piece of equipment through which data traffic passes to reach other devices, is well suited to this type of application. BNS-2000 provides multiple interfaces that allow diverse equipment to communicate using different data protocols, ISDN interworking, and several concentrator and multiplexer options that make remote access to the CO-LAN economical from locations that require either a few or many ports.

Data is transported over existing telephone lines to the central office, switched there in the BNS-2000, and routed to destinations on the customer's data network or to a PDN gateway. Access options to the CO-LAN include the following:

- EIA RS-232-C access using matched AT&T Voice/Data Multiplexers (VDMs), one located at the central office, the other at the customer device
- EIA RS-232-C access using matched modems, one located at the central office, the other at the customer device
- access via any of the BNS-2000 concentrators or multiplexers located on the customer premises, using standard concentrator links from 56 Kbps to T1 or E1, or up to 8 Mbps over fiber cable for limited distances.

This arrangement permits universities or multi-location businesses to establish low-speed LANs economically, without bearing the costs for switching equipment, transmission media, or installations. It also enables telephone companies to seek new markets with enhanced services.

Some characteristic needs of this application include the following:

- data services that complement existing voice services at multiple, expanding locations
- bridging services for customer LANs between COs
- cost-effective initial LAN development gained by using existing resources
- connectivity for various terminals, PCs, hosts, printers and other data processing peripherals
- customer freedom from operation, administration, and maintenance of the LAN
- software options that allow some real-time customer control over end-user services, reconfiguration, and billing
- flexible, easily implemented solutions to an evolving network topology, extensions to network capacity, or new service requirements
- –48 VDC power.

Data Services and Features

Data Services and Features

This chapter provides a comprehensive description of the main data services offered by BNS-2000. Major subsections provide details on each data service and include a list of the interface module(s) or unit(s) associated with each service.

BNS-2000 data services and features are organized into four categories:

- Data Services
- Operational Features
- Terminal User Features
- Local Administration Features

The availability of particular features and service capabilities depends on the software feature package selected. Feature packaging allows customers to select and purchase base BNS-2000 software and administer the modules necessary to support services that are appropriate for their environments. See **Software Packaging and Configuration** for details on feature packaging.

Tables show overall compatibility of the modules and list the hardware components in which modules can be placed. Complete hardware, performance, and capacity specifications for interface modules are provided in **Hardware**.

Data Services

BNS-2000 data services are organized into four categories:

- Connection-oriented (CONS) data services
- Connectionless (CLNS) data services via SMDS
- Networking services
- Component compatibility

Connection-Oriented (CONS) Data Services

BNS-2000 supports switched and autoconnect (called PDD, for predefined destination) virtual circuit data services between compatible network endpoints. Both the switched and PDD connections require call setup by the node's Control Computer. Depending on the service, calls can be made to a compatible endpoint that is either on the same node, on another BNS-2000 node in the same network, on a *Datakit* II VCS node, a BNS-1000 node, or on another network, such as an AT&T Information Systems Network, or a national or international X.25 Packet Switched Public Data Network (PSPDN). As long as the virtual circuit remains up, the two connected

endpoints can communicate. Data services include the following:

- asynchronous services
- synchronous transport services
- switched bisynchronous services
- multiplexed host access services
- X.25 services
- X.75 National and International Gateway Services to X.25 PSPDNs
- LAN interconnect services
- frame relay service, including channelized T1 and E1 service
- special purpose Operations Systems (OS) services
- integrated applications processing

These services are delivered through a variety of components and related products as shown in Figure 3-1. More information about each data service follows.

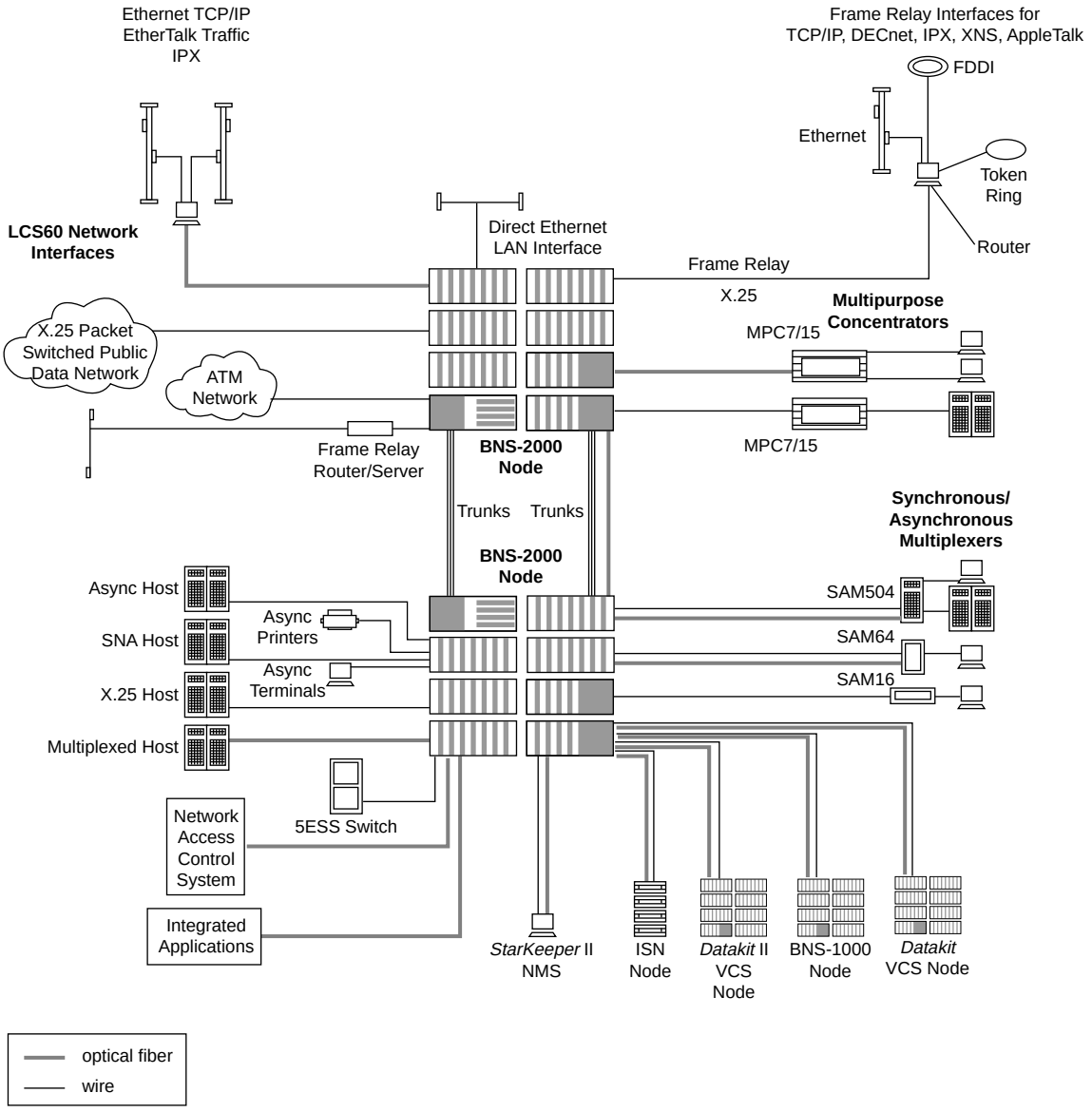

FIGURE 3-1. Connection-Oriented Network Connectivity

Asynchronous Services

BNS-2000 asynchronous service provides switched and nonswitched connectivity between terminals, printers, modems, personal computers, host computer ports, and other devices via EIA RS-232-C (or V.35 for TSM8) interfaces. With basic asynchronous service, BNS-2000 will set up an asynchronous call, either on demand or as a PDD, with other devices connected to any of the following:

- *Datakit* II VCS, *Datakit* VCS, and ISN asynchronous interfaces
- *Datakit* II VCS, *Datakit* VCS, and ISN multiplexed host interfaces, including devices on LANs connected by a multiplexed host interface to LAN Communications Systems equipment
- BNS-1000 nodes
- BNS-2000 nodes
- Definity 75/85 Communications System
- 5ESS Switch
- X.25 hosts and X.25 PSPDNs
- X.75 interface

BNS-2000 asynchronous services support speeds from 75 bps to 115.2 Kbps. Table 3-1 briefly describes the interface modules that support asynchronous services.

TABLE 3-1. Asynchronous Services Interface Modules

Module Name	Description
MSM	(Multispeed Module.) The MSM uses downloadable software, and provides 12 serial, asynchronous, full-duplex EIA RS-232-C ports for high-speed, remote access to devices on LANs, and connectivity to higher speed dial-in modem pools. Modems, terminal servers, terminal emulation packages, and workstations that support a range of speeds from 75 bps to 115.2 Kbps are supported. The MSM can be installed in a BNS-2000 node or in Multipurpose Concentrators (MPC7/MPC15).
TY12	(Terminal Module 12-port.) The TY12 provides 12 serial, asynchronous, full-duplex EIA RS-232-C ports for devices such as terminals, personal computers, hosts, printers and modems. It has the window setting capability required for interworking with Asynchronous Interface Modules (AIMs) located in ISN nodes. The TY12 can be installed in BNS-2000 nodes or Multipurpose Concentrators. It is the module of choice for asynchronous service. It supports speeds from 300 bps to 19.2 Kbps. It supports XON/XOFF and EIA flow control, or no flow control.

TABLE 3-1. Asynchronous Services Interface Modules (continued)

Module Name	Description
TY6	(Terminal Module 6-port.) The TY6 provides six serial, asynchronous, full-duplex EIA RS-232-C ports for devices such as terminals, hosts, personal computers, printers and modems. It is functionally similar to the TY12, and can be installed in both BNS-2000 nodes and Multipurpose Concentrators. It supports speeds from 75 bps to 19.2 Kbps. It supports XON/XOFF flow control, or no flow control.
CPY1 (SAM16)	The CPY1 provides eight serial, asynchronous, full-duplex EIA RS-232-C ports for devices such as terminals, hosts, personal computers, printers and modems. The CPY1 can be installed only in a SAM16. Downloadable software enables the CPY1 to support asynchronous switching service, with speeds from 75 bps to 19.2 Kbps. The CPY1 supports XON/XOFF and EIA flow control, or no flow control. For asynchronous service, settings allow flow control of the device by the SAM16, or flow control of the SAM16 by the device.
TERM32	(Terminal Interface Module 32-port.) The TERM32 provides 32 serial, asynchronous, full-duplex EIA RS-232-C ports for devices such as terminals, hosts, personal computers, printers, and modems. The TERM32 can be installed in the SAM64 and SAM504. Downloadable software enables the TERM32 to support asynchronous switching, with speeds from 75 bps to 19.2 Kbps. Window setting, required for interworking with AIMs located in ISN nodes, is supported. The TERM32 supports XON/XOFF and EIA flow control, or no flow control. For asynchronous service, settings allow flow control of the attached device by the SAM or flow control of the SAM by the attached device.
TSM8	(Transparent Synchronous Module 8-port.) Although primarily used for synchronous applications, the TSM8 can provide either eight asynchronous full-duplex EIA RS-232-C ports or one V.35 and three EIA RS-232-C ports that support connections for asynchronous devices through PDDs only. It can be installed in BNS-2000 nodes or Multipurpose Concentrators. The TSM8 supports speeds from 75 bps to 19.2 Kbps, and EIA flow control, or no flow control.

Synchronous Transport Services

BNS-2000 provides transparent synchronous data communication between hosts, front-end processors, terminals, and terminal cluster controllers. The service is provided over PDDs for compatible synchronous devices using an EIA RS-232-C or V.35 interface, for both interactive and batch-oriented communication. The protocols supported are High Level Data Link Control (HDLC), Synchronous Data Link Control (SDLC), Bisync, Digital Data Communications Message Protocol (DDCMP), Link Access Procedure Balanced (LAPB)/X.25, Burroughs Poll/Select®, Uniscope®, and Airline Line Control (ALC).

Network connections can be point-to-point or multipoint. The TSM8 module supports virtual multipoint bridging (fanout) for the HDLC, SDLC, and Bisync protocols. TSM-T1 supports virtual multipoint bridging for HDLC and SDLC. Fanout enhances transport capabilities by multiplexing physically different access lines onto a single multipoint host line. The host sees the connection as a single multipoint line.

Synchronous transport service also provides improved performance via pipelining—transmitting data as it arrives at the interface without waiting until a frame is filled.

Table 3-2 describes the modules that support synchronous transport services.

TABLE 3-2. Synchronous Transport Services Interface Modules

Module Name	Description
TSM8	(Transparent Synchronous Module 8-port.) The TSM8 provides either eight full-duplex, EIA RS-232-C ports or one V.35 and three EIA RS-232-C ports for synchronous communication using PDDs only. It supports the following synchronous protocols: SDLC, HDLC, DDCMP, Bisync, LAPB/X.25, Burroughs Poll/Select, and Uniscope. It serves as a transport mechanism for these protocols, removing all extraneous fill or sync characters from the synchronous data stream. It uses downloadable software and can be used with six different I/O distribution boards that permit configuration of the module as either DTE or DCE. The module can be installed in BNS-2000 nodes or Multipurpose Concentrators. The TSM8 supports speeds from 2400 bps to 19.2 Kbps configured as DCE, and 48, 56, and 64 Kbps configured as DTE. For synchronous service, it supports pipelining of data at three speeds. For the HDLC and SDLC protocols, the pipelining speed is adaptive.
TSM-T1	(Transparent Synchronous Module-T1.) The TSM-T1 provides four V.35 DTE ports for synchronous connections to modems, DSUs, hosts, cluster controllers, and routers, at line speeds from 9600 bps to 2.048 Mbps using PDDs only. It supports SDLC and HDLC synchronous protocols. The TSM-T1 uses downloadable software. It can be installed in BNS-2000 nodes or in Multipurpose Concentrators.
CPY1 (SAM16)	The CPY1 provides eight ports for synchronous devices such as terminals and hosts. The CPY1 can be installed only in a SAM16. Downloadable software enables the CPY1 to support synchronous transport service, with speeds to 19.2 Kbps. The CPY1 supports the following synchronous protocols: ALC, SDLC, HDLC, DDCMP, Bisync, LAPB/X.25, Burroughs Poll/Select, and Uniscope. For Bisync, it supports ASCII and EBCDIC coding. For ASCII coding, it supports NRZI signaling.
TERM32	(Terminal Interface Module 32-port.) The TERM32 provides 32 serial, synchronous, full-duplex EIA RS-232-C ports. The TERM32 can be installed in the SAM64 and the SAM504. Downloadable software enables the TERM32 to support synchronous transport service, with speeds from 110 bps to 9.6 Kbps. The TERM32 supports the following synchronous protocols: ALC, SDLC, HDLC, DDCMP, Bisync, LAPB/X.25, Burroughs Poll/Select, and Uniscope. For Bisync, it supports ASCII and EBCDIC coding. For ASCII coding, NRZI signaling is supported.

Switched Bisynchronous Services

Switched bisynchronous service provides individual 3270-type terminals with switched access to 3270-type hosts when both are connected to the network. Access to a compatible host is selectable from an individual terminal independent of other terminals on the same control unit or the same line. Terminals connect via already deployed control units through communication lines to the BNS-2000 interface.

Table 3-3 describes the module that supports switched bisynchronous services.

TABLE 3-3. Switched Bisynchronous Services Interface Module

Module Name	Description
SYNC8	(Synchronous Module 8-port.) The SYNC8 (referred to as bsc3270 in software) provides eight ports for terminals or hosts supporting switched bisynchronous service using the Binary Synchronous Communications (BSC) protocol. The module contains a board that accepts software downloaded from the BNS-2000 Control Computer and one of four different I/O boards that permit configuration as DTE or DCE. When configured to support terminal lines, the SYNC8 module supports eight ports at 19.2 Kbps. When configured to support host lines, the SYNC8 supports a single port at up to 56 Kbps using V.35 or eight ports at 19.2 Kbps using EIA RS-232-C. It cannot be used simultaneously for host and terminal service. The SYNC8 can be installed in BNS-2000 nodes or Multipurpose Concentrators.

Multiplexed Host Access Services

In addition to RS-232-C asynchronous interface connections for host computers, BNS-2000 provides interfaces that support high-speed multiplexed connections over fiber optic links to various computer systems.

BNS-2000 works with all supported versions of CommKit Software to connect multiplexed hosts to the node. When compared to RS-232-C connections, a multiplexed interface can significantly reduce the cost of host connectivity while improving performance. It allows the user to take advantage of additional UNIX system capabilities such as remote login, remote execution, remote file sharing, remote print, and file transfer.

Splice Feature

The splice feature allows the network to reroute a call to an intermediate destination (a multiplexed host), establish a separate virtual circuit from the intermediate to the final destination, and combine the two calls by removing the intermediate host. For example, the intermediate host might act as a security server for the destination host. Once a caller passes the security check, the intermediate host calls the destination and drops out of the spliced circuit.

AT&T CommKit Software Vendor Program

AT&T Network Systems licenses CommKit Software to major hardware suppliers. CommKit Software is available for equipment from Amdahl®, Hewlett-Packard (HP), Pyramid™, Stratus®, Sun®, Tandem®, and others. Contact your vendor account manager or CommKit Software Product Management for information.

TABLE 3-4. Multiplexed Host Access Services Interface Modules

Module Name	Description
CPM-HS	(Computer Port Module–High Speed.) The CPM-HS provides a high-speed bit-serial connection for a fiber optic link to select AT&T host computers and workstations. AT&T CommKit Host Interface Software is required. AT&T Fiber Interfaces are required for the host connections. The CPM-HS can be installed in nodes and Multipurpose Concentrators.

X.25 Services

BNS-2000 provides transport of X.25 data traffic. Support for the X.25 protocol is based on the 1988 CCITT X.25 specifications. All mandatory and many optional facilities are supported. An integral asynchronous PAD capability is available, which is based on CCITT 1988 X.3, X.28, and X.29 PAD standards. X.121 addressing is supported for the North American Numbering Plan (NANP) with several extensions for support of international addressing. Closed user group (CUG) security, as well as BNS-2000 security, is supported. Both switched virtual circuits (SVCs) and permanent virtual circuits (PVCs) are supported for all services.

The X.25 capability provides X.25–to–X.25 switched service which allows X.25 hosts/endpoints to communicate with other X.25 hosts/endpoints on the network. The integrated asynchronous PAD service provides connectivity between asynchronous endpoints and X.25 hosts/endpoints on the network.

BNS-2000 networks interface with X.25 networks via the X.75 module, using the CCITT X.75 standard, as described under X.75 Gateway Services. This allows either asynchronous users or X.25 hosts/endpoints on the BNS-2000 network to communicate with X.25 hosts/endpoints on an X.25 network.

NOTE: The X.25 network can be a 5ESS or 4ESS running ISDN. BNS-2000 cannot, however, act as a tandem network between two other packet networks, such as ACCUNET® and Pinet.

The BNS-2000 X.25 capability has been tested for interoperability with the 5ESS Switch, and many other vendors' X.25 equipment/capabilities. These include Siemens and Telematics for customers such as EasyLink and Brazil's Telepar network. In addition, the X.25 service has been tested for interoperability with some international networks, such as the Deutsche Bundespost and Spain's IBERPAC network. The Public Data Network (PDN) interface has been certified with

ACCUNET, Telenet®, and Sprintnet®.

The X.25 service is supported by two modules that have different operating characteristics:

- X.25 module — This module supports up to 100 X.25 SVCs and PVCs per module. All 1988 CCITT mandatory facilities and some optional facilities are supported. Packet sizes of 128 and 256 bytes with level 3 window sizes of 1-7 are supported. This module supports an integrated asynchronous PAD service as well as switched X.25 service. The X.25 module has four ports: four RS-232 ports or one V.35 DTE port and three RS-232 ports. Speeds supported are 1200 bps to 64 Kbps. Total throughput of the module is approximately 80 Kbps.
- X.25P module — This module supports up to 507 SVCs/PVCs at packet sizes of 128, 256, 512, and 1024 bytes and Level 3 window sizes of 1 to 7. Both integrated asynchronous PAD service and full X.25 switched services are supported. The X.25P module has a throughput of approximately 4 Mbps, and can be configured either with four V.35 DTE ports or eight RS-232 ports. Packet and window sizes as well as speed are configurable by port. Supported speeds are 1200 bps to 64 Kbps, with higher speeds possible up to T1/E1. In addition to supporting all of the mandatory 1988 CCITT capabilities, this module supports additional optional facilities, including packet segmentation, X.25 hunt group address substitution, and X.25 SVC-to-PVC connectivity.

NOTE: Both the X.25 and X.25P modules can interwork with X.25 endpoints connected to BNS-2000 Synchronous/Asynchronous Multiplexers (SAMs) via a DKAP application.

TABLE 3-5. X.25 Services Interface Modules

Module Name	Description
X.25	The X.25 module provides four ports. Each port can be individually configured to permit a variety of I/O distribution options. Four ports can be configured at 9.6 or 19.2 Kbps or one port can be configured at up to 64 Kbps and three ports configured at up to 9.6 Kbps. An integral PAD converts the ASCII data stream to X.25 packets and vice versa. The module accepts downloadable software. It can be installed in a BNS-2000 node or Multipurpose Concentrator.
X.25P	The X.25P module provides four V.35 DTE ports at speeds up to 64 Kbps, or eight DCE or DTE ports at speeds up to 19.2 Kbps. In addition, 1 or 2 V.35 DTE ports are supported at speeds from 64 Kbps to E1 rate (see the *Data Networking Products Planning Guide* for more information). PAD service is supported for asynchronous calls. The X.25P is a downloadable module, and can be installed in a BNS-2000 node or in a Multipurpose Concentrator (MPC7/MPC15).

X.75 Gateway Services

The X.75 gateway service extends the existing X.25 service on BNS-2000 networks by providing a gateway between BNS-2000 and X.25 networks in public networking environments. The X.75 Gateway allows BNS-2000 to serve as a public national and international network that can route calls to other Packet Switched Public Data Networks (PSPDNs) through the X.75 Module. The X.75 interface supports the 1988 CCITT X.75 Recommendation. An X.75 national gateway provides an interface to another network that serves the same country (that has the same Data Country Code or Telephone Country Code). An X.75 international gateway provides an interface to another network in a different country that has a different DCC or TCC.

The X.75 module supports four V.35 I/O ports with DTE interfaces that can connect to other interfaces, such as G.703, through an external modem or converter. The V.35 board supports one T1/E1 port and up to four 64 Kbps ports. The X.75 module provides throughput of 300 128-byte packets per second to the T1/E1 port and about 50 packets per second to each of the four 64 Kbps ports. The module supports 512 channels, 507 of which are available for data transfer. The maximum number of switched and permanent virtual circuits per module and data line is thus 507. Each port on the X.75 module can be configured as an international or national gateway. The maximum number of international gateways in the BNS-2000 network is 256.

X.75 supports the 1988 International X.121 Numbering Plan. The E.164 Numbering Plan (the Numbering Plan for the ISDN) can be selected for use in place of the X.121 Numbering Plan by using escape codes. Calls can thus be routed to a PSPDN through an X.75 gateway using X.121 and E.164/E.163 addressing. Using X.75, calls can also be routed to or from an asynchronous (TY12, CPM, SAM) host or an X.25 host endpoint on an X.75 Gateway.

The X.75 module provides an integrated PAD service for virtual calls and PVCs that connect to asynchronous devices (TYs, MSMs, SAMs, and CPMs), including the LCS60. PAD service is the same as that provided by the X.25 services, which support 100 PAD calls with a maximum packet size of 256 bytes and a maximum window size of 7. The X.75 integrated asnychronous PAD service is based on CCITT 1988 X.3, X.28, and X.29 Recommendations.

Table 3-6 describes the module that supports BNS-2000 X.75 Gateway Services.

TABLE 3-6. X.75 Gateway Services Interface Module

Module Name	Description
X.75	The X.75 Module provides up to four V.35 I/O ports. A single port can be configured at up to T1/E1 rates. The four ports can be configured at up to 64 Kbps. The X.75 module also supports an integrated PAD service for asynchronous calls. It accepts downloadable software, and can be installed in a BNS-2000 node or Multipurpose Concentrator.

LAN Interconnect Services

BNS-2000 technology and product line components provide a variety of services for wide area networking of multiple geographically dispersed local area networks (LANs). LANs can be interconnected using BNS-2000 as a frame relay network with either commercial routers or bridges or with direct Ethernet LAN interface for Transmission Control Protocol/Internet Protocol (TCP/IP) hosts. LANs can also be interconnected via high performance LAN bridge/router equipment, using BNS-2000 to network many geographically disparate LAN segments into one large LAN.

BNS-2000 LAN interconnect services provide

- high speed frame relay interfaces for LANs that allow access and routing across the network for geographically dispersed LANs
- direct Ethernet LAN interfaces for TCP/IP hosts for access to other directly connected LANs or hosts on frame relay networks
- local routing and quick, efficient switching for inter-LAN traffic
- vertical services that include security features, and centralized operation, administration, and maintenance by *StarKeeper* II NMS

The LAN Communications Systems (LCS) product line includes equipment that provides unique functionality as network interfaces, gateways, and routers.

BNS-2000 provides Open Network Interfaces (ONIs) to a variety of AT&T and commercial vendor LAN gateway and LAN bridge/router products, allowing users to implement LAN interconnect services as their need for services grows. Open Network Interface support provides a transport network that integrates LAN interconnect traffic with traditional terminal-to-host non-LAN traffic, optimizing use of bandwidth and switching resources. As a user's networking applications evolve towards additional needs for LAN interconnect services, users can migrate LAN segments onto the BNS-2000 technology platform with a minimum of effort and expense.

In addition, a variety of high-speed bridge/routers, including the LCS product line and equipment from other vendors, are supported as follows:

- HDLC point-to-point connectivity over the TSM8 and TSM-T1 modules at speeds up to T1
- X.25 networked connectivity over the X.25 module at speeds up to 64 Kbps
- Frame relay networked connectivity over the FRM at speeds up to 2.048 Mbps

Frame Relay Services. Frame relay is a frame-based high-speed interface specification that provides dynamic bandwidth allocation with high throughput and low delay to support the increasing amount of bursty traffic in the corporate environment, particularly that traffic associated with LAN interconnect. The frame relay protocol defines a standard format for Data Link Layer frames, which are transmitted over the BNS-2000 network.

Frame relay comprises a two-layer protocol stack. Frame relay interfaces rely on the existing intelligence of end-user equipment, such as routers, and today's higher quality digital transmission facilities. Frame relay can be thought of as a streamlined version of X.25.

Streamlining is accomplished by stripping away all of the X.25 network layer (Layer 3), adding a statistical multiplexing capability via individually addressed frames at the Data Link Layer, and reducing the required processing at Layer 2 by removing error correction and retransmission capabilities. Frames are passed across the BNS-2000 network using PVCs, with minimal processing by the network nodes.

The BNS-2000 frame relay service supports user access through high-speed interfaces which provide users with efficient LAN interconnections over wide areas with a single physical link. The BNS-2000 frame relay interface operates with commercial bridges and routers from any vendor that supports the frame relay protocol. The frame relay reduced network transit time for data exchange, reduced facility expense, and reduced network complexity are important advantages in BNS-2000 networks.

BNS-2000 supports both the Frame Relay User-to-Network Interface (UNI) as well Network-to-Network Interface (NNI). The UNI is an agreement on how frame relay users communicate with and through a frame relay network. UNI access through a high-speed interface provides users with efficient LAN interconnections over wide areas via a single physical link. The NNI is an agreement on how frame relay networks talk to each other. The agreement provides support for the optional bi-directional PVC management procedures defined in ANSI. With normal PVC management, the end system polls the network for status, and the network responds. Bi-directionality allows the network to initiate the polling. With this agreement, PVC status (and link integrity) information can be passed from network to network, and thus have end-to-end meaning. Bi-directionality will be supported for ANSI, CCITT, or LMI PVC management.

BNS-2000 supports frame relay services which are compliant with existing ANSI, ITU-T, and Frame Relay Forum standards. The BNS-2000 frame relay interface supports three PVC management procedures that comply with ANSI T1.617 Annex D, CCITT Q.933 Annex A, and the local management interface (LMI). The procedures provide the means for notification of a new PVC or the outage and subsequent recovery of existing PVCs. Congestion detection monitors internal resource use for each frame relay data link connection identifier (DLCI), and notifies the access device of pending congestion by setting the forward explicit congestion notification (FECN) and backward explicit congestion notification (BECN) fields in the frame header.

Committed Information Rate (CIR) enables network providers to define a certain level of service that can be subscribed to by end users. Minimally, the CIR is a level of throughput which the network agrees to provide (per PVC) when there is no congestion. A network provider can go beyond that, however, and offer a guaranteed CIR even during times of congestion. Alternately, the service provider can offer a statistical guarantee of CIR (say 95%). It is important to understand that CIR should be considered a *minimum* level of service. Users should be able to burst beyond their CIR if the network is not busy.

Excess Burst (Be) allows network providers to place a *maximum* limit on the amount of data that a user may transmit into the network. Data received beyond this limit is discarded on ingress. For maximum flexibility, Be would be equivalent to the full port speed. In other words, data received up to the CIR will be delivered. Data received beyond the CIR may be discarded if the network is congested. Data beyond the excess burst will be discarded.

The BNS-2000 implementation of CIR supports setting the CIR and Be parameters on a PVC

basis. The CIR can be set at any arbitrary level between zero and the port speed. The excess burst level can be set anywhere between the CIR level and the maximum port speed.

The multicast feature enables an attached access device to transmit a single message to the frame relay network interface for delivery to multiple destination endpoints over a multicast DLCI.

The Frame Relay service is supported by two modules: the FRM and the FRM-M2. Both the FRM and the FRM-M2 are compliant with all current Frame Relay standards and provide frame relay service as described above.

- *FRM Module*—This module supports up to four V.35 connections or a single channelized T1 or E1 connection. Each V.35 connection supports connections ranging in speed from 9600 bps to 2.048 Mbps, subject to the aggregate module throughput of 4 Mbps (2.048 Mbps in each direction). The channelized T1 connection supports up to 24 independent frame relay interfaces (also called virtual ports): one for each of the 24 DS0 time slots present in a T1 signal. Each virtual port may be a single DS0 signal or any combination of $n \times$ DS0 up to $n = 24$. The channelized E1 connection supports up to 31 independent frame relay interfaces (also called virtual ports): one for each of the 31 DS0 time slots present in a E1 signal. Each virtual port may be a single DS0 signal or any combination of $n \times$ DS0 up to $n = 31$. For both the channelized T1 and E1 connection, the assignment of DS0 time slots to virtual ports is done administratively. Either contiguous or non-contiguous time slots can be assigned to a virtual port.

  The FRM is a single-board downloadable module. Each FRM supports up to 507 user channels (DLCIs). The FRM can be located in a BNS-2000 node on a Series M1 Shelf or in a Multipurpose Concentrator.

- *FRM-M2 Module*—This module supports up to six channelized T1/E1 connections. The channelized T1 connection supports up to 24 independent frame relay interfaces (also called virtual ports): one for each of the 24 DS0 time slots present in a T1 signal. Each virtual port may be a single DS0 signal or any combination of $n \times$ DS0 up to $n = 24$. The channelized E1 connection supports up to 31 independent frame relay interfaces (also called virtual ports): one for each of the 31 DS0 time slots present in a E1 signal. Each virtual port may be a single DS0 signal or any combination of $n \times$ DS0 up to $n = 31$. For both the channelized T1 and E1 connection, the assignment of DS0 time slots to virtual ports is done administratively. Either contiguous or non-contiguous time slots can be assigned to a virtual port.

  The FRM-M2 is a single-board downloadable module that supports up to 2000 user channels (DLCIs). The FRM-M2 supports 2, 3, and 4 octet addressing. The FRM-M2 can only be located in a BNS-2000 node on a Series M2 shelf.

Ethernet LAN Interfaces. Direct Ethernet LAN interfaces are supported on the LAN Protocol Module (LPM). LAN-connected hosts are able to communicate with other network elements using industry standard TCP/IP and Ethernet cabling without requiring additional routing or DSU equipment. These hosts can also communicate with any frame relay endpoints provided by a variety of customer-based access devices which provide seamless logical connections with other frame relay endpoints anywhere in the network.

Both Ethernet and 802.3 Media Access Control (MAC) layers and associated encapsulation are supported. IP data packets are routed between local area networks (LANs), equipment connected

to FRM ports, and ports on other LPMs. For routing purposes, these ports are addressable as LAN ports or as frame relay ports for frame relay via PVCs which terminate on a given LPM. A unique Ethernet address is assigned to each physical LAN port.

IP data that arrives at the LPM is encapsulated with the proper protocol and routed (according to the IP header address) to other IP addressable endpoints, which reside either across the frame relay network or across LAN ports to network elements, which are physically connected to the LAN.

A standards-based frame relay protocol is supported on the LPM for communication to frame relay endpoints. If the LPM is routing an IP datagram over a frame relay virtual port, the IP datagram is encapsulated as a frame relay frame and is transmitted over the frame relay network across a frame relay PVC. The frame format is a link access procedure for frame mode bearer services (LAPF) and consists of an opening flag, an address field containing a DLCI, an information field, a check sequence at the end, and a closing flag. The frames are broken into packets for high-speed transport across the network to another frame relay endpoint. Once an IP datagram has been encapsulated as a frame relay frame and a DLCI has been identified for its transmission, the LPM performs the same routing functionality as a FRM. See Frame Relay Services for a description of the frame relay protocol.

The LAN services include PVC management, congestion detection, CIR, provisioned IP routing, fault-tolerant routing, IP routing security, and diagnostic capabilities.

Address Resolution Protocol (ARP) is supported for each physical LAN port. Inverse ARP is supported for each logical port. DLCI throughput (data window) tuning parameters and CIR can be configured for PVC originating or receiving traffic on the LPM. The LPM monitors internal resource (buffer) use for each DLCI and notifies the access device of pending congestion conditions by setting the FECN and/or BECN fields in the frame header. These bits remain set until the access device modifies its traffic pattern to reduce congestion.

The LPM also supports a CIR for each DLCI. CIR allows a bandwidth allocation to be assigned to each PVC on an LPM port. The maximum aggregate CIR supported by an LPM port is a configurable option but can be up to four times the capacity of the virtual frame relay ports of the LPM.

Each physical LPM port can support data traffic at speeds up to 1.544 Mbps per port in full duplex mode (simultaneous traffic in both directions) with each IP packet experiencing low transmission delay. The LPM supports up to 500 PVCs to other LPMs and frame relay ports. The virtual circuit endpoints are organized as up to 27 LPM virtual frame relay ports, each of which consist of one or more virtual circuit endpoints.

IP routes through the LPM are administered statically, which gives the network administrator complete control over routing paths. Fault-tolerant routing is available at both the frame relay PVC (DLCI) and physical port level. Multiple routes are configured to the same destination so that if the next hop to a destination is another LPM or device connected to a frame relay port and the virtual circuit fails, the LPM will choose an alternate route to the destination. Preferred routing is configurable based on the routing path speed, number of hops, or other criteria.

From the BNS-2000 console, a broadcast ping is available which allows the administrator to determine which hosts on any of the interconnected IP networks are available. It also allows the

administrator to determine which of the interconnected LPM modules are active.

Security for the LPM is integrated in existing node security which provides more control than would be possible at the IP level. All information used by the security filters is under the exclusive control of the network administrator. The physical ports (*lanports*) and virtual ports (*frports*) from which data can be received on the LPM are screened to prevent unauthorized transmission of data.

The LPM does not support the standard IP features of IP Broadcast and Multicast. This ensures that IP traffic routed by the LPM stays within the private network.

LCS Products. The LAN Communications Systems (LCS) product line can be used to implement LAN interconnect services on BNS-2000 networks. The product line consists of the LCS60 Network Interface.

Details on this product are in the chapter on **Related Products**.

Table 3-7 describes the BNS-2000 modules that support LAN interconnect services.

TABLE 3-7. LAN Interconnect Services Interface Modules

Module Name	Description
FRM	(Frame Relay Module.) The FRM is a single-board downloadable module that supports up to four V.35 connections or a single channelized T1/E1 connection. Each V.35 connection supports connections ranging in speed from 9600 bps to 2.048 Mbps, subject to the aggregate module throughput of 4 Mbps (2.048 Mbps in each direction). The channelized T1 connection supports up to 24 independent frame relay interfaces (also called virtual ports): one for each of the 24 time slots present in a T1 signal. Each TI time slot can be configured to operate at either 56 Kbps or 64 Kbps. The channelized E1 connection supports up to 31 independent frame relay interfaces or virtual ports: one for each of the 31 time slots present in an E1 signal. Each E1 time slot operates at 64 Kbps. Time slots on either an individual channelized T1 or E1 connection can be grouped to form higher speed frame relay interfaces or virtual ports. Each FRM supports up to 507 user channels (DLCIs). The FRM can be located in a BNS-2000 node or a Multipurpose Concentrator.
FRM-M2	(M2 Frame Relay Module.) The FRM-M2 is a single-board downloadable module that supports up to six channelized T1/E1 connections. Each channelized T1 connection supports up to 24 independent frame relay interfaces (also called virtual ports): one for each of the 24 time slots present in a T1 signal. Each TI time slot can be configured to operate at either 56 Kbps or 64 Kbps. Each channelized E1 connection supports up to 31 independent frame relay interfaces or virtual ports: one for each of the 31 time slots present in an E1 signal. Each E1 time slot operates at 64 Kbps. Time slots on either an individual channelized T1 or E1 connection can be grouped to form higher speed frame relay interfaces or virtual ports. Each FRM-M2 supports up to 2000 user channels (DLCIs). The FRM-M2 can only be located in a BNS-2000 node on a Series M2 Shelf.
LPM	(LAN Protocol Module.) The LPM provides IP router functionality over frame relay via two 802.3 10Base-T ports. The LPM routes IP packets to and from these ports, equipment connected to frame relay ports, and ports on other LPMs. The LPM supports up to 27 independent virtual frame relay ports with up to 507 virtual circuits. The LPM software is downloadable. The module can be located in a BNS-2000 node or a Multipurpose Concentrator (MPC7/MPC15).

Special Purpose Services

Special purpose services provide interfaces that support the service provider Operations Systems (OSs). See Table 3-8.

TABLE 3-8. Special Purpose Services Interface Modules

Module Name	Description
E2A	The E2A module has four telemetry ports, each operating asynchronously at 1200 bps. The E2A module provides data connectivity between Operations System hosts and their analog switches, and is not available for other applications. It can be installed in a BNS-2000 node or MPC15.
SLM	(Synchronous Line Module.) The SLM provides data connectivity between OS and digital switches or electronic equipment that supports the BX.25 Issue 2 protocol. It provides four ports at speeds of 2400 bps or 9600 bps. The module contains two boards that must occupy two adjacent slots: an SC/DKI interface board and a processor board. Software is downloadable from an OS host. The SLM is customized to meet the needs of certain OS applications and is not available for other applications. It can be installed in a BNS-2000 node or MPC15.

Customer Programmable Services

BNS-2000 provides a general-purpose processing environment for the creation of customer-specific applications such as call splicing, protocol conversion, and authentication. The platform for providing such applications is the DKAP. AT&T offers a service for developing customer-specific DKAP applications.

Table 3-9 describes the module that supports vertical services on a BNS-2000.

TABLE 3-9. Customer Programmable Services Application Module

Module Name	Description
DKAP	The DKAP module is a module that plugs into the node with access to the backplane. It includes a processor, 64 KB ROM, and 2 MB RAM. It accepts downloadable software. Applications on the DKAP look to the network like any other host-resident applications, and can originate calls to, and receive calls from, any other application or device on the network.

Connectionless (CLNS) Data Services via SMDS

SMDS is a connectionless, packet-switched service that provides subscriber LANs with high-speed interconnect capabilities throughout the broader geographic boundaries of metropolitan and wide area networks. The service is particularly well suited to interconnect LANs over a wide area because it shares the connectionless attributes of LAN routing.

In a wide area SMDS network, multiple Local Exchange Carriers (LECs), Interexchange Carriers (ICs), and multiple networks provide SMDS services to subscribers and to each other. These services include the *Exchange SMDS*, *Interexchange SMDS*, and *Exchange Access SMDS*.

A BNS-2000 network serves as an SMDS switching system for both LECs and ICs. With BNS-2000, LECs can offer Exchange SMDS and Exchange Access SMDS, and ICs can use Exchange Access SMDS and offer Interexchange SMDS. LECs can establish serving arrangements in a Local Access Transport Area (LATA) and still operate and administer their networks separately.

The service provides access interfaces at DS0, fractional T1, T1/E1, and T3/E3 transmission rates for subscriber equipment. The subscriber equipment connects to the network at the SNI. In general, the CPE can be multiprotocol routers or DSUs that support T1 or T3 SMDS interfaces. This equipment connects to the SMDS Switching System, operated by the SMDS service provider, through an SMDS access distributed queue dual bus (DQDB) attached to an AI module. For SMDS, BNS-2000 supports AI-T1, AI-T3, and AI-T3P modules, plus AI-E1 and AI-E3 modules for international applications for SMDS access.

The SMDS definition provides two configurations for the access DQDB:

- single-CPE access that supports a single router or other equipment connected to the DQDB
- multiple-CPE access that supports two or more routers or other equipment sharing the same DQDB.

Most existing SMDS subscriber equipment supports the single access configuration. BNS-2000 SMDS Switching Systems support both single- and multiple-CPE access DQDB.

Subscriber equipment attached to SMDS AIs must support the SMDS Interface Protocol (SIP). SIP defines access to the network for both T1/E1 and T3/E3 interfaces for the electrical and physical level (SIP Level 1), and two higher protocol levels (SIP Levels 2 and 3).

BNS-2000 SMDS complies with the following Bellcore requirements:

- TR-TSV-000772
- TR-TSV-000773
- TR-TSV-000774
- TR-TSV-000775
- TA-TSY-000378
- TR-TSV-001060
- TR-TSV-001063.

Complete details on this service are available in the *BNS-2000 SMDS Guide*.

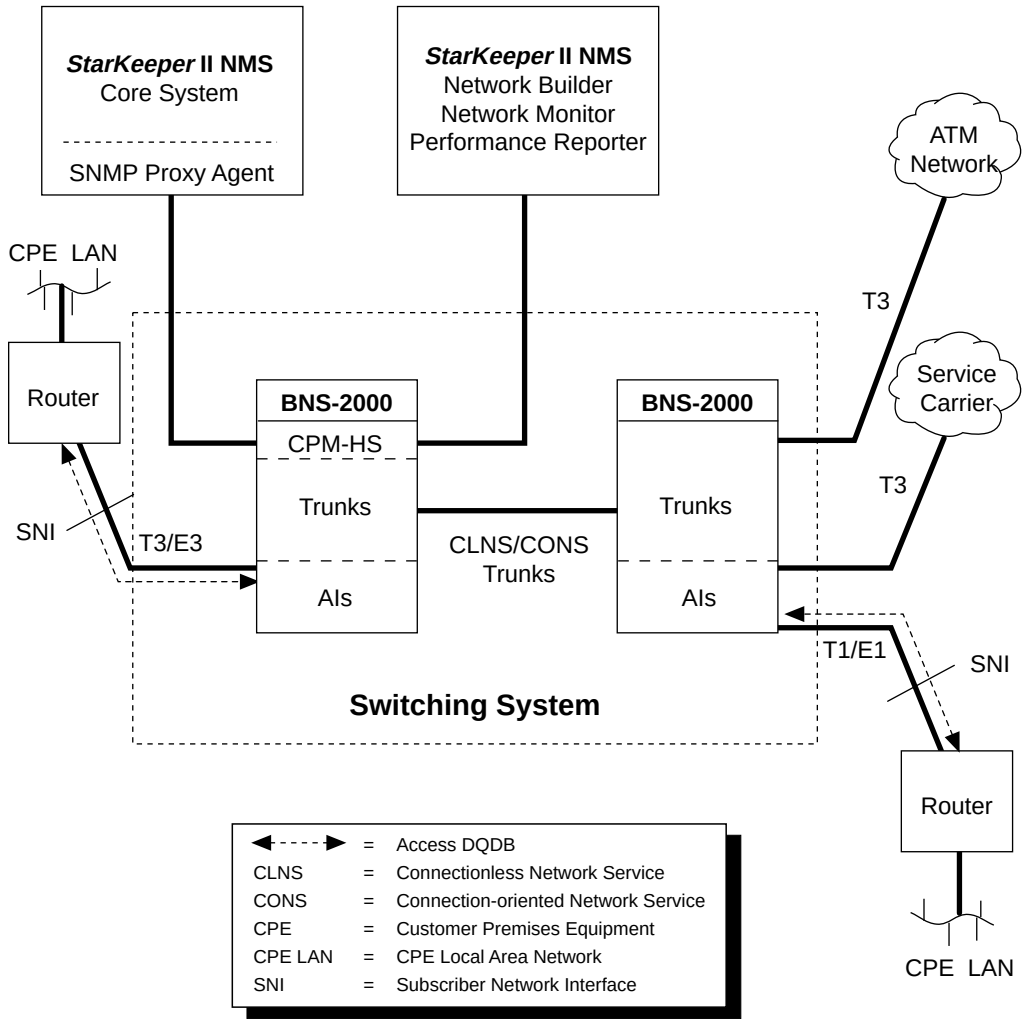

FIGURE 3-2. BNS-2000 Connectionless Network Connectivity

Features

SMDS features include nationwide SMDS, intercompany SMDS arrangements, the Intercarrier Interface (ICI), and separate routing for official traffic.

Nationwide SMDS. In a nationwide SMDS network, carriers provide services to SMDS subscribers and to each other. These services are described below:

- ***Exchange SMDS*** is the transport of data units between SMDS subscribers located in the same exchange serving area. In general, Local Access Transport Areas (LATAs) define exchange serving areas. Local Exchange Carriers (LECs) provide Exchange SMDS to subscribers they serve directly. Government regulations generally prohibit LECs from transporting their subscriber's data across LATA boundaries.
- ***Interexchange SMDS*** is the transport of data units between SMDS subscribers located in different LATAs. Interexchange Carriers (ICs) provide Interexchange SMDS to subscribers served by LECs and to subscribers they serve directly.
- ***Exchange Access SMDS (XA-SMDS)*** is the means by which a LEC provides its subscribers access to Interexchange SMDS and to subscribers served directly by ICs. A LEC provides XA-SMDS to an IC. It gives the IC access to all subscribers that are served by the LEC. For originating XA-SMDS, the LEC delivers a subscriber's data unit to the IC of the subscriber's choice. For terminating XA-SMDS, the LEC delivers data units arriving from an IC to subscribers the LEC serves directly.

A BNS-2000 network can serve as an SMDS switching system for both LECs and ICs. BNS-2000 enables LECs to offer Exchange SMDS and XA-SMDS, and allows ICs to use XA-SMDS and to offer Interexchange SMDS.

Intercompany Serving Arrangements. There may be several LECs in a LATA, each offering SMDS to a portion of the LATA. To provide Exchange SMDS to subscribers served by different LECs in the same LATA, LECs connect their networks and establish intercompany serving arrangements. With BNS-2000, LECs can establish serving arrangements in a LATA and still keep the operation and administration of their networks separate.

InterCarrier Interface. BNS-2000 supports a Bellcore-defined network-to-network interface called an InterCarrier Interface (ICI). XA-SMDS and intercompany serving arrangements are available via the ICI. Since the ICI is an open interface, BNS-2000 networks can interconnect with other vendors' SMDS networks that comply with the Bellcore requirements.

Separate Routing for Official Traffic. Many LECs are both providers and users of SMDS. When a LEC provides service to itself, the endpoints it operates are referred to as *official* endpoints, for historical reasons. LECs typically operate networks that span many LATAs and, as users of SMDS, need to transport data between official endpoints in different LATAs. While LECs are not permitted to transport their customer's data across LATA boundaries, they can carry their own official, or *private*, traffic. With BNS-2000, LECs can connect their networks in different LATAs with private interLATA trunks. Traffic that originates from an official endpoint can cross private interLATA trunks to reach endpoints served by the LEC in a different LATA. Traffic from other endpoints must use the services of an IC to reach endpoints outside the

originating LATA.

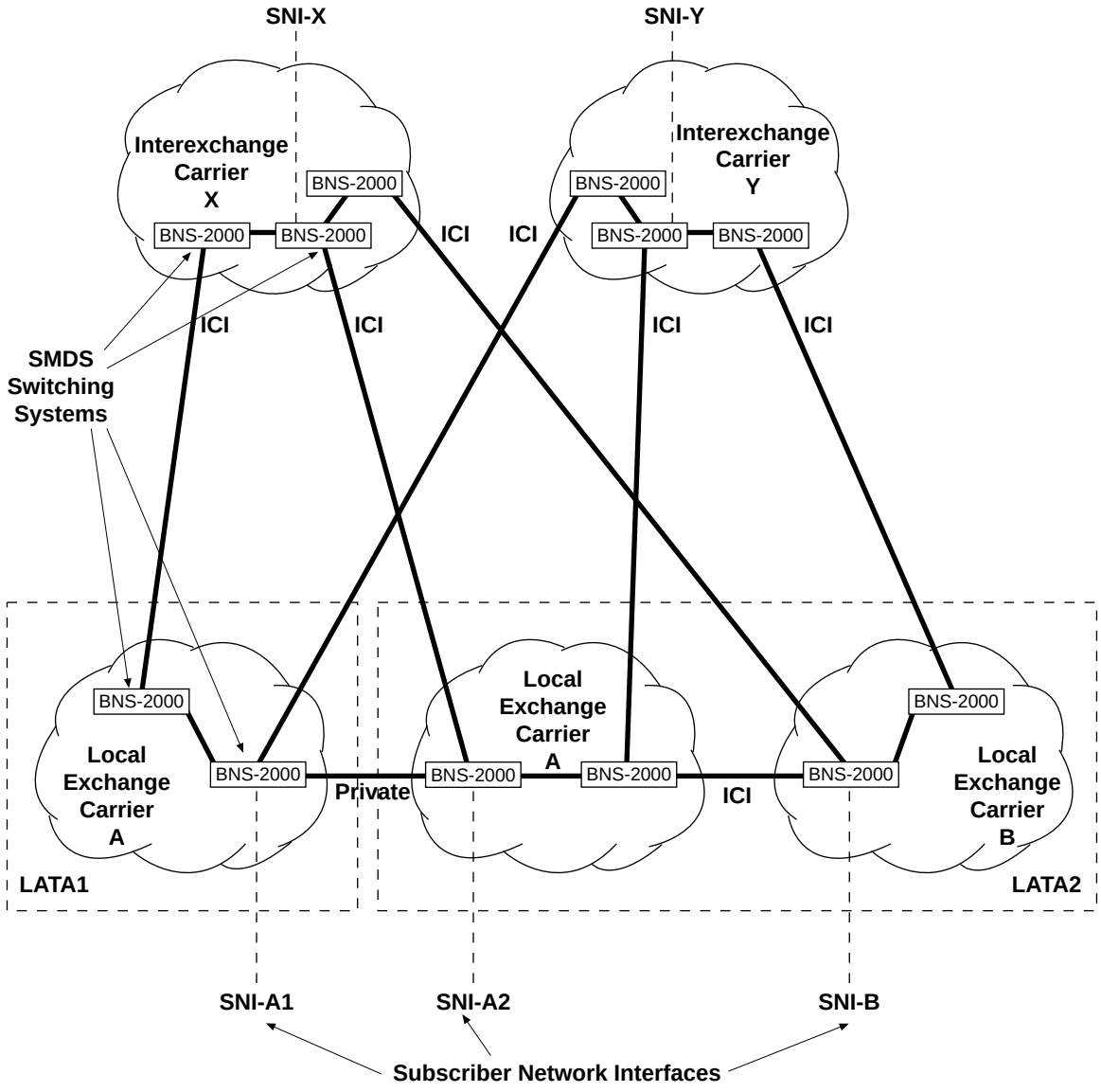

FIGURE 3-3. BNS-2000 SMDS Platform

Functional Description

BNS-2000 provides a high-speed, high-performance networking platform. BNS-2000 uses a distributed topology, so that BNS-2000 nodes can be located to optimize network access and operation. This section briefly describes BNS-2000 SMDS Switching System components. It covers the following topics:

- switching node architecture
- Access Interface (AI) modules
- trunk modules which support connectionless services
- Group Address Resolver (GAR) module
- subscriber equipment
- access class

Switching Node Architecture. A BNS-2000 node contains two types of cabinets, or shelves. See the *Node Reference* and the *Planning Guide* for specific details on BNS-2000 node architecture.

- Series M2 Shelves include the Series M2 Switch Shelf and the Series M2 Extension Shelf. All shelves share a common 200 Mbps backplane. The AIs, trunks that support connectionless service, and GAR modules all reside on Series M2 Shelves.
- Series M1 Shelves include the Series M1 Control Shelf and the Series M1 Port Shelf. Each Series M1 shelf has a separate 8 Mbps backplane. Series M1 Port Shelves are optional and provide additional slots for user interface and trunk modules, which neither carry nor interact with SMDS/CLNS traffic.

Access Interface Modules. Access Interface (AI) modules provide SMDS subscribers access to an SMDS network through one or more Subscriber Network Interfaces (SNIs). The SNI is the interface between a carrier's SMDS network and the subscriber-owned, customer premises equipment (CPE). At this interface, the CPE attaches to an access facility—such as a DS1 digital transmission facility (DTF)—that connects it via a dedicated path to an AI module in a Series M2 Shelf.

Table 3-10 lists the BNS-2000 modules that support access to an SMDS network through SNIs.

TABLE 3-10. Access Interface Modules

Module Name	Description
AI-T1	(Access Interface–T1). The Access Interface–T1 (AI-T1) module provides four DS1-rate SNIs. This module has four separate ports; each port functions independently of the others. This module does not support fractional T1 rates.
AI-E1	(Access Interface–E1). The Access Interface–E1 (AI-E1) module provides three E1-rate SNIs. This module has three separate ports; each port functions independently of the others. This module does not support fractional E1 rates.
AI-T3	(Access Interface–T3). The Access Interface–T3 (AI-T3) module provides a single DS3-rate SNI.
AI-E3	(Access Interface–E3). The Access Interface–E3 (AI-E3) module provides a single E3-rate SNI.
AI-T3P	(Access Interface–T3P). The Access Interface–T3P (AI-T3P) also provides one DS3-rate SNI. The AI-T3P is a two-board module, with one board dedicated to handling ingress traffic and one board dedicated to handling egress traffic. This allows the AI-T3P to achieve higher level of performance for full-duplex traffic (simultaneous ingress and egress traffic) than the AI-T3.

TABLE 3-11. ICI Modules

Module Name	Description
GAR	(Group Address Resolver). The GAR module interacts with the TRK-T3I module to provide group-addressed data unit transport across several carriers' networks. The GAR module enables a carrier to serve as a Group Address Agent (GAA) for group addresses that have members outside the carrier's local network. The GAR module is not needed in every network; it is only needed in SMDS networks that are serving as GAAs for group addresses that have members outside the carrier's local network. For more information on the GAR module, see the *Node Reference*, and for more information on group addressing, see the *SMDS Guide*.
TRK-T3I	(Trunk-T3I). The Trunk-T3I (TRK-T3I) module provides a T3-rate ICI and carries only connectionless traffic. The Trunk-T3I is a two-board set module, with one board dedicated to handling ingress traffic and one board, egress traffic.

Subscriber Equipment

Subscriber equipment, commonly called customer premises equipment (CPE) by service providers, connects to the network at the SNI.

In general, the subscriber equipment may be a router or bridge/router. The router and its associated DSU must implement the same SMDS interface as the AI module to which it is connected. The function of the router is to take messages from the LAN (such as a local Ethernet segment) and send them to the BNS-2000 node for delivery to a router at some other point in the network. SMDS subscriber equipment manufactured by other router vendors may also be attached to the AI modules.

Access Class

For DS3 SMDS access, five access classes are defined: access classes 1, 2, 3, 4, and 5, corresponding to the Sustained Information Rate (SIR) of 4, 10, 16, 25, and 34 Mbps, respectively. For E3 SMDS access, only access classes 1, 2, 3, and 4 are applicable.

The SMDS access class mechanism, as defined by the Bellcore standards, is intended to prescribe *limits* on the rate of sustained information transfer from the Customer Premises Equipment (CPE) to the network, and on the burstiness of the information transfer from the CPE to the network. Therefore, from a service provider's perspective, access class is defined for traffic in the ingress direction into the service provider's network. It is not applicable to egress traffic from the network to the CPE.

As defined in the standards, access class is designed to be a protection mechanism for the service provider's network. It is *not* intended to be (nor should it be used as) a guarantee of the end user's throughput. Actual end-to-end throughput for the user is dependent on a variety of factors, including the size of the user messages (i.e., size of the L3_PDUs), the specific data traffic pattern, the number of nodes and trunks in the network, and the load of the other system resources (e.g., trunks) in the network at the time.

Access class for an end user is determined at subscription time. An end user can subscribe to a particular access class based on the specific application needs.

Both the AI-T3 module and the AI-T3P module can be configured for access class 1, 2, 3, 4 or 5. As stated earlier, the actual performance of the module varies depending on, among other factors, the size of the message and the specific mix of the ingress and egress traffic data.

The AI-T3 module is a single-board module which provides DS3 SMDS access. For very large messages with only ingress traffic (for which access class is defined), the AI-T3 module can support access class 5 performance. The AI-T3P module is a high performance, 2-board set DS3 SMDS access interface module, with one board dedicated to the handling of ingress traffic and the other board dedicated to the handling of egress traffic. This allows the AI-T3P module to support access class 5 performance even when handling heavy traffic in both the ingress and egress directions simultaneously.

For maximum credits given to enforce the SIR, refer to the *SMDS Guide.*

Trunk Modules that Support Connectionless Services

Trunk modules which support connectionless services connect BNS-2000 nodes within an SMDS network; they can also connect two carriers' SMDS networks. The following sections describe trunk modules that carry SMDS traffic. See the *Trunk Module Reference* for more details.

Internodal Trunks. LECs use internodal trunks to connect BNS-2000 nodes within a LATA. ICs use internodal trunks to connect all BNS-2000 nodes in their networks, regardless of LATA boundaries. The Trunk-T3S (TRK-T3S), Trunk-E3S (TRK-E3S), Trunk-T3A (TRK-T3A), and Trunk-E3A (TRK-E3A) modules transport both connectionless and connection-oriented traffic between nodes. These trunks must be used when transporting connectionless traffic. When transporting connection-oriented traffic, these trunks provide a high-speed trunking option. For additional details on these trunks, see the **Networking Services** section.

Intercarrier Trunks. An intercarrier trunk connects a BNS-2000 network to another carrier's network. The Trunk-T3I (TRK-T3I) module provides a T3-rate ICI connection. The TRK-T3I carries only connectionless traffic. The TRK-T3I only provides a connection to another carrier's network; it cannot be used as an internodal trunk between BNS-2000 nodes or to another vendor's equipment (provided that equipment is compliant with Bellcore ICI standards) within the other carrier's network.

The Trunk-T3I is a two-board set module, with one board dedicated to handling ingress traffic and one board, egress traffic. The Trunk-T3I has three different applications:

- A LEC provides XA-SMDS to an IC. The TRK-T3I is on the LEC side of an IC-to-LEC connection.
- An IC obtains XA-SMDS from a LEC. The TRK-T3I is on the IC side of an IC-to-LEC connection.
- An intercompany serving arrangement between two LECs. The TRK-T3I is on one side of a LEC-to-LEC connection, where both LECs reside in the same LATA.

Private InterLATA Trunks. Private interLATA trunks are used by LECs to connect BNS-2000 nodes that reside in different LATAs. The Trunk-T3S (TRK-T3S) and Trunk-T3A (TRK-T3A) can be configured as a private interLATA trunk. It carries both official connectionless and connection-oriented traffic between nodes at T3 rates.

Networking Services

Any number of BNS-2000 nodes can be interconnected using a variety of trunking options. The options range from low-speed DDS (Digital Data Service) trunks operating at speeds of less than 64 Kbps to trunks operating at DS3 rates (45 Mbps). BNS-2000 nodes can be trunked together in any configuration to support the characteristics and requirements of a given network. All network communication services operate efficiently across multiple nodes.

The virtual circuit that is established at call setup time is determined automatically by the Control Computer and is constructed on a node-by-node basis. The routing of the call is based on the address of the call destination and routing tables stored at each node.

An alternate call setup routing feature permits the network administrator to define multiple routes between any two nodes as a trunk group. If a trunk has failed or is busy on call setup, the next alternate route is used, and the success of an attempted call does not depend on the availability of a single path. An outgoing call is automatically advanced to a route over a trunk group different from the incoming trunk group for the call. A call that fails because of a path failure to the destination node is cranked back to the originating node and rerouted to a secondary node for a retry. A hop count capability provides a loop detection mechanism for R2.1 and later networks. It permits administrators to set a value for the number of internodal hops that is one smaller than the number of nodes in the length of the longest path in the network. Call attempts that exceed the specified value will fail. It also provides information that may be useful to troubleshoot call failures that may occur when call setup attempts are looping over trunk channels. Calls are distributed over the trunks toward the destination using either a round-robin or sequential scheme. The network administrator specifies the preferred scheme at configuration time.

Default routing makes trunk management of large networks easy, as long as the network topology uses a hierarchical hub and leaf node design. It permits centralized address knowledge in a small set of hub nodes. The default routing feature allows leaf nodes to route calls containing unknown address information to the hub node. This allows quick node additions or deletions with less administrative activity.

Trunks connecting BNS-2000 nodes can also be administered to support session maintenance, a feature that provides fault tolerance for trunk facility failures. Active sessions on a failed trunk are rerouted around the failed facility over unused trunk bandwidth in the network. This feature is described later in this chapter.

The same options supporting trunks between nodes also support links between nodes and concentrators (except alternate routing). In some cases, the same type of module used to provide trunks between nodes can be used to provide concentrator links to the node (hence references to trunk/link modules). Concentrators provide methods of distributing BNS-2000 connections throughout a geographically dispersed network.

In LAN applications on customer premises, concentrators can extend the distribution limit of data services beyond distance limits of the SYSTIMAX® Premises Distribution System (PDS). Because of their reduced size, concentrators can fit into a customer’s office environment without special power and coding requirements.

Every BNS-2000 concentrator is networked through a link to one "home" node. They cannot be cascaded; that is, links between concentrators are not supported. Multipurpose Concentrators optionally support a cold spare trunk module that can be used to restore the link to the home node manually if the primary trunk module or the link fails.

Table 3-12 lists the modules that provide trunk and link interfaces and support networking services on BNS-2000.

TABLE 3-12. Networking Services Trunk/Link Modules

Module Name	Description
SWT	(Standard Wire Trunk.) The SWT is used in pairs to provide a wire trunk connecting either two BNS-2000 nodes, or a wire link connecting a BNS-2000 node and a Multipurpose Concentrator. The SWT is also used to provide a connection from the node to a remote ISN Concentrator or to an ISN node. The SWT supports up to 506 virtual circuits for end users at speeds from 2.4 Kbps to 2.048 Mbps, including fractional T1. The SWT can be optioned for an EIA RS-232-C, RS-422/449, G.703, or V.35 interface to an external multiplexing device like a channel service unit/data service unit (CSU/DSU).
SFT	(Standard Fiber Trunk.) The SFT provides a limited distance, high-speed, point-to-point fiber cable connection over distances of up to 3 km. The SFT can be used in pairs to connect two BNS-2000 nodes, or to connect a BNS-2000 node to either of the Multipurpose Concentrators. It also connects a BNS-2000 node to a fiber ISN Concentrator or to an ISN node. The SFT supports speeds up to 8 Mbps. It supports up to 2042 virtual circuits for end users.
Trunk-PQ	(Trunk-Priority Queueing.) The Trunk-PQ is a single port wire interface that provides fair queuing and enhanced buffering for multi-protocol traffic, and enforcement of CIR for frame relay traffic at up to T1/E1 rates. A V.35 DTE I/O board provides a V.35 DTE connection to the external device. Up to 2038 end user channels are available.
Trunk-64	(Trunk-64.) The Trunk-64 is a single-board module that is recommended to connect two BNS-2000 nodes over a digital transmission facility. The module operates at speeds of 9.6, 19.2, 48, 56, or 64 Kbps and provides both EIA RS-232-C and V.35 I/O connections. It supports up to 504 virtual circuits for end users. The module can interface with a *Dataphone*® DDS network or equivalent analog circuit using modems at speeds of up to 9.6 Kbps and duoplexors at speeds up to 19.2 Kbps.
Trunk-T1	(Trunk-T1.) The Trunk-T1 is used in pairs to provide long-distance, high-speed, point-to-point communication over a T1 digital transmission facility between two BNS-2000 nodes or between a BNS-2000 node and a *Datakit* II VCS node. It supports internodal speeds up to 2.048 Mbps, and up to 2042 virtual circuits for end users. The module also provides connections from BNS-2000 nodes to SAM504s or SAM64s at speeds from 56 Kbps up to 2.048 Mbps. It connects to a T1-Trunk in the SAMs.

TABLE 3-12. Networking Services Trunk/Link Modules (continued)

Module Name	Description
Trunk-HS	(Trunk-High Speed.) This 8 Mbps fiber interface module is used in pairs for connections between two BNS-2000 nodes, or between a BNS-2000 node and a *Datakit* II VCS node. When the Trunk-HS is used to connect nodes, it can be installed in any slot available to interface modules in the node cabinet. It can also be used to connect a BNS-2000 node to a SAM504 or SAM64. An HS-Trunk is used in the SAM to complete the connection. The Trunk-HS supports up to 2042 virtual circuits for end users for distances of up to 3 km.
Trunk-T3S	(Trunk-T3S.) The Trunk-T3S is used in pairs to connect two BNS-2000 nodes over a T3 facility. The Trunk-T3S transports both connectionless and connection-oriented traffic. The Trunk-T3S is a downloadable module which can only be located in a Series M2 shelf.
Trunk-E3S	(Trunk-E3S.) The Trunk-E3S is used in pairs to connect two BNS-2000 nodes over an E3 facility. The Trunk-E3S transports both connectionless and connection-oriented traffic. The Trunk-E3S is a downloadable module which can only be located in a Series M2 shelf.
Trunk-T3A	(Trunk-T3A.) The Trunk-T3A is used in pairs to connect two BNS-2000 nodes either directly over a T3 facility or through an ATM network. The Trunk-T3A transports both connectionless and connection-oriented traffic. The Trunk-T3A also provides support for CIR for frame relay service. The Trunk-T3A is a downloadable module which can only be located in a Series M2 shelf.
Trunk-E3A	(Trunk-E3A.) The Trunk-E3A is used in pairs to connect two BNS-2000 nodes either directly over an E3 facility or through an ATM network. The Trunk-E3A transports both connectionless and connection-oriented traffic. The Trunk-E3A also provides support for CIR for frame relay traffic. The Trunk-E3A is a downloadable module which can only be located in a Series M2 shelf.
SAMML	(SAM Multiport Link.) The SAMML provides a wire link that connects a BNS-2000 node with SAM16s, SAM64s, and SAM504s. It is installed in the node, where it occupies only one slot but provides up to 8 ports. Its counterpart modules in the SAMs are the SAMSL in the SAM504 and SAM64, and the SAMDL in the SAM64. The SAM16 has an integrated SAMSL. The maximum configurations are as follows: eight lines operating at 9.6 Kbps (full-duplex); four lines operating at 19.2 Kbps; or one line at 64 Kbps, with a total bandwidth limit of 128 Kbps.
SAMSL	(SAM Single Link.) This wire trunk module terminates, at both ends, the DDS or analog transmission facility connecting a BNS-2000 node and a SAM. It supports up to 504 end user channels at speeds ranging from 9.6 to 64 Kbps. (In the SAM16 it is integrated with control and port interface components.) The SAMSL presents either an EIA RS-232-C or V.35 interface to an external multiplexing device or modem.
SAMDL	(SAM Dual Link.) The SAMDL provides dual wire links between a SAM64 and a SAMML in the node and supports 64 virtual circuits. The overall dual link throughput is 9.6 or 19.2 Kbps. The SAMDL presents an EIA RS-232-C interface to an external multiplexing device or modem. It can only be used in the SAM16 and the SAM64.

Internetworking Services

BNS-2000 nodes can interwork with the following:

- *BNS-1000 or Datakit* II VCS nodes — *BNS-2000 nodes can be trunked to BNS-1000 or Datakit* II VCS nodes using SFT, SWT, Trunk-64, Trunk-HS, Trunk-T1, or Trunk-PQ modules.
- *Datakit* VCS nodes running Generic 3.3 or 3.4 — BNS-2000 nodes can be trunked to *Datakit* VCS nodes using Trunk-64, Trunk-T1, or Trunk-HS modules. The two products fully interwork for all compatible services.
- *ISN nodes running Version 7.0.1I software* — Wire trunk connections via the SWT or fiber trunk connections via the SFT are available. Asynchronous connections, multiplexed host services, synchronous transport service across BNS-2000 only, and LAN bridging services are supported. There are some limitations in addressing, security, and features. See ISN documentation for details. ISN asynchronous-to-X.25 service must be provided via BNS-2000.
- *Definity 75/85 Communications System* — A user will see two dial prompts (one from BNS-2000 and one from Definity 75/85) when switching across these interfaces. BNS-2000 trunks can use the trunk-sharing facility provided by Definity 75/85. The trunk-sharing facility is transparent to BNS-2000.
- *5ESS Switch* — The BNS-2000 X.25 service supports two-way communication to the 5ESS switch across the X.25 interface, with X.121 addressing and CUG security. The BNS-2000 network is considered an access point on the 5ESS Switch. Connectivity is supported for devices using asynchronous services and multiplexed host services. BNS-2000 is physically connected by a V.35 link to an ISDN Terminal Adapter that ends a 2B+D Digital Subscriber's Loop (DSL) from the 5ESS Switch.

Refer to the previous section on Networking Services for descriptions of the modules that support internetworking between BNS-2000 and other network products.

Component Compatibility

End-to-end data transport requires module compatibility. Frequently the data services explained earlier in this chapter can be achieved using interfaces provided by several different modules. Table 3-13 shows the interface modules (except for trunk/link interfaces) that are compatible. To use the table, find a module in the left column and read across. The check marks show compatible modules, i.e., those that provide data transport service when used together with the module in the left column.

TABLE 3-13. Interface Module Compatibility—Connection-Oriented Modules

Modules	CPY1	CPM-HS	E2A	FRM	FRM-M2	LPM	MSM	SLM	SYNC8	TERM32	TSM8	TSM-T1	TY6	TY12	X.25	X.25P	X.75
CPY1	√	√[1]					√			√	√	√	√[1]	√[1]	√[1]	√[1]	√[1]
CPM-HS	√[1]	√	√				√	√		√[1]	√[1]		√	√	√[1]	√[1]	√[1]
E2A		√															
FRM				√	√	√											
FRM-M2				√	√	√											
LPM				√	√	√											
MSM	√[1]	√[1]					√			√[1]	√[1]		√	√	√[1]	√[1]	√[1]
SLM		√															
SYNC8									√								
TERM32	√	√[1]					√[1]			√	√	√	√[1]	√[1]	√[1]	√[1]	√[1]
TSM8	√	√[1]					√[1]			√	√	√	√[1]	√[1]			
TSM-T1	√									√	√	√					
TY6	√[1]	√					√			√[1]	√[1]		√	√	√[1]	√[1]	√[1]
TY12	√[1]	√					√			√[1]	√[1]		√	√	√[1]	√[1]	√[1]
X.25	√[1]	√[1]					√[1]			√[1]			√[1]	√[1]	√	√	√
X.25P	√[1]	√[1]					√[1]			√[1]			√[1]	√[1]	√	√	√
X.75	√[1]	√[1]					√[1]			√[1]			√[1]	√[1]	√	√	√

1. For asynchronous communication.

Table 3-14 shows the connectionless modules (except for trunk/link interfaces) that are compatible.

TABLE 3-14. Interface Module Compatibility—Connectionless Modules

Modules	AI-T1	AI-E1	AI-T3	AI-T3P	AI-E3
AI-T1	√		√	√	
AI-E1		√			√
AI-T3	√		√	√	
AI-T3P	√		√	√	
AI-E3		√			√

Table 3-15 shows support for interface module placement.

TABLE 3-15. Placement of Interface Modules

Module	Node M1	Node M2	Multi Conc	SAM504, 64	SAM16
BASIC ASYNCHRONOUS SERVICES					
MSM	√		√		
TY12	√		√		
TY6	√		√		
TERM32				√	
CPY1					√
SYNCHRONOUS TRANSPORT SERVICES					
TSM8	√		√		
TSM-T1	√		√		
TERM32				√	
CPY1					√
SWITCHED SYNCHRONOUS SERVICES					
SYNC8	√		√		
MULTIPLEXED HOST INTERFACE SERVICES					
CPM-HS	√		√		
X.25 SERVICES					
X.25	√		√		
X.25P	√		√		
X.75	√		√		
LAN INTERCONNECT SERVICES					
LPM	√		√		
FRM	√		√		
FRM-M2		√			
SPECIAL PURPOSE SERVICES					
E2A	√		√*		
SLM	√		√*		
CUSTOMER PROGRAMMABLE SERVICES					
DKAP	√				
CONNECTIONLESS SERVICES					
AI-T1		√			
AI-E1		√			
AI-T3		√			
AI-T3P		√			
AI-E3		√			
GAR		√			

* For use with MPC15 only.

Networking and internetworking are provided by compatible trunk/link modules. Some trunk/link modules must be used in pairs at both ends of the trunk, some are compatible with different modules, and some can only be used with a counterpart trunk/link module that is designed for placement in a specific component. Table 3-16 shows trunk/link module compatibility for Series M1 Shelf trunks. Modules in the left column can be used with any module checked to the right.

TABLE 3-16. Trunk/Link Module Compatibility

Modules	TRK-HS	TRK-PQ	TRK-T1	TRK-64	SFT	SWT	SAMML	SAMSL	SAMDL	HS-TRK	T1-TRK
TRK-HS	√									√	
TRK-PQ		√									
TRK-T1			√								√
TRK-64				√							
SFT					√						
SWT						√					
SAMML								√	√		
SAMSL							√	√			
SAMDL							√				

Table 3-17 shows connectionless trunk/link module compatibility for Series M2 Shelf trunks.

TABLE 3-17. Trunk/Link Module Compatibility

Module	TRK-T3S	TRK-E3S	TRK-T3A	TRK-E3A
TRK-T3S	√			
TRK-E3S		√		
TRK-T3A			√	
TRK-E3A				√

Table 3-18 shows BNS-2000 components in which a trunk/link module can be placed.

TABLE 3-18. Placement of Trunk/Link Modules

Module	Node-M1	Node-M2	Multi Conc	SAM64, 504	SAM16
TRK-PQ	√				
TRK-64	√				
TRK-HS	√				
TRK-T1	√				
SFT	√		√[1]		
SWT	√		√[1]		
SAMML	√				
SAMSL	√			√[1]	√[2]
SAMDL				√[3]	
HS-TRK				√[1]	
T1-TRK				√[1]	
TRK-T3S		√			
TRK-E3S		√			
TRK-T3A		√			
TRK-E3A		√			

1. For connection to the node only
2. Functionality integrated in SAM16
3. In SAM16 and SAM64 only

Table 3-19 shows the trunk modules that provide networking or interworking between BNS-2000 and other network components. Trunk modules in the left column, residing in a BNS-2000, provide trunk connections to any components checked to the right.

TABLE 3-19. BNS-2000 Trunk Connections to Other Network Components

Trunk Module	Other Component						
	***Datakit* II VCS**	***Datakit* VCS**	**ISN Node**	**Conc**	**SAMs**	**BNS-1000**	**BNS-2000**
TRK-HS	√	√			√[1]	√	√
TRK-DDS	√	√					
TRK-PQ	√					√	√
TRK-T1	√	√			√[1]	√	√
TRK-T3S							√
TRK-E3S							√
TRK-T3A							√
TRK-E3A							√
TRK-64	√	√[3]				√	√
SFT	√		√	√		√	√
SWT	√		√	√		√	√
SAMML					√[2]		
SAMDL					√[4]		
SAMSL					√[2]		

1. SAM504, SAM64
2. SAM504, SAM64, SAM16
3. Trunk-DDS in the *Datakit* VCS
4. SAM16 and SAM64 only

Operational Features

BNS-2000 software is designed to provide a rich set of operational features that supplement the main data transport services. These features are organized into three categories:

- Connection-oriented operational features
- Connectionless operational features
- Common operational features

Connection-Oriented Operational Features

The following sections describe connection-oriented operational features.

Addressing

BNS-2000 supports a network addressing scheme in which the address of any destination can be an alphanumeric mnemonic name, a numeric address, or both. The addressing scheme is hierarchical; each address can contain four levels in either or both of the following formats.

Mnemonic BNS-2000 addresses use the format:

network/area/exchange/station[.optional parameters]

Numeric BNS-2000 addresses use the format:

DNIC/SR/SA/EPN[.optional parameters]

For example, BNS-2000 addresses might appear as:

usa1/nj/monmouth/host22

4444/333/222/1111

Each level of a mnemonic name can contain up to eight characters; the number of digits each field of a numeric address may contain varies. This is explained below.

- *Network or Data Network Identification Code (DNIC)* — The network level is the fourth and highest level of addressing and is used to route calls to other PSPDNs. Network level addresses can be represented by 4-digit numbers called DNICs (Data Network Identification Codes).
- *Area or Service Region (SR)* — The third level of addressing is used to route calls to an area that contains a group of exchanges. The Service Region is a three-digit number.
- *Exchange or Service Area (SA)* — The second addressing level is used to route calls to a grouping of stations that can be on one or more nodes. The Service Area is a three-digit number.
- *Station or Endpoint Number (EPN)* — This is the first and lowest level of addressing. This level is used to route calls to local stations within the same exchange. A station is the

representation of a channel to a destination device. The EPN corresponds to a station name and is a four-digit number. Each station can be assigned one or a range of EPNs.

The minimum required level of address is a station name or EPN. Each higher level can be added as a way to further define the address. Users can always enter all four levels of an address, and may mix the numeric and mnemonic parts of the address.

Address and routing tables can be configured in node databases that allow users to communicate throughout the network without needing to remember routing information. A destination's name is all that is necessary for a user to enter. The address is translated on the local node and the node understands if the destination is within the exchange or SA, routing the call to the correct station or EPN. If a destination is not within the same exchange, routing is done on the exchange or SA. If a destination is in a different area or SR, routing is done on the area or SR, and so on. A mechanism prevents calls from being routed back over the same trunk on which they arrived.

Service Addressing A BNS-2000 address can include a string of optional parameters appended to the end which are application-dependent. The frame relay service takes advantage of this optional string to identify the destination module, port, and DLCI used in a permanent virtual circuit between two FRM endpoints. The format of the string in this case is

<address>.<module address>.<port number>.DLCI

where module address can be the slot number of the module including the concentrator slot number if the FRM is in a concentrator. See the *Frame Relay Module Reference* for more information on defining addresses of this form.

X.121 Addressing. Support for X.121[1] addressing enables the BNS-2000 node to route calls to specified X.25 interfaces and transparently pass user-specified addresses to a PSPDN for further routing by that network. Incoming traffic from an X.25 PSPDN is routed to the appropriate endpoint on the network.

The NANP is the default used, and requires the structure of the address to be as described above—a 4-digit DNIC, a 3-digit Service Region, a 3-digit Service Area, and a 4-digit Endpoint Number.

Terminal users specify the address (a mnemonic or X.121 (BNS-2000 address) of the integrated PAD at the **`DESTINATION:`** prompt. When the user connects to the BNS-2000 X.25 module that provides the PAD service, a profile defines the parameters of the call. This profile, called an X.3 profile[2], can be designed by the BNS-2000 network administrator, can be a default profile provided by BNS-2000, or can be configured by the terminal user if permission is granted by the administrator.

X.28 commands and service signals[3] are supported for communication between the user's

1. See CCITT Recommendation X.121.
2. See CCITT Recommendation X.3.
3. See CCITT Recommendation X.28 and the *Data Networking Products Terminal User Guide.*

terminal and the X.25 modules' integrated PAD.

After connecting to the PAD, users can communicate with it using the appropriate X.28 command and then call out by specifying the X.121 address of the X.25 host or service on the remote PSPDN they wish to call.

X.75 International Addressing. Using the X.75 National and International Gateway Feature, a call can be routed to a PSPDN using X.121 and E.164/E.163 addressing. X.75 supports the 1988 International X.121 Numbering Plan. The E.164 Numbering Plan (the Numbering Plan for the ISDN) can be selected for use in place of the X.121 Numbering Plan by using escape codes. Calls may thus be routed to a PSPDN through an X.75 gateway using X.121 and E.164/E.163 addressing. Using X.75, calls can also be routed to or from a BNS-2000 asynchronous (TY12, MSM, CPM, SAM) host or an X.25 host endpoint on an X.75 Gateway.

This release includes the following:

- A call can be routed to a PSPDN through an X.75 gateway using X.121 and E.164/E.163 addressing.
- At the X.75 gateway interface, address mapping is not required.
- For both E.164 and X.121 addressing, Data Country Code (DCC), Country Code (CC), and Telephone Country Code (TCC) suppression for national gateways is supported.
- For international calls, the number analysis is 4 to 10 digits for X.121 International addresses and 1 to 7 digits for E.164 addresses. Routing is non-hierarchical.
- For X.121 International Addresses, the extended digit analysis supports Private Data Network Identification Codes (PNICs) defined in the CCITT X.121 Recommendation.
- The BNS-2000 X.121 Numbering Plan (the four-level hierarchical NANP) is supported.

Quickcalls. A quickcall feature allows users the option of calling both the address of the PAD on BNS-2000 and the X.121 address on the PSPDN in one step. The format is

<**BNS-2000 PAD address**>.<**X.121 address**>

This option establishes a connection directly with the final destination on the PSPDN or X.25 host.

Speedcalls. A speedcall name is a BNS-2000 addressing feature that provides a network administrator with the capability to create an alias name for a destination address. Users enter the alias name, usually a short, easy-to-remember name for a destination that might otherwise be hard to remember.

Speedcalls also provide an additional measure of security. Users cannot determine from the speedcall name whether the host they are accessing is local or remote, or the exact address of the destination.

Default Routing. Default routing simplifies management of large BNS-2000 networks. It permits centralization of address knowledge in a small set of nodes. Every node in the network does not need to have knowledge of all service addresses to reach exchanges or areas not defined

on the node.

Default routing is implemented by separating the network into hub nodes and leaf nodes at their respective levels. Using an administered set of default names, the leaf nodes channel all unknown mnemonic and numeric addresses to their hub nodes via trunk groups. The hub nodes then channel the call on, either to a higher level hub node or down to a leaf node at the same level.

This feature reduces the number of nodes to update when a new non-local address must be administered.

Destination Parameters. BNS-2000 address formats also provide a field for destination parameters, which may correspond to a service on a multiplexed host interface, information used by an X.25 PAD interface, or information used by a modem pool dialer.

Autobaud Detection

Autobaud detection allows an asynchronous terminal to configure its network interface port at connection time without a prespecified port baud rate. The interface module detects the transmission speed of the terminal and sets the port accordingly.

Grade of Service (GOS)

Communications between modules internal to BNS-2000 use a communications protocol with a Grade of Service. The Grade of Service (GOS) is the level of support provided for certain protocol features, one of which is error detection and correction. The five grades of service implemented for certain interface modules in the BNS-2000 network are shown in Table 3-20, which describes GOS error control available on BNS-2000 modules. The Grades of Service provided by individual modules are covered in **Hardware**.

TABLE 3-20. Grades of Service

Service	Explanation
GOS1	No flow control; no error control.
GOS2	Flow control; no error control.
GOS3	No flow control or retransmission; provides error detection.
GOS4	Flow control and error detection are provided; no retransmission of corrupted or missing blocks.
GOS5	Flow control; error detection; retransmission.

BNS-2000 switches data with minimum delay and moves it through the network as fast as possible with minimum buffering. Flow control, determined by the GOS, is used to manage congestion by limiting the amount of data that can build up within a virtual circuit. BNS-2000 specifies, for each virtual circuit, a limit to the volume of data that can be in transit at any one moment. The data is not permitted to occupy more than a predetermined amount of queue space; the excess data is stored for transmission in a buffer.

BNS-2000 flow control features permit the network administrator to set flow control using a

variety of options. For asynchronous devices, BNS-2000 supports flow control through software (XON/XOFF) or hardware (RTS/CTS) options. In addition, BNS-2000 can either flow control the devices, be controlled by them, or both. Administrators can also select no flow control.

To avoid data loss, the network administrator should select a flow control option when configuring module ports. Flow control available with BNS-2000

- limits the amount of data in transit on a virtual circuit to the internal buffer size
- provides end-to-end flow control with the connecting devices

To avoid data loss, if no flow control option is selected, the connecting devices must insure that the volume of data in transit in each direction of a virtual circuit is less than the buffer limit for that type BNS-2000 module.

Groups

The group feature allows the network administrator to associate a list of receiving ports — such as host ports, modems, or trunks — with a service address, giving an end user access, via a single address, to a destination served by multiple ports or trunks. A service address can point to as many as four different groups. The members of a group are searched in either round-robin or first-listed, first-called order. The round-robin search routes calls to each group member in turn. If the first member receives a call, the second member receives the next call whether the first member is available or not. The first-listed, first-called search always starts with the first-listed group member. If the first is unavailable, the call is routed to the second member, and so on.

Host Autobaud

Host autobaud sets the remote asynchronous network port to match the speed of the local asynchronous port. This capability (also known as *speed matching*) allows the use of a uniform end-to-end transport speed. It requires the destination host to allow incoming autobaud.

Modem Pools

Modem pools can be administered so that a group of ports is associated with a single service address. A user can thus identify a single address to gain access to a pool of modems.

Security

BNS-2000 supports a number of security methods. Network access restriction, originating group security, PVC security, CUG security, trunk and CPM host call screening, X.25 incoming/outgoing calls barred, X.75 utilities, Network Access Control System, and customer programmable services security are all security methods implemented within BNS-2000 software. Each method is described in the following subsections.

If a network is configured to use multiple security checks, calls will not be established unless all security checks pass. If any check fails, the call is denied.

Network Access Restriction. Network access restriction is an optional feature that is based on and supported by originating group security. The feature ensures security for ports that provide access to devices located outside secure areas. When a device connects to the network, and a

password has been configured for the device's originating group, the user is prompted for the network access password to gain access to the network. The node does not send the **DESTINATION:** prompt if the user does not provide the correct password.

Originating Group Security. This type of security is based on the principle that every device attached to the network must belong to a group: a potential call originator is assigned to an originating group or two-way group; a call destination is assigned to a receiving group or two-way group and is assigned a service address. The network administrator can implement call restrictions that allow each network destination to either accept or deny a call from members of certain originating groups by defining security patterns for each service address that specify which originating groups are allowed access. These controls ensure that only members of specified originating groups can complete calls to the destination. This feature can be enabled separately from network access restrictions, and separately for each node in the network.

The select group feature allows a user to change to a new originating group name during a session. A password is required before acquiring the new group identity. The network administrator enters the special group **select** for each node. After the **select** group is entered, the administrator can associate a terminal port with it, or a user with permission may access the **select** feature from command mode. By selecting a new group identity, the user acquires the calling permissions of the new group.

PVC Security. In a switched environment, a caller can connect to a variety of destinations. A permanent virtual circuit (PVC) or predefined destination (PDD) is an administrator-provisioned circuit connecting two endpoints and essentially shutting off switching capability for those endpoints. PVCs/PDDs allow an administrator to establish a circuit so that two endpoints can communicate only with each other and with no other endpoints in the network. Permanent virtual circuits are used in services such as frame relay and to provide additional security in a switched environment.

Trunk Call Screening. Trunk call screening security allows sets of permissible security patterns to be defined for calls entering a node from each trunk. Incoming dialstrings can be screened at strategic points in networks to confine access to particular hosts, such as a Network Access Controller, nodes, or sets of nodes located elsewhere in the network. This gives local node administrators total control of security domains and network resources.

Through trunk call screening security, network administrators can

- limit accessible domains at network interconnection points so that one network's restrictions cannot be defeated by changes in originating node definitions within another network
- share network capacity with trunks from or between potentially untrustworthy nodes without allowing full network access

When a call is placed over an internodal trunk, the incoming dialstring is matched against the security set specified for the trunk. If the destination string matches the security set, the setup call is passed to its destination. Otherwise, the call is blocked and recorded. Trunk call screening security is checked before originating group and CUG security are checked.

CPM Call Screening. CPM host call screening allows the network administrator to configure limits on calls made from the CPM-connected host, and thereby prevent unauthorized host-to-

host calls. CPM call screening functions are the same as trunk call screening functions, described above.

X.25 Closed User Group Security. Closed user group (CUG) security provides a set of X.25 facilities that support

- closed user groups for subscribed endpoints
- closed user groups with incoming access for subscribed endpoints
- closed user groups with outgoing access for subscribed endpoints
- closed user group selection
- closed user group with outgoing access selection

CUG security restricts members of a CUG to access to endpoints that are members of the same CUG. An endpoint, hunt group, or gateway is configured with a CUG profile. This profile contains the list of closed user groups to which that entity may belong, whether the entity has outgoing or incoming access, and a preferential closed user group for that entity.

Outgoing access permission allows an endpoint to make calls to endpoints that do not have CUG security configured (known as the open part of the network) or to endpoints that have incoming access permission.

Incoming access permission allows an endpoint to belong to a CUG and receive calls from endpoints in the open part of the network or from endpoints that have outgoing access permission.

X.25 Incoming/Outgoing Calls Barred. For endpoints connected to X.25 ports, network administrators can implement security that prevents the endpoint from originating or receiving calls. Normally, calls into or out of X.25 endpoints have both incoming and outgoing switched virtual circuit (SVC) access. Administrators can restrict SVC access to these endpoints through the following X.25 facilities:

- incoming calls barred
- outgoing calls barred

Another feature, one-way logical channels incoming/outgoing, applies to logical channels on a two-way X.25 port that are administered for SVC calls. The administrator can define a range of SVC logical channels on a two-way port that can only originate calls, or only receive calls. If all the SVC logical channels on that port are defined as one-way incoming, the effect is the same as outgoing calls barred. If all the SVC logical channels are defined as one-way outgoing, the effect is the same as incoming calls barred.

X.75 Utilities. The X.75 Gateway feature supports the following utilities based on the CCITT 1988 X.75 Recommendation:

- *Closed user group indication* — The closed user group indication is a network utility used to enable the establishment of virtual calls by DTEs that are members of international closed user groups. The use of this network utility at the gateway interface is subject to a bilateral agreement between administrations.

- *Closed user group with outgoing access indication* — This utility must be supported on both national and international gateways. When using the closed user group with outgoing access indication utility in the call request packet, the gateway indicates that the virtual call is requested on the basis of valid international closed user group membership. Closed user group screening also applies to this utility.
- *Check of traffic agreements for incoming calls* — For incoming international calls, a check is performed to determine if traffic agreements exist with the originating country. The check is based on the DNIC or CC of the calling DTE and the network's routing tables.

  For an invalid calling DNIC or CC, the call is rejected with the cause **`Network Congestion`** and the diagnostic code is **`Unknown Calling DNIC`**.
- *Disallowing new calls over a gateway module* — The network administrator is able to manually disallow further calls through the gateway at any time without dropping existing calls. This provides the capability to schedule service outages without disrupting active calls. This will apply for calls in both directions.

Network Access Control System. The Network Access Control System augments the basic security functionality of a BNS-2000 network through a software package that runs on an HP9000 Model 715/75. See **Related Products** for more detailed information.

Customer Programmable Services Security. Additional levels of security are available through various software applications running on the DKAP module. Call back modem (CBM) software is AT&T-provided software that runs on the DKAP, providing security for network destinations for which CBM security is defined. When a user dials a destination defined for CBM software, the call is routed to the CBM software. The CBM software performs user authentication, disconnecting the call if it passes authentication. The CBM software then calls the final destination, calls back the user at a number stored in its memory, and splices the user to the destination.

Session Maintenance

Session maintenance is a feature that provides trunk transport reliability for active calls. To configure trunks for session maintenance, administrators use *StarKeeper* II NMS Network Builder to partition the existing channels on physical trunks into sets of logical channels, called channel sets. As the channel sets are configured for each trunk, administrators exercise the option to designate some of them *active* channel sets, which support normal call setup and data transport. The remaining channel sets can be designated as *standby* channel sets. Standby channel sets are not used for normal data traffic; they are reserved to provide facilities that support alternate paths through the network when active channel sets from a failed trunk must be rerouted.

Using the data supplied by administrators for trunk configuration, Network Builder also generates configuration database tables, called Node Reroute Tables (NRTs), for each node in the network. These tables contain all the information needed for nodes to determine, in real-time, available reroute paths around a failed trunk. Network Builder, through the *StarKeeper* II NMS Core System, downloads an NRT to each node in the network, distributing an accurate, intelligent database for the session maintenance feature throughout the network. With trunks configured for session maintenance, NRTs downloaded, and some additional node tuning parameters defined,

the network can actively support session maintenance.

Continual, real-time testing routines permit the nodes to detect highly errored or failed trunks within an administrator-defined window of time. When a node detects that the error rate of a trunk configured for session maintenance exceeds an administrable threshold, it invokes a reroute by locating standby channel sets on other trunks that can provide alternate routes for the affected trunk channels. The node attempts to locate standby channel sets even if the affected channels do not happen to contain active calls at that time.

To locate the standby channel sets, the node looks at information about neighbor nodes in its NRT. A node that is seeking alternate routes for channel sets on the failed trunk is thus capable of locating a path parallel to the failed trunk or, in the absence of a parallel path, of negotiating with other nodes for unused bandwidth on other facilities. In the second case, the node issues requests to neighbor nodes for reroute paths over any available standby channel sets through these neighbor nodes. The alternate path that is eventually negotiated may be a multi-hop path around the failed trunk traversing up to three neighbor nodes.

After reroute requests are acknowledged and honored by neighboring nodes and a full path is negotiated, channel sets are rerouted to the newly established paths. Detection of a failed or highly errored trunk and the steps taken to reroute the affected channel sets can be accomplished within ten seconds, transparent to the devices and users engaged in sessions which may have been set up over the trunk. Rerouting is performed by the Control Computer and Eswitch module.

After the failed trunk is declared healthy (when it again passes the continual, real-time testing routines), channel sets that were routed around the failure can be moved back to their original path via a single administrative command.

Speed Conversion

The speed conversion feature enables two endpoint devices to communicate through the network at differing speeds. This capability is provided through buffering and flow control. Speed conversion is fully supported for any device that can accept flow control. Asynchronous flow control options are EIA (hardware) or XON/XOFF (software) flow control.

Splice

The splice feature allows the network to reroute a call to an intermediate destination (a multiplexed host), establish a separate virtual circuit from the intermediate to the final destination, and combine the two calls by removing the intermediate host. For example, the intermediate host might act as a security server for the destination host. Once a caller passes the security check, the intermediate host calls the destination and drops out of the spliced circuit. Splice is also available on the DKAP module.

Connectionless Operational Features

The following sections describe connectionless operational features.

Addressing and Security Features

Addressing and security features include the following:

- individual addressing
- group addressing
- source address validation
- source address screening
- destination address screening.

Each SNI must be assigned at least one unique individual E.164 address. The subscriber equipment must insert this address in the source address portion of the L3-PDU. The access interface in the switching system checks for an E.164 address in each L3-PDU entering the network.

Customers can define a set of individual addresses as a member of a group. A subscriber may insert a group address into the destination address portion of the L3-PDU so that the same message is sent to multiple destinations (all members of one group). Group addressing is analogous to the LAN multicast feature in which copies of the packet are delivered to a specified subset of destinations.

Although each SNI must have at least one individual E.164 address, a single SNI can be assigned up to 16 different individual addresses. Multiple addresses per SNI may be useful to allow a customer to operate and distinguish different protocols by using different addresses for each. This feature also supports the multiple-CPE access configuration where up to 16 CPE stations are connected to one SNI.

Source address validation takes place in the access interface for each L3-PDU on ingress. The source address in the L3-PDU must match one of the individual E.164 addresses assigned to this SNI. PDUs with invalid source addresses are logged and then discarded for security reasons.

A customer can administer individual and group address screening tables for each SNI. These tables specify the address screening values for data sent and received by the subscriber equipment. If an L3-PDU has a source address that the screening table does not permit, source address screening bars the AI from transmitting this PDU to the CPE. Screening is invoked for each L3-PDU on egress from the network, and functions by checking the source address of each L3-PDU against the individual screening table. Group addresses are not used in source address screening; the source address is always an individual address.

If an L3-PDU has a destination address that the screening table does not permit, destination address screening bars the AI from receiving this PDU from the CPE. Destination address screening is invoked for each L3-PDU on ingress to the network. In destination screening, the destination address is checked against the screening tables. Both individual and group addresses

can be screened with destination address screening.

PDUs that fail either type of address screening are logged and discarded at appropriate access interfaces.

Connectionless Routing

SMDS traffic is connectionless traffic, sometimes called datagram service. Routing for connectionless traffic is entirely different from routing for connection-oriented traffic, which the BNS-2000 node also supports. To route connection-oriented traffic, the network must first establish a virtual circuit (VC). Once such a circuit is established, a series of messages can be exchanged between the source and the destination endpoints.

In contrast, connectionless traffic is broken into individual messages at the source, and these messages are routed independently through the network. The originating router segments each SMDS data unit (Level 3 Protocol Data Unit [L3-PDU]) into fixed-length Level 2 PDUs (L2_PDUs). The L2_PDU carrying the first segment of each message contains the addressing information for the message and a message ID (MID) field. The addressing information is used to determine the routing for that message. If there is more than one segment in the message, each L2_PDU after the first one is routed according to the MID. An L2_PDU traverses BNS-2000 switching nodes from the source to the destination without the need to establish any virtual circuits along the route. Thus, for connectionless routing, a virtual circuit is never required.

In a network providing connectionless network service (CLNS), the end user is not aware of the existence of the switching network between LAN segments; as a rule, the network appears to the user to be an extension to the local segment of the LAN. In this environment, routing is accomplished dynamically by logic in the SMDS Switching System that refers to a set of routing tables. The connectionless routing tables are set up by each switching node, based on the network topology and network addresses that have been administered.

The basic principle of connectionless routing is that each L2_PDU is broadcast on the backplane bus to all SMDS modules.

- If the L2_PDU is addressed to an SNI at a local AI module, that module responds by delivering it to the destination SNI.
- If the L2_PDU is addressed to an SNI on a remote node, the appropriate connectionless trunk module routes it towards that node. Each node along the route forwards it in a similar fashion until it reaches the node to which the destination SNI is attached. Once the L2_PDU reaches the destination node, it is delivered by a local AI module to the destination SNI.

Therefore each AI or trunk module responds only to L2_PDUs that are addressed to endpoints within its jurisdiction. An AI module determines whether to receive a L2_PDU according to the addresses that are administered for its SNIs. A trunk module determines whether to forward a L2_PDU according to the connectionless routing tables.

Maximum Concurrent Data Units (MCDU) Feature

After the subscriber equipment starts to transmit the first segment of a multi-segment message, it may have other messages queued for transmission. The SIP allows more than one message to be sent or received concurrently through an SNI, so that several messages may be in transit in the network concurrently. The number of messages that an SNI can send or receive concurrently is called the maximum concurrent data units (MCDU). An SNI can be configured to use this feature for ingress (from the CPE), for egress (to the CPE), or both.

Common Operational Features

The software download feature is common to both connection-oriented and connectionless modules.

Downloadable Modules

A downloading feature allows module application software to be stored by the Control Computer or a host. When a downloadable module is put into service, the application software can then be loaded into the module memory.

With downloadable modules, users can upgrade module software faster and with less expense, upgrading all modules at the same time. The same module can be used for more than one function depending on the application software that is downloaded into it.

Depending on the module type, downloading occurs automatically when the module is first placed in service, when the module determines that the software is corrupted, or when off-line diagnostics are run on a module that is out of service. Otherwise, downloading is performed when module restores are explicitly requested by the network administrator.

The following table indicates which interface modules accept downloadable software.

TABLE 3-21. Interface Modules Accepting Downloadable Software

Interface Module	Downloadable	Not Downloadable
AI-E3	√	
AI-T1	√	
AI-T3	√	
AI-T3P	√	
CPM-HS		√
CPY1	√	
DKAP	√	
E2A		√
FRM	√	
FRM-M2	√	
GAR	√	
LPM	√	
MSM	√	
SLM	√	
SYNC8	√	
TERM32	√	
TSM-T1	√	
TSM8	√	
TY12		√
TY6		√
X.25	√	
X.25P	√	
X.75	√	

The following table indicates which trunk modules accept downloadable software.

TABLE 3-22. Trunk Modules Accepting Downloadable Software

Trunk Module	Downloadable	Not Downloadable
SAMDL		√
SAMML	√	
SAMSL		√
SFT		√
SWT		√
TRK-DDS		√
TRK-E3S	√	
TRK-E3A	√	
TRK-HS		√
TRK-PQ	√	
TRK-64		√
TRK-T1		√
TRK-T3S	√	
TRK-T3A	√	

The MRC function receives downloading only on request from the MRC function maintenance port (see the MRC function section in **Hardware**). Downloads to the MRC function may be needed when loading a new BNS-2000 software release.

Terminal User Features

User access to BNS-2000 is through asynchronous and synchronous devices connected to the BNS-2000 local node directly, or indirectly through concentrators or remote nodes.

Users on BNS-2000 or ISN nodes have available only the set of services that is supported by their local node. Users are able to make calls to compatible devices, with minimal BNS-2000 interaction beyond call setup and disconnection.

BNS-2000 offers a simple, easily understandable interface to the asynchronous terminal user. The following features, which are detailed in the *Terminal User Guide*, are described below.

NOTE: These terminal user features pertain only to connection-oriented (CONS) data services.

Call Hold

The network administrator can enable the call hold feature for a given port. When the terminal user, from command mode, requests the current call to be held, the network suspends the call without terminating it and prompts for a new destination. The caller can have eight simultaneous calls in progress, i.e., seven calls on hold and one active call, and by assigning a tag, or name, to each held call, can switch between calls by name.

Dialer Interface

The dialer interface is an automatic dialer that accepts a telephone number as a destination parameter included in a destination request. The interface can also accept the telephone number in response to a prompt sent to the caller. Operating at speeds up to 9600 bps, the autodialer is used to place a call from a BNS-2000 endpoint device out over a switched telephone network.

Dialing

The BNS-2000 addressing scheme — similar to the dialing plan in the telephone network — is hierarchical, with network services identified by logical addresses of the form *network/area/exchange/station.* When the network's **`DESTINATION:`** prompt appears on the terminal screen, the terminal user requests a connection by entering the address of the desired destination. If the destination is in the same exchange as the caller, only the station address is necessary. If the destination is in the same area as the caller, only the exchange and station addresses are necessary. If the destination is in the same network as the caller, only the area, exchange and station addresses are necessary.

The four elements of an address are usually mnemonic (rather than strictly numeric, as in the telephone system), and the network administrator can associate any four-level address with a single-level speedcall address. This shorter address simplifies dialing by making the address easy for users to remember.

Directory Assistance

The BNS-2000 node can store a directory of network addresses entered by the network administrator. If the administrator enables this feature, the terminal user can enter **?** at the **DESTINATION:** prompt to get help for directory assistance and information to gain access to the subset of those services that he or she is authorized to call. The directory assistance feature displays addresses one screen at a time.

The user can find out what services are available on another node by entering **area/exchange/?** or **exchange/?**, using the area and exchange of the remote node. The network sends the request to the remote node, which sends back the relevant subset of its directory.

Displaying and Setting Options

Each network port has certain parameter options set by the network administrator, including network attention signal, baud rate, parity, and flow control. The administrator can enable a terminal user to display all and change some of these options for the current session. Administrator-defined options are restored for subsequent sessions.

Help

From command mode, the terminal user can enter **help** to get access to a help menu explaining all available commands. (This menu is different from port to port, depending on the options administered for each port.)

Messages

A status or welcoming message, called the message of the day, can be entered by the network administrator. It appears on the screen when the terminal user connects to the network. Other messages sent to user terminals explain errors made either while entering responses to BNS-2000 prompts or while entering commands. The messages suggest an action the user should take to correct the situation.

Network Attention Signal

To get the attention of the node Control Computer, terminal users enter a signal at the keyboard. For example, to put an active call on hold and start a new call, a user first enters the network attention signal. The default attention signal is Break Break, entered within a one-second interval. The network administrator can redefine the attention signal, however, on a per-port basis, and can also authorize the individual terminal user to change it for the current terminal session. An administrator can configure a station so that the attention signal terminates the call, or can configure a station for no attention signal. The latter configuration requires turning off the terminal to terminate calls. The attention signal can be optioned to put the terminal user in command mode, which then allows users to access help screens, use call hold, or display and set terminal options.

Passwords

If the password feature is enabled by the network administrator, the terminal user is required to enter a password to gain access to the network and receive the **`DESTINATION:`** prompt. Passwords can also be required of users who attempt to select membership in different originating groups.

Local Administration Features

BNS-2000 provides integrated administration software with each node. All administration and operation for the local node can be done at the console attached to the node. The administration ports communicate with the node without disrupting service.

Multinode networks are more effectively administered and managed by *StarKeeper* II Network Management System; see the **Overview**.

The administrative interfaces provide a powerful and flexible set of tools for network operations, administration, and maintenance (OA&M) functions:

- configuration
- fault detection
- diagnostics
- measurements collection
- billing

Administrative Access

Administrative access to the BNS-2000 node is determined by a combination of the hardware interfaces used and how they are connected to the node, and by whatever security arrangements are made. In multinode networks, all nodes can be administered remotely from a central *StarKeeper* II NMS.

Node Console Interfaces

Administrative tasks are performed at a console connected to an administration port (port A) on the Control Computer. A second port connects to a dedicated printer. When the administrator enters a command on the console (port A) it also appears on the printer (port B). Port B can also be configured as both console and printer. In that case, commands entered at port B can also be seen at port A. The administrative interfaces include

- an asynchronous video display terminal (VDT) and keyboard, referred to as the *console*, with which the administrator can enter commands and receive system reports
- a dedicated printer, used for hard-copy output, that can be configured to receive reports and automatic alarm messages sent by the Control Computer

Console Equipment

The equipment that the administrator uses to manage a BNS-2000 node can vary. The recommended terminal is the AT&T Model 605, 615, or 620. Any ASCII terminal with an EIA RS-232-C interface, however, can be used as the network administration console as long as it provides lowercase characters (uppercase is optional). This console is typically connected to the node via a dedicated port (port A) in the back of the Control Computer.

Printer

The printer is used for hard-copy printouts of information typed at the system console, and can be configured to print status reports, error messages, and all system alarm messages. The administrator can choose to direct other output normally directed to the console screen to the printer as well.

Any serial printer that will handle the ASCII character set can be used.

The printer is usually connected to a port, referred to in the software as port B, in the back of the Control Computer.

Remote Administration

Either administration port on the node can optionally be connected to *StarKeeper* II NMS.

Nodes equipped with the MRC function can use it as a multiport maintenance interface to the node that allows automatic recovery through the redundant Control Computer in the node. The MRC function also allows the administrator to do remote maintenance or to reboot the node from a remote location, permitting reboot without the manipulation of switches. Remote maintenance and remote reboot capabilities are available on nodes with single or dual Control Computer configurations. *StarKeeper* II NMS can also be connected to the MRC function.

In an MRC function-managed node, the administrative interfaces (console, printer, *StarKeeper* II NMS) must be connected to the MRC function, which is in turn connected to the Control Computer.

Console Security

Unauthorized access from the console to the administration interface port on the BNS-2000 can also be protected by requiring a password entry. This feature may be optioned by the administrator. Entered passwords are not echoed to the administration output device.

Connection-oriented Billing

The billing process gathers and reports information on all calls made through the network, keeping track of the date and time of connection, identity of the originator, identity of the destination, and packet count for the duration of the call. The administrator sets up the billing feature and then enables it for a given port or service name as it is configured and brought into service. Records are sent either to a dedicated terminal or printer or to *StarKeeper* II NMS.

Connectionless Billing

SMDS Billing complies with the Bellcore standard TR-TSV-000775. The current SMDS Billing architecture consists of BNS-2000, *StarKeeper* II NMS, and the Billdats® Network Server. (See Related Products.)

SMDS Billing provides the capability to collect usage measurements that give the number of L2 and L3 PDUs transported by an AI towards the customer premises (egress) for each unique E.164 source and destination pair. In addition, audit counts are collected that give the number of L3

PDUs transported by the AI towards the customer premises for each SNI.

These usage measurements and audit counts are retrieved by the Billdats Network Server for the BNS-2000 switch, stored, aggregated, formatted into AMA records, and sent to the Regional Accounting Office (RAO) Billdats Collector.

The AI module will collect the usage measurement data at the egress SNI for each E.164 source and destination pair. The AI module will notify the Billdats Network Server of the availability of the usage measurements when any of the following conditions occur:

- the end of a 15-minute interval is reached
- the AI is removed from service (optional)
- global billing is turned off
- buffer overflow has occurred on the AI
- a time change has occurred on the node.

The AI module will also collect the audit counts for each egress SNI. The Control Computer (CC) will request audit counts from the AI when the following occur:

- the end of a 15-minute interval is reached
- global billing is turned off
- a time change occurs on the node.

The AI sends the audit data to the CC when the following occur:

- the CC makes a request
- an AI overflow occurs
- the AI is removed from service (optional).

The CC will send the audit counts to the Billdats Network Server when the following occur:

- the 15-minute interval has ended
- a time change occurs on the node.

SMDS billing is controlled by the administrator, via *StarKeeper* II NMS Network Builder, through the setting of two billing flags:

- a node-wide global billing flag
- a billing flag set per SNI.

Both flags must be on for usage measurements and audit counts to be collected and sent to the Billdats Network Server.

For specific administration procedures for interoperating with the Billdats Network Server, refer to the *Billdats Network Server User's and Administrator's Guide* for Release 1 (AT&T 190-136-120). The feature is based on Bellcore TR-TSV-000775, Issue 1, March 1990.

Database Configuration

Local administration of database configuration is only available for connection-oriented traffic. All connectionless services' configuration data must be administered via *StarKeeper* II NMS Network Builder (NB). However, while frame relay services can be configured locally, *StarKeeper* II NMS NB provides enhanced support for end-to-end PVC administration and is the recommended method for configuring frame relay services.

Network configuration is supported by more than 150 commands for provisioning services, including commands for

- entering, changing, deleting, and verifying information in the configuration database
- backing up the database to disk, tape, or host and restoring it from disk, tape, or host
- controlling the service state of network components

Most configuration commands can be entered at the console keyboard as simple English sentences comprising a command verb and object, such as **retire alarm**. The node also recognizes abbreviations and truncations of these command verb-objects.

Many commands require additional specification of various parameters. When the administrator enters a verb-object combination, the node will prompt for these parameters. For example, if the administrator types **enter ty** at the console, successive prompts ask for more information, such as the module's slot location and the baud rate, parity convention, and flow control for each port. For many commands, the administrator can shortcut the prompt sequence by entering the command verb, object, and values for all parameters on a single line.

Administrators can keep an event-log file of all administrator-entered commands and the system responses to them if an administration port is configured for a printer.

Autoresize

A standard database configuration can not meet the needs of every network configuration. If a network uses more of a given resource than the standard configuration allows, one of the internal database tables will run out of space. If this condition occurs during an upgrade to the current release, the system automatically invokes the **dbresize** command to change the size of internal database tables, shifting unused capacity from underused resources to resources that need the space.

Diagnostics

BNS-2000 provides the administrator with extensive diagnostic capabilities for isolating faults on network components, including trunks, modules, and individual ports on modules. These diagnostics at most disrupt service only to the single port or facility being diagnosed, and are executed entirely from the console without requiring manual switch setting on modules. Loopback tests, which are provided at the module and port level, can trace errors to a specific hardware unit. Loopback tests require special external loopback connectors or cables.

There are also diagnostics for the control modules that allow administrators to isolate faults.

These may cause a service disruption.

Fault Detection

BNS-2000 has a wide range of self-testing capabilities for automatic fault detection and notification:

- The network regularly polls all interface modules, including those in concentrators, for their status. If a module fails to report its status or indicates a fault, an alarm message is generated.
- The network detects secondary or transient failures such as parity errors or buffer overflow, and generates an appropriate alarm message.
- Individual modules can execute sanity tests of their various hardware components, including memory. These diagnostics exercise the hardware to ensure normal functioning, and generate alarm messages if faults occur.
- The network executes periodic automatic loopback tests, without disrupting service, on all trunk and multiplexed host connections to check their integrity. Failure generates an appropriate alarm.
- A watchdog timer, an external hardware option functioning independently of the node, requires the node's Control Computer to send periodic messages. If these messages are absent for a fixed period, the watchdog process activates an (optional) alarm indicating a node crash.

BNS-2000 sends alarm messages to the console to alert the administrator to fault conditions. By configuring a printer to receive these messages, the administrator can keep a log of all fault conditions; the messages indicate the severity, date, and time of each fault. With the appropriate auxiliary equipment, alarms can also generate an audible warning tone. Most modules have three LEDs that show whether the module is in on-line, off-line (diagnostic), or fault mode.

Measurements Collection

BNS-2000 provides the administrator with measurements collection and reporting capabilities, both on demand and automatically at scheduled intervals specified by the administrator. Measurements, including the following, are available for the Control Computer and for trunks, interface modules, and ports:

- byte, packet, and message counts
- call counts (number accepted; number rejected; abnormal terminations and reasons)
- utilization (module, line, or port)
- error counts
- failure statistics
- buffer overflow statistics

Some measurements are available only through *StarKeeper* II NMS.

Hardware

Hardware

This chapter describes the following categories of BNS-2000 networking equipment:

- ***The Node*** is the basic component of the network. It is the center for call processing and also enables administrative and diagnostic functions for the modules and devices connected to the node.
- ***Concentrators*** distribute connections to devices grouped in remote locations in a geographically dispersed network. They link a group of users to the node over a fiber link or wire link facilities, and provide various data services that support both small and large communities of users. This alternative to direct connection increases the physical capacity of the node, saves node capacity for other equipment and reduces cabling costs.
- ***Trunk Modules*** are circuit boards located in nodes, Multipurpose Concentrators, and Synchronous/Asynchronous Multiplexers (SAMs) that provide networking services between switching equipment or between switching and concentration components. They also provide internetworking services between BNS-2000 nodes and compatible nodes in other networks.
- ***Interface Modules*** are circuit boards that plug into nodes and concentrators and variously support asynchronous and synchronous services, frame relay, X.25 services, X.75 Gateway services, multiplexed host interface services, special purpose services, and vertical services.

BNS-2000 Node Physical Design

The design of the BNS-2000 node facilitates building node configurations of various physical sizes via stacking modular cabinets that all share the same external dimensions and exterior design. The cabinets are 30" wide by 17" high by 29" deep.

Up to four modular cabinets can be arranged in a single stack, allowing for greater switching capacity without increasing the node "footprint." The maximum physical size of a node consists of two adjacent stacks, totaling eight modular cabinets in various combinations that address the needs of a specific application.

Power can be supplied and distributed to the individual cabinets through either a base power unit or CO frame. In customer premises environments, each stack of cabinets is set on a base power unit. For telephone company CO environments, BNS-2000 hardware includes a specially designed CO frame that complies with special power, stacking, and cabling requirements.

Regardless of the physical size, network application, or operating environment, all BNS-2000 nodes consist of various combinations of the two BNS-2000 cabinet types, which are the Series M2 and Series M1 Cabinets:

- ***Series M2 Switch Cabinet*** has a 200 Mbps backplane; provides the segment switching and timing functions of the node.
- ***Series M2 Extension Cabinet*** extends the 200 Mbps backplane; functions as a port carrier by providing additional space for high-speed interface and trunk modules.
- ***Series M1 Control Cabinet*** has an 8 Mbps backplane; provides the central processing function, disk and tape storage, and administration and maintenance interfaces for the node.
- ***Series M1 Port Cabinet*** has an 8 Mbps backplane; functions as a port carrier by providing additional space for interface and trunk modules.

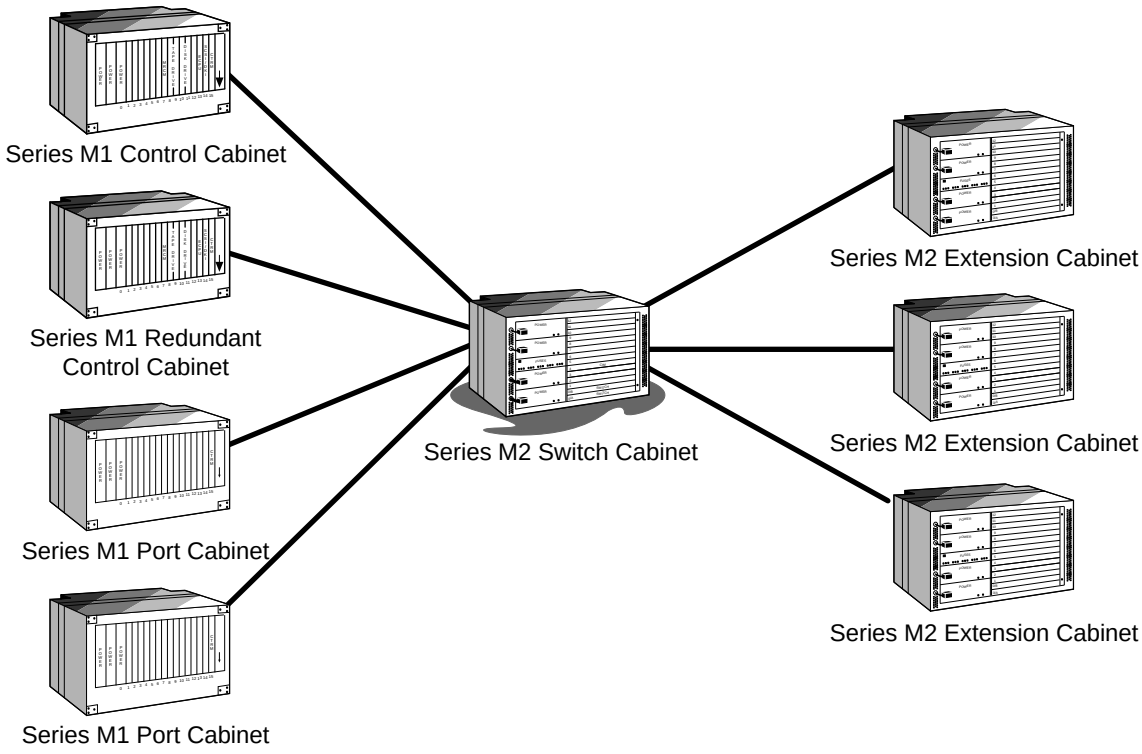

FIGURE 4-1. BNS-2000 Node Star Topology

Star Topology

The star topology of BNS-2000 nodes is made possible by a full-duplex fiber link between the Cabinet Interface Module (CIM) in the Series M2 Switch Cabinet and the Clock/Trunk/Repeater Module (CTRM) in each Series M1 Control or Port Cabinet. Fundamentally, the CIM and CTRM act as a gateway for interworking between the two cabinets.

The fiber connection between Series M1 Cabinets and the Series M2 Switch Cabinet means each Series M1 Cabinet has an 8 Mbps performance capacity independent of other Series M1 Cabinets in the node.

Cabinet Configurations

A node *must* contain one Series M2 Switch Cabinet and one Series M1 Control Cabinet. Beyond that the node can include up to the maximum combination of eight cabinets configured to support various functions and capabilities, populated with modules that address specific switching, reliability, and service requirements. Planning and network engineering guidelines to configure nodes for specific applications are covered in the *Planning Guide*. The table shows acceptable combinations of BNS-2000 cabinets.

Combinations of Series M2 and Series M1 Cabinets

Series M2 Cabinets		Series M1 Cabinets		
Switch	**Extension**	**Control**	**Port**	**Max. Total**
1	—	1 or 2	up to 6	7
1	1	1 or 2	up to 5	6
1	2	1 or 2	up to 4	5
1	3	1 or 2	up to 3	4

Internally, each cabinet has a shelf that is divided into slots. Series M2 cabinets are designed with horizontal slots; Series M1 cabinets are designed with vertical slots.

Fiber cable carries the bus and timing signals between Series M1 Cabinets and the Series M2 Switch Cabinet. Multi-coaxial cable is used to connect each Series M2 Extension Cabinet to the Series M2 Switch Cabinet.

The processing and interface functions in the node are performed by modules (plug-in circuit packs) which slide into the slots in the front of the cabinet. Each slot is designated by a number that identifies the module in the node database.

At the rear of each cabinet, the backplane carries data, timing, and contention signals, and power to the I/O boards associated with the modules. Most modules require I/O boards. They plug into pin fields at the same slot location on the rear of the backplane. The I/O boards connect the modules to endpoints or to other modules.

Modules fall into the following categories:

- ***Switching complex modules*** provide clock and switching functions.
- ***Control complex modules*** include the processor, disk and tape, and maintenance functions.
- ***Interface modules*** control communications and provide access to devices such as routers, terminals, and host computers connected to the node.
- ***Trunk modules*** provide communications with other nodes and with concentrators.

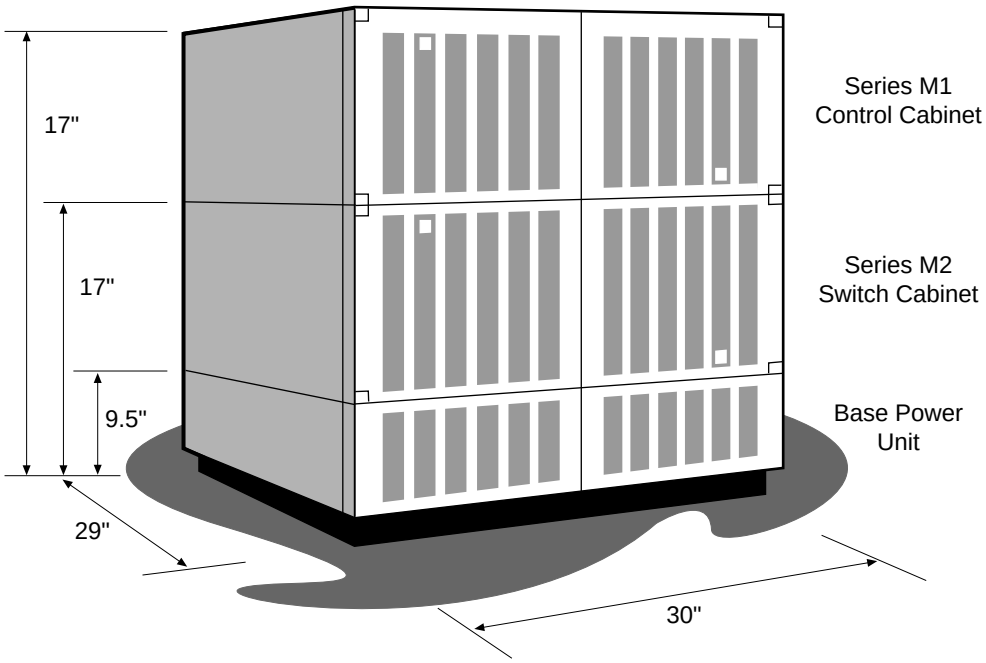

FIGURE 4-2. Basic Node and Base Power Unit: Cabinet Exterior

In Series M1 Cabinets all control and interface modules and I/O boards are connected to a backplane. The bottom of each Series M1 Cabinet contains a replaceable fan tray housing four fans that cool the internal circuit boards. Each Series M1 Cabinet is provided with three power supplies.

In Series M2 Cabinets, the Switch modules, interface modules, and I/O boards are connected to a high-speed backplane. The fan tray is located on the side. Each Series M2 Cabinet is provided with four power supplies. Power input options include the following:

- 200 to 240 VAC, 50/60 Hz
- –48 to –60 VDC.

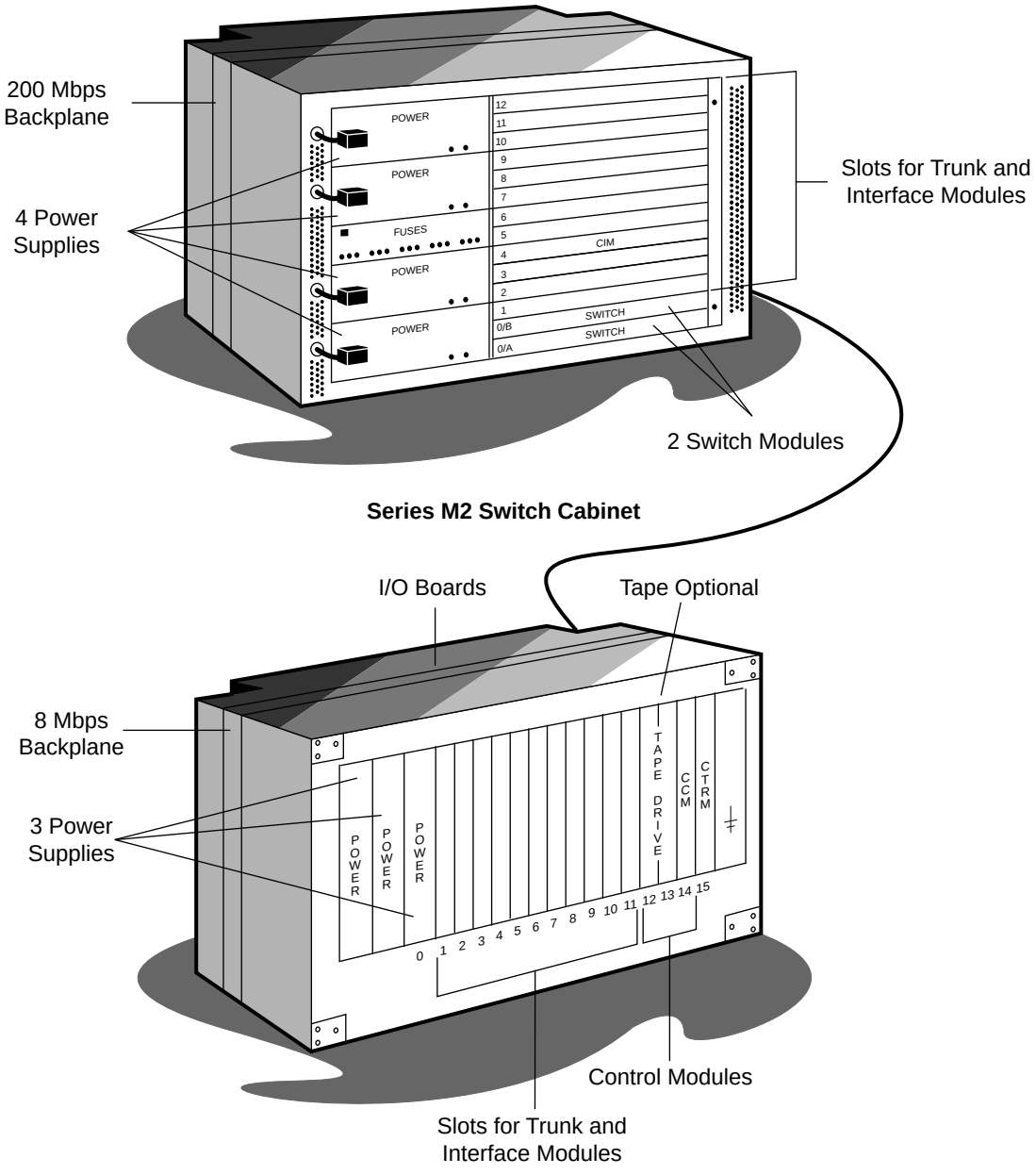

FIGURE 4-3. Basic Node: Functional Components

CO Frame

In CO installations, a node can have one or two stacks of cabinets with a maximum of four cabinets per stack. The cabinets are mounted in a frame that meets standard CO environmental requirements for earthquake and other protection. Panels cover the front and sides of the frame. An Alarm Relay Unit (ARU), which provides audible signals if the node fails, is mounted in the front of the CO frame. The ARU is connected to the Series M1 Control Cabinet.

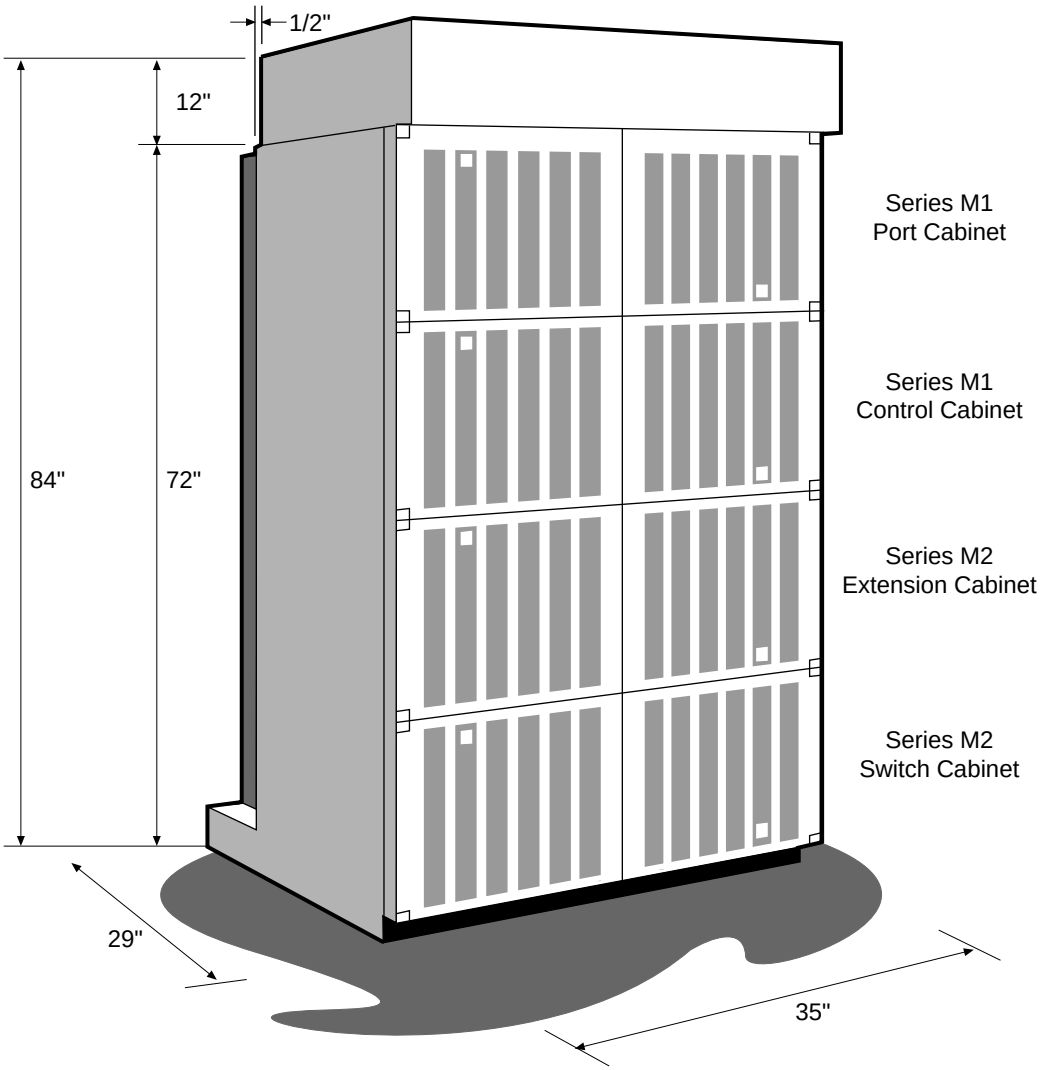

FIGURE 4-4. Central Office Frame Configuration: Front View

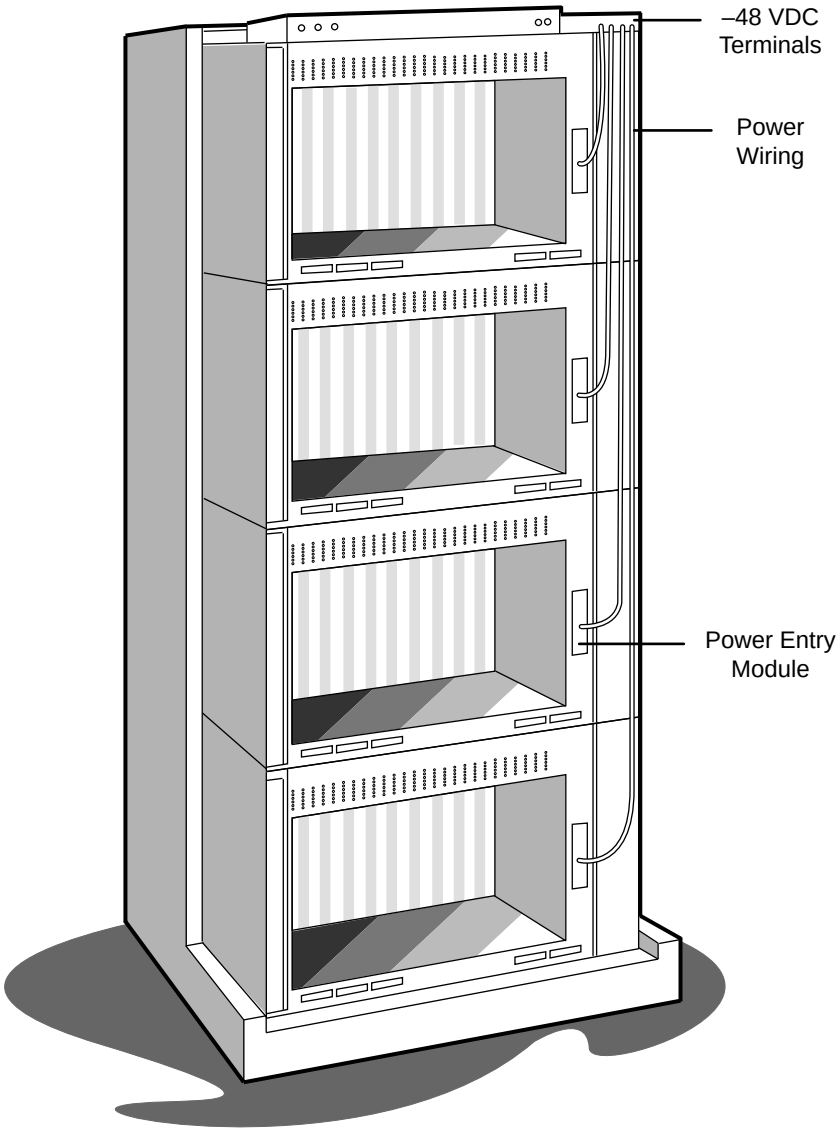

FIGURE 4-5. Central Office Frame Configuration: Rear View

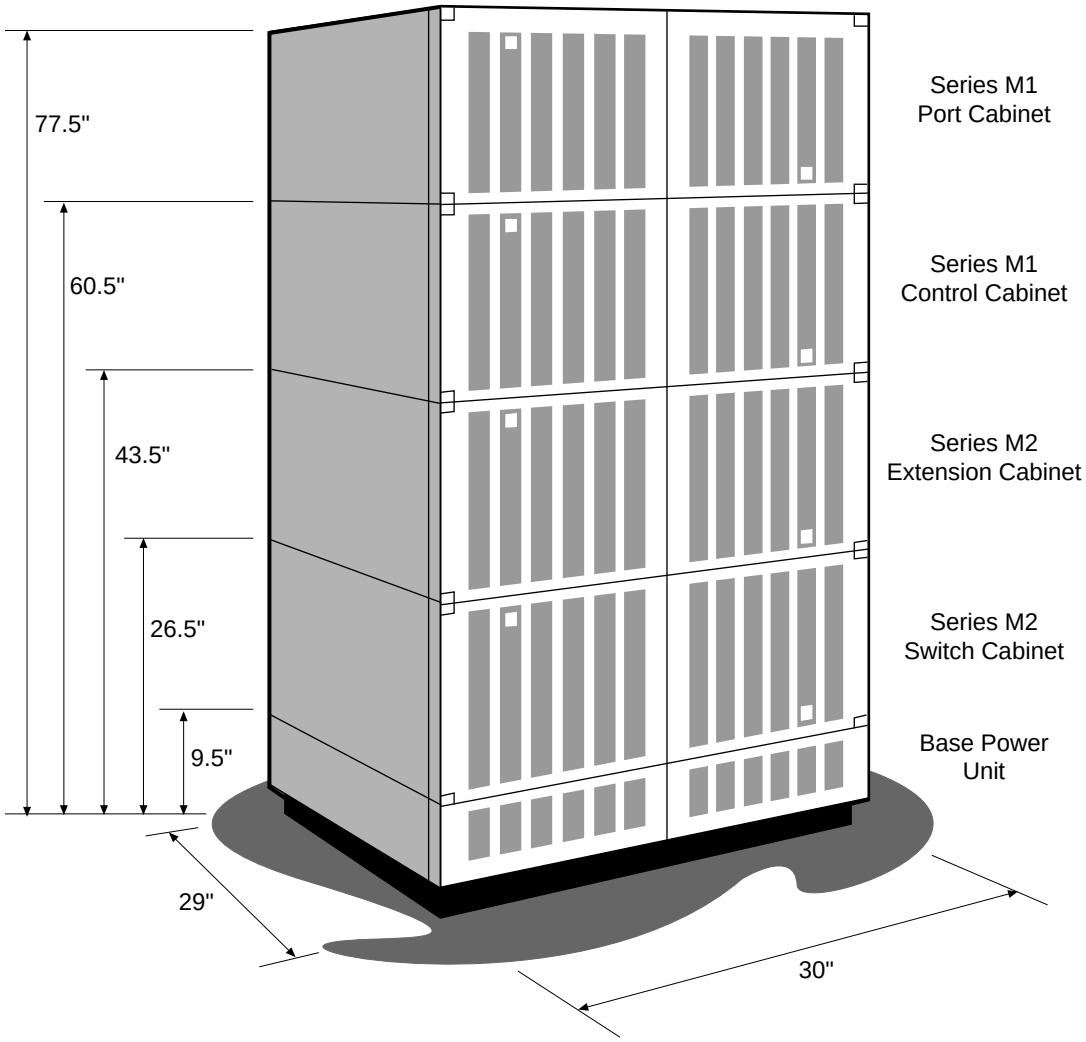

FIGURE 4-6. BNS-2000 Node Stack: Front View

Node Components

The components common to BNS-2000 nodes include the following:

- Series M2 Switch and Extension Cabinets
- Series M1 Control and Port Cabinets
- control modules
- power supplies and options, including the base power unit.

Series M2 Switch Cabinet

The data switching function of the node is managed by the Series M2 Switch Cabinet. The bus in the Switch Cabinet provides 216 Mbps (nominally described as 200 Mbps) of bandwidth for transport of variable length segments of data. The minimum segment size is 20 octets containing 12 octets of payload. The maximum segment size is 56 octets containing 48 octets of payload. The data rate is approximately 428,571 segments per second for the largest size segment.

The Series M2 Switch Cabinet has 12 horizontal physical slots available for interface and trunk modules. It includes the following:

- two Switch Modules
- an Intershelf Cable/Clock I/O board (ICCIOB), which provides an interface for up to three Series M2 Extension Cabinets
- a Clock to maintain facility synchronization (The Clock enables AI modules to be phase locked to the facility timing signal.)
- up to seven CIMs for fiber connections to CTRMs residing in Series M1 Control or Port Cabinets
- four power supplies.

Switch Module (CMA1)

For redundancy, two Switch modules are required in the Series M2 Switch Cabinet. Switch modules are supported in BNS-2000 Series M2 Cabinets only. These modules accept data segments from the other modules in the node, validate the integrity of each segment, and route the segments to the appropriate destinations.

For CONS traffic, packets originating in interface modules are formatted into segments and placed on the transmit bus. The segments contain the address of the originating module.

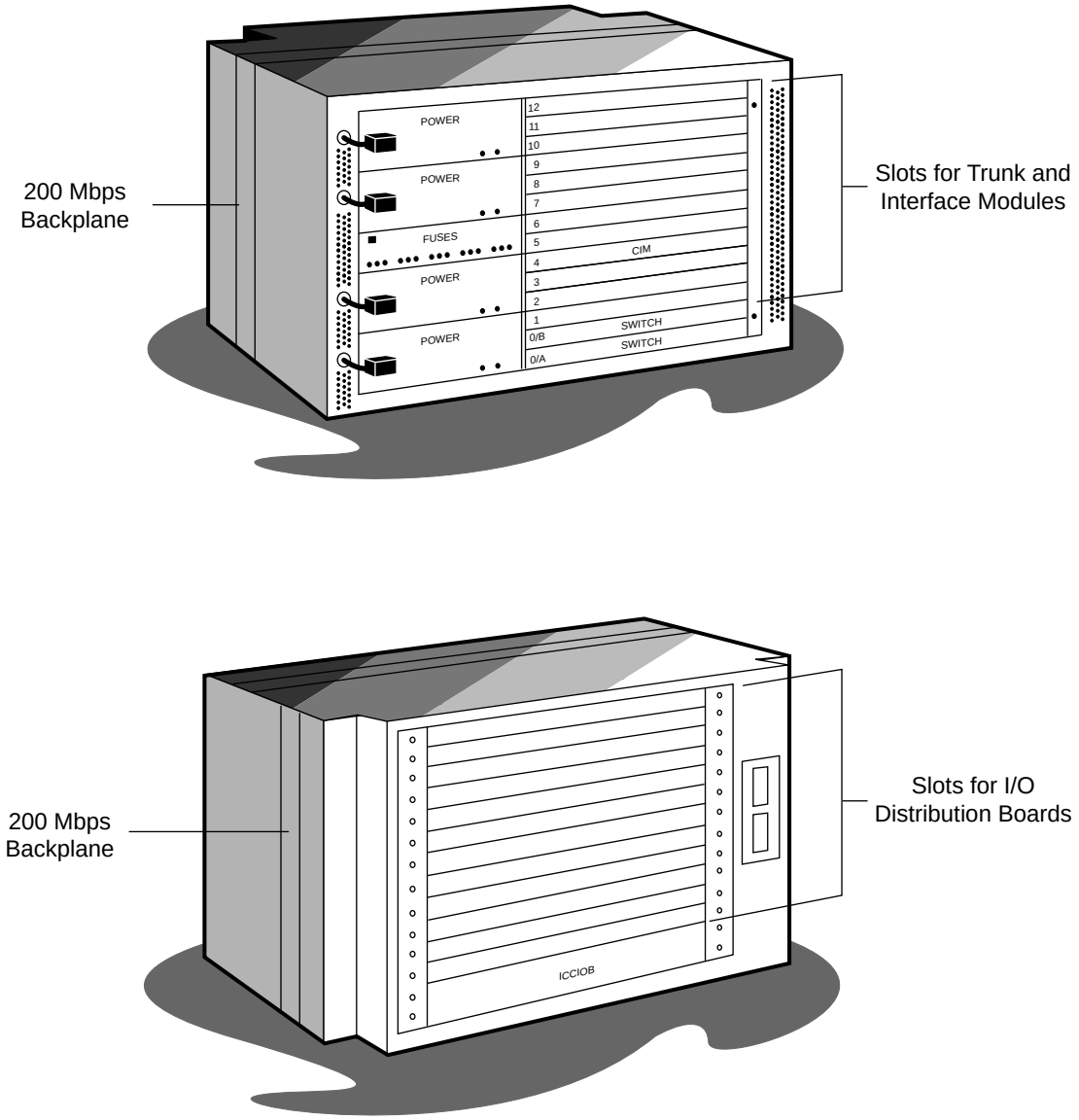

FIGURE 4-7. Series M2 Switch Cabinet: Front and Rear Views

The Switch module switches the segments by exchanging the address of the origin for the destination interface address. The re-addressed segments emerge from the Switch module on the broadcast bus, where they are received by the destination interface module.

The Switch module control memory contains information about all existing virtual circuits. This memory is updated by the Control Computer whenever virtual circuits are connected or disconnected.

The Switch contains 64 kilobytes of random access memory (RAM), enough capacity to support 30,000 endpoints (15,000 virtual circuits).

Error reporting features of the Switch module simplify the task of isolating faults within a node. The Switch module can capture the source address (module and channel number) of any segment causing an error. This source address is reported in the Switch module's status packet, ultimately allowing the network administrator to isolate a module that is generating bad packets or segments.

The Switch module detects and properly handles parity errors. It can also detect packet count rollovers.

Both Switch modules are placed in shelf zero (0), in physical slots A and B. The Control Computer can issue commands to the Switch modules either collectively over a common command channel, or individually over individual command channels.

While only one Switch module is active at a time, the standby Switch module shadows the active Switch. During normal operation the routing memory in both Switch modules will be identical. The Control Computer has the capability to set which Switch module is active and which is standby. The Control Computer also has the capability to monitor the sanity and integrity of the standby Switch module. This monitoring ensures that the standby Switch module is ready to participate in an automatic recovery from failure of the active Switch module.

The Switch module requires an ICCIOB (CNA1) and a Status I/O board (CMC3). The second Switch module requires no additional I/O board.

Stratum 4 Clock (CMC3)

The Stratum 4 Clock (SSM4) provides Data Signal 1 (DS1) synchronization for the primary and secondary timing references on a node supporting SMDS modules and/or M2 Frame Relay modules. The SSM4 function is provided by the CMC3 I/O board located at the rear of the node in physical slot 2 (logical slot 0/B). The CMC3 also provides status reports, for example, power supply failure, fan failure, or high temperature, for the Series M2 Shelves.

CIM (CMA2)

The Series M2 Switch Cabinet can contain up to seven CIMs for fiber connections to CTRMs residing in 8 Mbps Series M1 Control or Port Cabinets. The CIM provides an interface between Series M1 and M2 Cabinets. Each CIM in the Switch Cabinet requires a CMC2 I/O board.

Series M2 Extension Cabinet

Identical hardware assemblies are used for the Series M2 Switch Cabinet and the Series M2 Extension Cabinet. The Series M2 Extension Cabinet provides space for additional high-speed interface modules. It includes four power supply modules and has 14 horizontal physical slots. An Extension Shelf Cable/Clock I/O distribution board (ECCIOB) (CNA2) in slot A provides connectivity with the Switch Cabinet. The front of slot A remains empty in the Series M2 Extension Cabinet. The 13 remaining physical slots are available for high-speed interface and trunk modules.

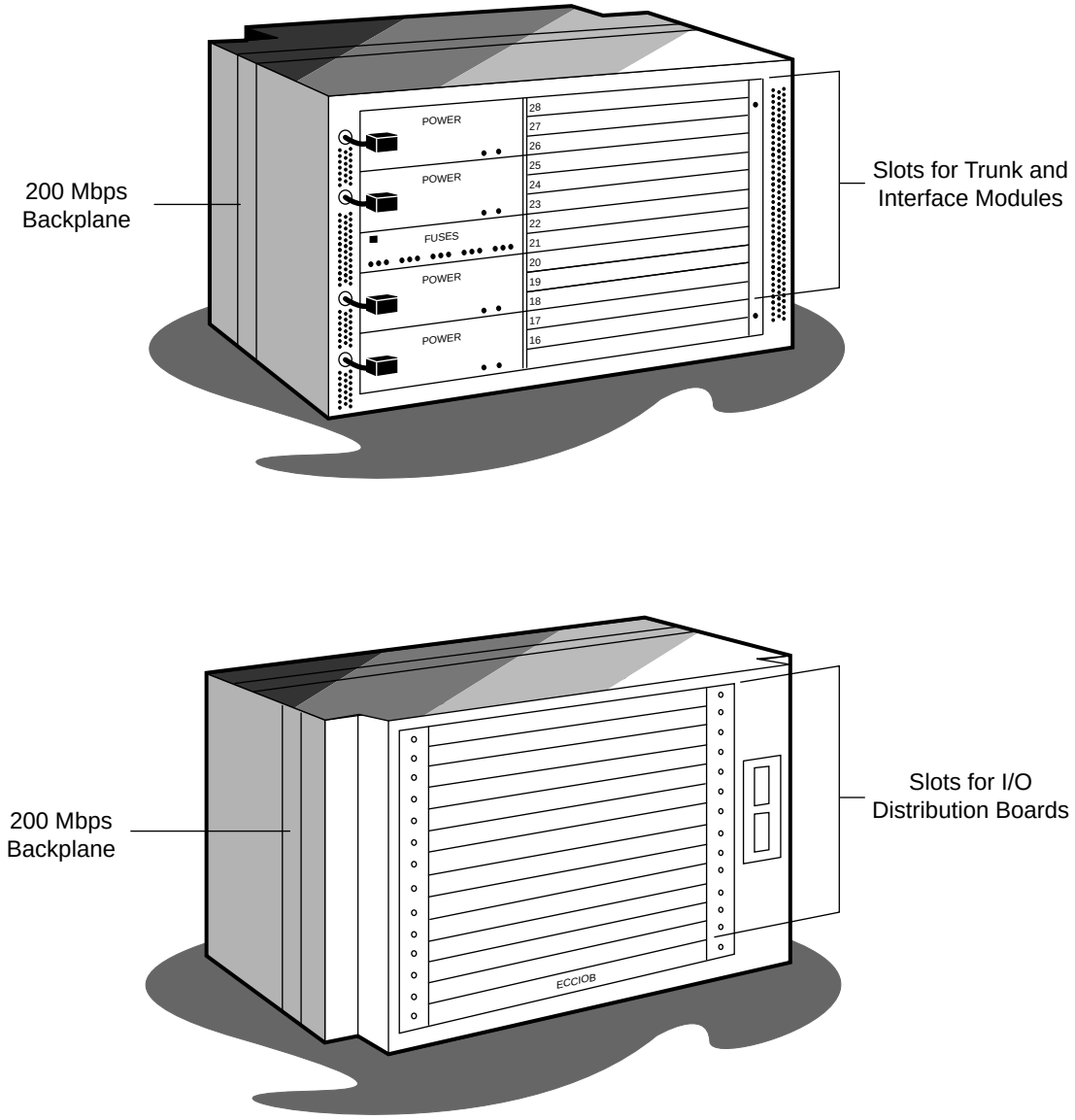

FIGURE 4-8. Series M2 Extension Cabinet: Front and Rear Views

Series M1 Control Cabinet

The Series M1 Control Cabinet contains critical modules for node functions. A node must contain at least one Series M1 Control Cabinet. One of the two Control Computer configurations in the following section must be used for the Control Cabinet.

Configurations

The following two configurations of Control Computer equipment are currently available:

- The ***Control Computer Module (CCM)*** configuration consists of a single-slot module that provides the functions of the Central Processor Unit, a dual Small Computer System Interface (SCSI), a disk drive, and an optional Maintenance and Redundancy Controller Input/Output (MRCIO). CCM configurations can have either one internal or one external tape drive per node.
- The ***Enhanced Central Processing Unit (ECPU)*** configuration consists of a multi-module system that provides the functions of the Central Processor Unit, a dual SCSI and controller, a Maintenance and Redundancy Control Module (MRCM), and a disk and tape drive subsystem on separate module and input/output boards.

CCM Configuration

The CCM configuration includes the single board CCM and separate, optional Digital Data Storage functionality. The CCM performs administrative and maintenance functions, monitors the network, and sends reports and alarms to the system console and printer. A CCM configuration consists of:

- CCM module
- Either:
  - MRCIO (if using MRC functionality)
  - Controller I/O (if not using MRC functionality)

Additional optional components include:

- Internal tape drive:
  - Digital Data Storage (DDS) Tape Module
  - Digital Data Storage (DDS) Tape I/O
- External Digital Data Storage (DDS) Tape Drive

Figure 4-9 illustrates a typical CCM configuration.

CCM (TN2235). The CCM is a Motorola 68060 Microprocessor-based design that incorporates RAM memory, a disk drive, dual SCSI interfaces, and a backplane interface (DKI) into a single-slot circuit pack.

MRCIO (CTS1). The Maintenance and Redundancy Control Input/Output (MRCIO) replaces the MRCM module and companion I/O board of earlier BNS-2000 releases. The MRCIO is used behind a CCM to provide redundant controller and/or remote maintenance capabilities.

The MRCIO monitors the operational state of the Control Computer(s) in the node and sees that the network continues to function if a critical component of the Control Computer fails. It takes

power only from the backplane — it does not access the bus.

For high availability nodes — nodes that contain two Control Computers designated as active and standby — the MRCIO monitors the status of both Control Computers and determines which Control Computer is active at any given time. If the active Control Computer fails, the MRCIO performs an automatic recovery that can result in a switchover to the standby Control Computer or, simply, a reset of the active Control Computer.

For simplex nodes having only one Control Computer, the MRCIO provides remote access via the MRCIO maintenance port when the active Control Computer can be accessed to reboot, debug, and provide a backup connection from a remote location. This feature is also supported for nodes configured with the high availability option.

A two-character attention signal — preset to Escape Escape — allows the network administrator to toggle between the MRC command mode and the Control Computer connect mode. While in MRC command mode, the network administrator can communicate directly with the module via a special command set. These commands are contained in the *Commands Reference.* Additional information about administration and diagnostics via the MRCIO are contained in the *Node Reference*.

Controller I/O (CTS2). The Controller I/O is used behind a CCM to provide I/O connectivity for a simplex controller configuration without remote maintenance capabilities. It can also be used behind the second controller in a redundant controller configuration.

Digital Data Storage (DDS) Tape Module (TN2233). The DDS module replaces the existing 40MB tape drive (TN2097). It provides higher data capacity and allows a transition to a newer media (DDS) technology. The TN2233 tape module requires two backplane slots, and must be used with the CSD9 I/O board.

Digital Data Storage (DDS) Tape I/O (CSD9). The DDS Tape I/O is required when using the TN2233 DDS Tape Module. This board is also compatible with the 40MB TN2097 Tape Module to facilitate node upgrades to BNS-2000 Release 4.0.

Stand-Alone Digital Data Storage (DDS) Tape Drive. The Stand-Alone DDS Tape Drive is a portable, AC-powered DDS with a SCSI interface to the CCM controller complex. The stand-alone DDS configuration allows software to be downloaded to the controller without using a resident tape drive, thus freeing up two slots in the controller cabinet.

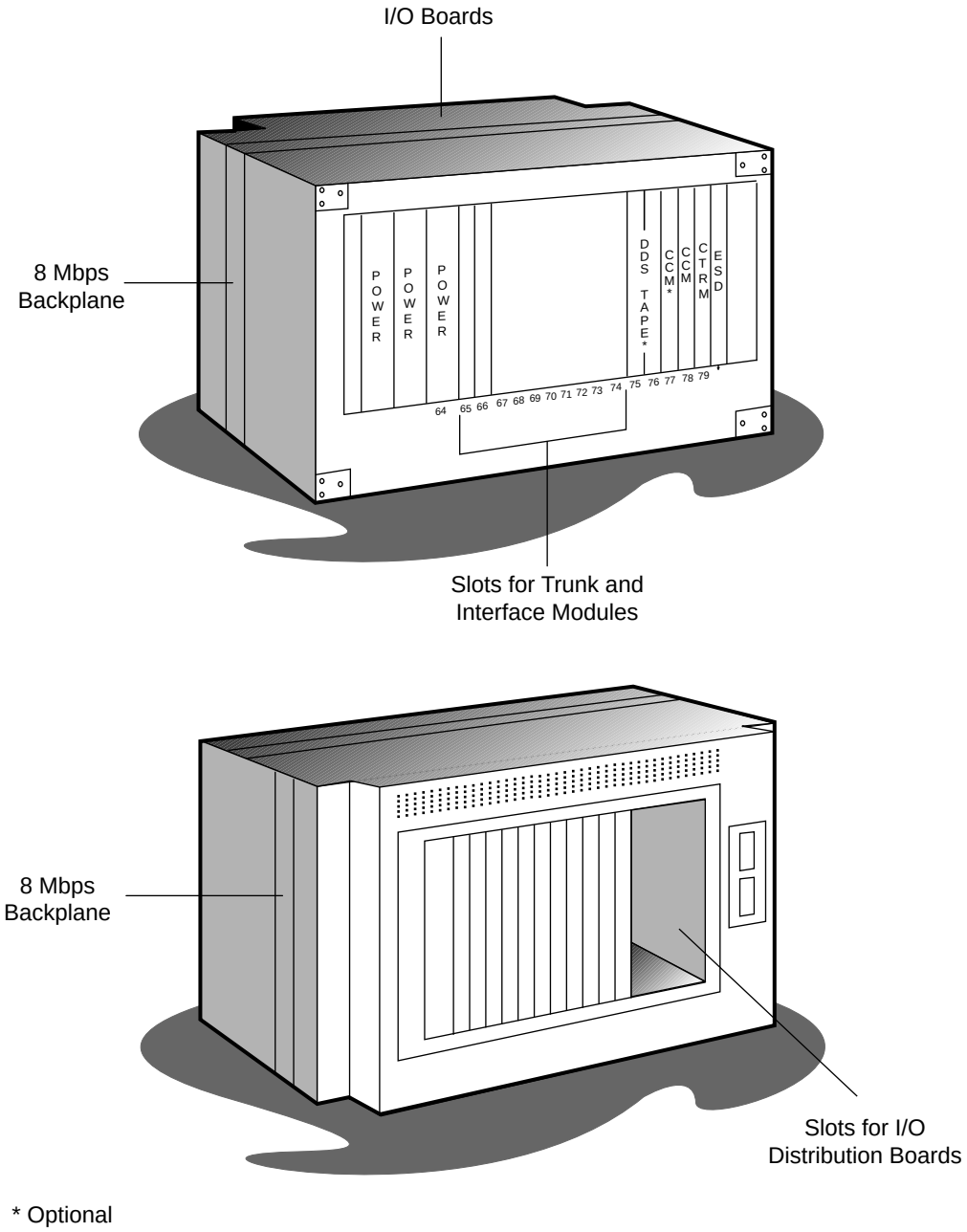

FIGURE 4-9. Series M1 Control Cabinet: Typical CCM Configuration

ECPU Configuration

The ECPU configuration consists of a multi-board complex. It performs administrative and maintenance functions, monitors the network, and sends reports and alarms to the system console and printer. An ECPU configuration includes the following components:

- Enhanced Central Processing Unit (ECPU)
- SCSI/DKI backplane interface
- Fixed Disk/Tape Subsystem
- MRCM

Figure 4-10 illustrates a typical ECPU configuration.

ECPU (MC1D138A-1). The ECPU is a single-board processor that monitors and controls operation of all other control modules and interface modules. It provides two ports for administrative interfaces to the node. The ECPU module is built on a 32-bit microprocessor, and contains 32 megabytes of on-board RAM. The ECPU uses an AWJ15 I/O board.

SCSI/DKI (UN635B). The SCSI/DKI is a single board that provides interfaces to both the SCSI bus and the backplane. The DKI functionality provides the interface between the ECPU and the backplane. The primary SCSI functionality provides the interface between the ECPU and the disk/tape unit. In a dual Control Computer configuration, the secondary SCSI functionality provides the interface between this ECPU and the disk/tape unit of the redundant Control Computer complex. The SCSI/DKI uses an ASP4B I/O board.

Fixed Disk/Tape Subsystem (TN2175B/TN2097). The Fixed Disk/Tape Subsystem consists of two boards. BNS-2000 Release 4.0 requires the TN2175B disk which contains the disk drive mechanism for booting the system. It also contains the network configuration database and operating software for the control complex. The disk drive uses an AWJ12 I/O board.

A streaming tape (TN2097) drive unit is used as a backup device. Software releases are distributed on tape. The tape unit is used to install the software on the fixed disk. The ASP8 I/O distribution board is used with the tape.

MRCM (TN2109C). The Maintenance and Redundancy Control Module (MRCM) is an intelligent single-board module that monitors the operational state of the Control Computer(s) in the node and sees that the network continues to function if a critical component of the Control Computer fails. It takes power only from the backplane — it does not access the bus.

For high availability nodes — nodes that contain two Control Computers designated as active and standby — the MRCM monitors the status of both Control Computers and determines which Control Computer is active at any given time. If the active Control Computer fails, the MRCM performs an automatic recovery that can result in a switchover to the standby Control Computer or, simply, a reset of the active Control Computer.

For simplex nodes having only one Control Computer, the MRCM provides remote access via the MRCM maintenance port when the active Control Computer can be accessed to reboot, debug, and provide a backup connection from a remote location. This feature is also supported for nodes

configured with the high availability option.

The following ports are available on the MRCM:

- *Seven EIA RS-232-C ports* — Of the seven EIA RS-232-C ports, three are workstation ports and four are Control Computer interface ports, or CCIO ports. The four CCIO ports connect with the A and B ports of the active and standby Control Computers, respectively. The three workstation ports — A, B, and M — are those ports to which data terminal equipment can be connected for direct communication with the MRCM or Control Computer. The workstation A port is typically connected to the local console. The workstation B port can be connected to a printer or it can be connected to a remote console for access via *StarKeeper* NMS. The workstation M port (the maintenance port) can be used to access the local workstation, the MRCM monitor directly, or the active or standby Control Computer remotely. The MRCM can be connected to a modem for remote access to the MRCM.
- *Two R ports* — The R ports provide signals to and from the MRCM and both Control Computers about the status of the Control Computers. The MRCM may send signals to reset any or both Control Computers over these ports.
- *One S port* — The S port provides an interface for status signals to the Clock module or Repeater module. The status signals ensure that the states of unused environmental alarms will be reported in the Clock module's or Repeater module's (whichever is in slot 31) status packet. The two signals sent via this port show that the MRCM is sane and that the state of the standby Control Computer is in-service or rebooting.

A two-character attention signal — preset to Escape Escape — allows the network administrator to toggle between the MRC command mode and the Control Computer connect mode. While in MRC command mode, the network administrator can communicate directly with the module via a special command set. These commands are contained in the *Commands Reference.* Additional information about administration and diagnostics via the MRCM are contained in the *Node Reference*. The I/O distribution board used with the MRCM is the AWJ16B.

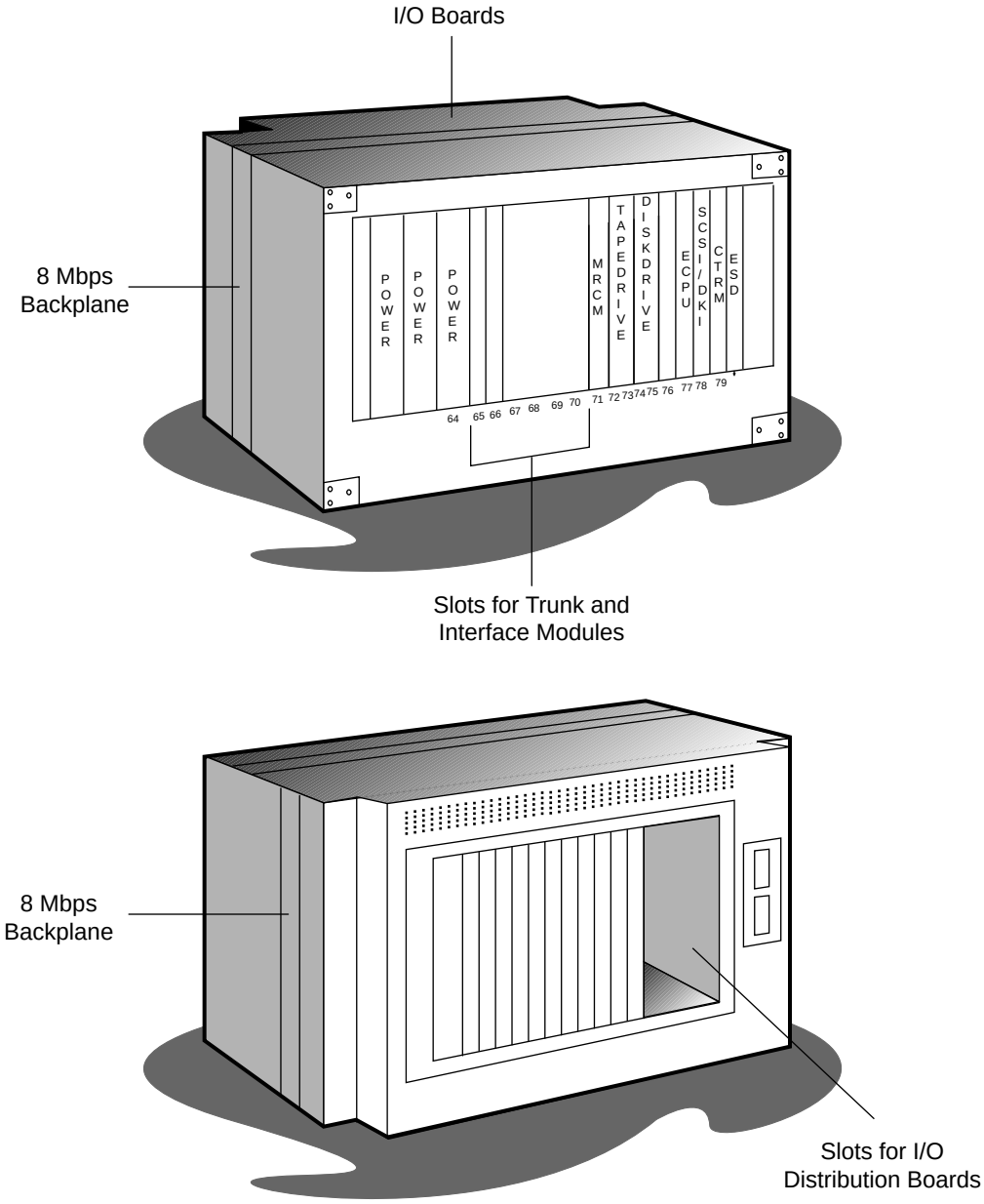

FIGURE 4-10. Series M1 Control Cabinet: Typical ECPU Configuration

Additional Control Modules

In addition to the modules that make up the Control Computer complex, two control modules are essential to full functionality of the BNS-2000 node: the MRC function and the CTRM.

CTRM (TN2096). A CTRM resides in each Series M1 Control or Port Cabinet and provides fiber interconnection between the Series M1 Cabinet and the Series M2 Switch Cabinet. Each CTRM is connected to a CIM in the Series M2 Switch Cabinet. The CTRM must always be in the highest active slot in the cabinet in which it resides, because the Control Computer will not activate for service any module placed above it. The module, which includes an internal repeater function, generates timing signals for the cabinet, polls each module in the cabinet for status, and reports the hardware status of each cabinet. The CTRM is a critical module; if it fails, the cabinet in which it resides also fails. The module uses an ASP7 I/O board.

Configuration of Control Components

For greater reliability, redundant control components are recommended. The possible Control Computer configurations are

- *Single Control Computer* — The minimal requirement for a node is one Control Computer. An MRC function is optional with this basic Control Computer configuration. The Control Computer complex can be installed in any Series M1 cabinet.
- *Dual Control Computer* — For nodes optioned with high availability, the basic configuration is backed up by a redundant basic configuration: two Control Computer configurations. In a typical configuration, one Control Computer configuration resides in any Series M1 cabinet, and the second interconnected Control Computer configuration resides in the next higher-numbered cabinet. For a CCM only, both Control Computer systems can reside in the same Series M1 cabinet. An MRC function, which ensures that one Control Computer is active and one is standby, is required in the lower-numbered cabinet or slot.

Hardware Redundancy

BNS-2000 hardware redundancy ensures network reliability and availability. Availability is normally calculated using the following two performance measurements:

- ***Mean Time Between Failures (MTBF)*** is the average time that a component can function before a hardware failure occurs. For a BNS-2000 node, the MTBF is about seven months.
- ***Mean Time To Repair (MTTR)*** is the time it takes an operator to repair a service-disrupting failure. For a BNS-2000 node, the time required to replace the backplane bus is two and one-half hours. All other common equipment and interface modules can be replaced in one-half hour.

Availability is based on the MTBF and MTTR figures, and is a function of the rate of occurrence of failure and the duration of repair time. A redundant Switch module is standard. Overall reliability and availability can be further increased by adding an optional redundant Control Computer.

Control Computer Availability

Availability of access to operations, administration, and maintenance (OA&M) functions is based on availability of the Control Computer.

The availability of a Control Computer is approximately 99.998%. This equates to 11 minutes of downtime per year. With the redundant option, availability of the Control Computer increases to greater than 99.999%.

Automatic recovery is available for redundant Control Computers. The automatic recovery option uses active and standby Control Computers monitored and controlled by an MRC function. The standby Control Computer contains a backup copy of the configuration database. The MRC function monitors the two Control Computers for sanity, and determines whether their status is active or standby. The MRC function can detect a problem in the active Control Computer in 15 seconds or less. When a problem is detected and the recovery option is set to *on*, the MRC function initiates the automatic recovery. It switches the status of the active and standby Control Computers and resets them, resulting in a warm reboot of the node. During the warm reboot, calls in progress are not affected; new calls can be placed and existing calls can be taken down after the warm reboot is completed.

Switch Module Availability

The redundant Switch module provides network reliability through a capability to recover from a failure of the active Switch module. This configuration includes two Switch modules in the Series M2 Switch Cabinet. The Control Computer issues commands to both Switch modules collectively over a common command channel, or individually over separate command channels. During normal operation one Switch module is recognized by the Control Computer as the in-service active Switch module, which functions as the node's switching mechanism, forwarding packets between addresses stored in its memory. The other Switch module is recognized by the Control Computer as the in-service standby. The standby Switch module shadows the active Switch module, so that during normal operation the routing memory in both Switch modules is identical. If the in-service active Switch module fails, a quick switchover with no data loss occurs. Availability of a single Switch module is greater than 99.999%. With the standard redundant configuration, both Switches must fail for service to be disrupted. This effectively results in 100% availability of the Switch.

Manual switchover can be accomplished as long as the standby Switch module responds to status and sanity polling and is in service. The network administrator initiates a command to make it the active Switch module.

Automatic switchover is accomplished by the Control Computer. The Control Computer monitors the health of both Switch modules to ensure that a successful recovery can be initiated if needed. Polling establishes the status and the existence of any detected errors for each Switch module, while also checking that the memory for both Switch modules is synchronized. Irregular conditions reported in the status packets of the active Switch module will cause the Control Computer to deactivate the active Switch module and automatically initiate a command to bring the standby Switch module to active status if the standby Switch module is in service. Unless there is a simultaneous problem with the standby Switch module which prevents it from participating in the switchover, the switchover is completed and a message is generated to

indicate the success of the recovery.

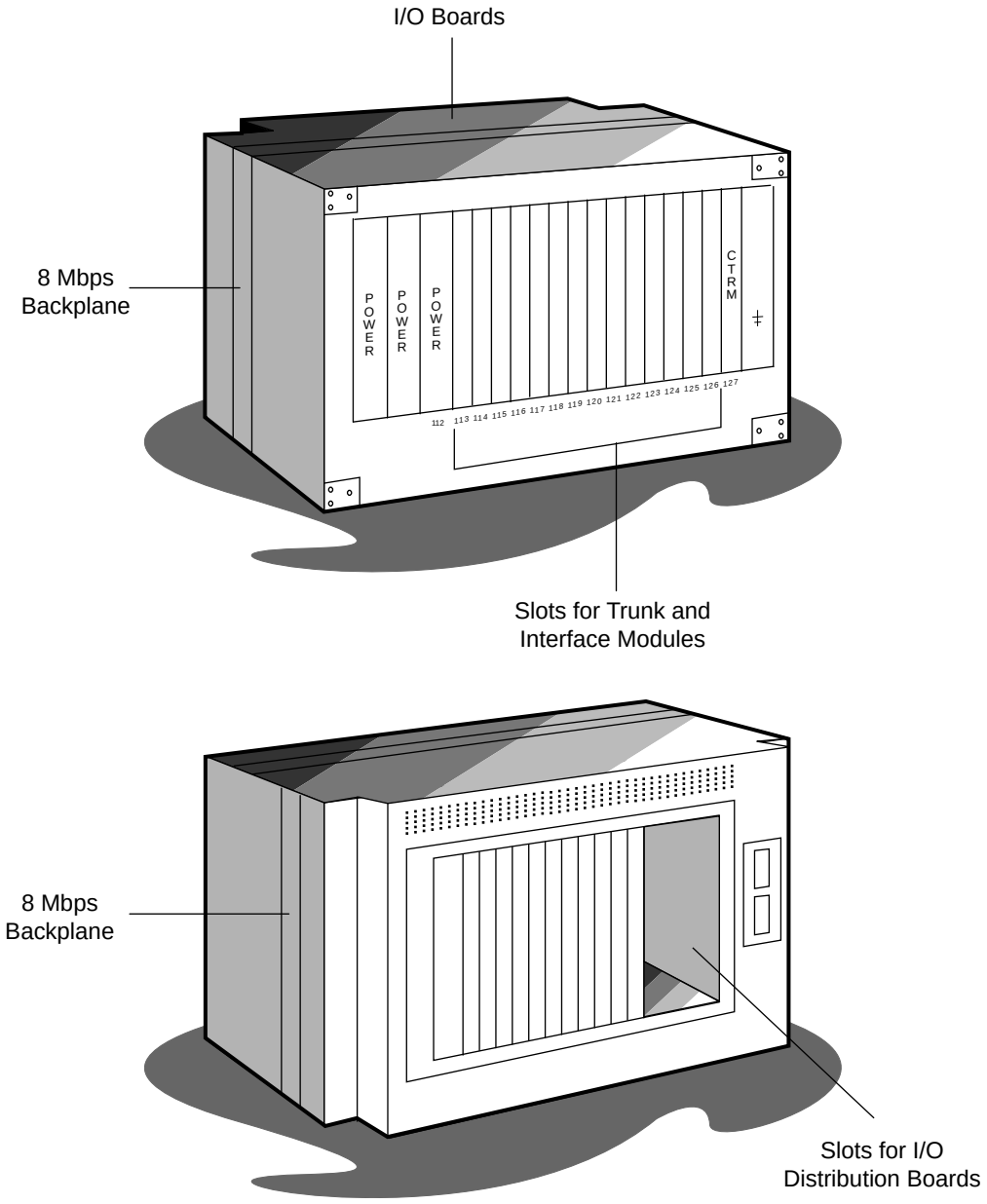

FIGURE 4-11. Series M1 Port Cabinet: Front and Rear Views

Series M1 Port Cabinet

When the number of interface and trunk modules required for connection-oriented services exceeds the number of slots available in the Series M1 Control Cabinet, a Series M1 Port Cabinet can be added. Up to six Series M1 Port Cabinets can be added to a node within the overall eight cabinet limit. Like the Series M1 Control Cabinet, each Series M1 Port Cabinet has 16 slots. A CTRM, which provides the connection to the Series M2 Switch Cabinet, must be installed in the highest slot address of the cabinet. The third power supply is installed in slot 0. The remaining 14 slots are available for interface and trunk modules.

Slot Numbering Scheme

The illustration shows the slot numbering scheme in a fully configured, multicabinet node. These logical slot numbers are the basis for the addressing scheme that allows either Control Computer to recognize the location of network components. Note that in shelf 0 one Switch module plugs into physical slot 1 and reports its location as logical address A. The second Switch module plugs into physical slot 2 and reports its address as B. The remaining slots in shelf 0 are addressable as logical slots 1 through 12. Logical addresses 13 through 15 do not exist.

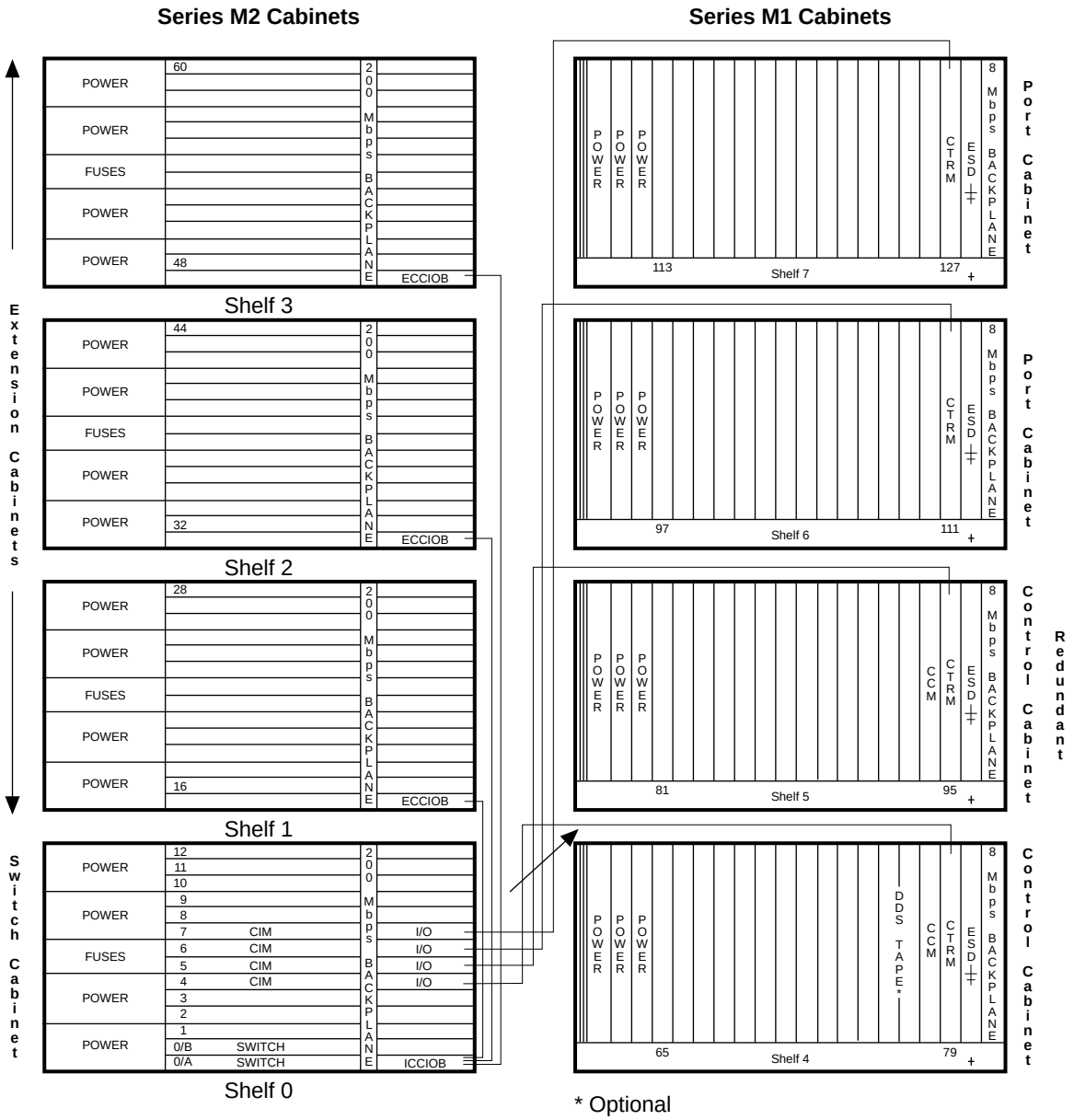

FIGURE 4-12. Slot Numbering Scheme

Bus Architecture and Segment Routing

The high-speed 200 Mbps bus system is designed to support the cell relay standard. It is used as the basic building block of the Series M2 Switch complex. It provides an aggregate throughput of 200 Mbps for the modules that reside on the bus.

The bus system is composed of four bus subsystems as follows:

- ***Contention Bus (CBUS)*** is a common bus between all modules in the Switch Cabinet. It provides the method for the modules to contend for access to the TBUS. The CBUS supports eight levels of priority contention with group arbitration (round-robin service) within each level.
- ***Transmit Bus (TBUS)*** is a common bus between all modules in the Switch Cabinet. It provides the method for source endpoints to send segments to the Switch module for routing to the destination endpoint. The Switch module receives all segments from the TTBUS.
- ***Broadcast Bus (FBUS)*** is a common bus between all modules on the switching complex. It provides the method for the destination endpoint to accept segments from the Switch module after they have their routing information changed. The Switch module transmits all segments on to the FBUS. All modules except the Switch module receive segments from the FBUS.
- ***Total Transmit Bus (TTBUS)*** is a 36-bit parallel bus that combines TBUS data from all high-speed buses. The high-speed bus system is a synchronous bus system that provides the contention mechanism for each segment time slot. Each segment time slot provides for transmission of a single, variable length (up to the limit of the cell size) segment to the Switch module. All network end devices are connected to specialized interface modules. The interface modules reside in Series M1 or M2 Cabinets that are in turn connected to the high-speed backplane of the BNS-2000 node. Each module contends for a segment time slot based on a priority level that is controlled by its contention priority, its group contention state, and its module address. All modules that have a segment to transmit contend simultaneously for the TBUS with only a single module gaining access for each segment time slot. The modules that lose contention will defer transmission and contend for the TBUS on the subsequent segment time slot. The module that wins contention will transmit its segment on the TBUS with its own module address and a destination channel number.

  The system distinguishes between connection-oriented and connectionless segments by checking the protocol identification (ID) field of the header of each segment. This indicates the type of traffic the segment is carrying.

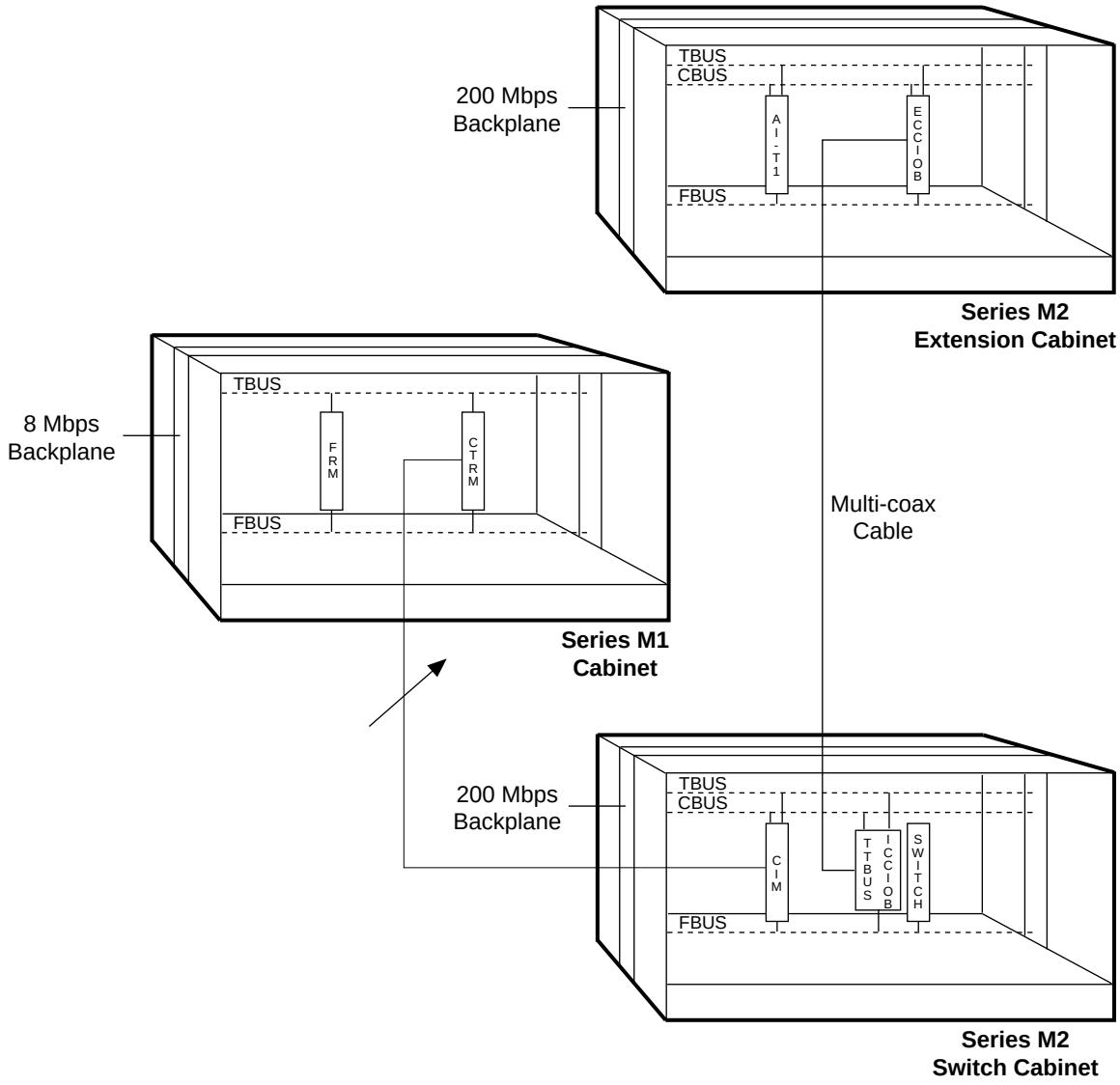

FIGURE 4-13. Bus System: Functional Diagram

Connection-oriented Service

For connection-oriented data segments, a virtual circuit between source and destination endpoints has been set up by the node Control Computer. This information is stored in Switch module memory. Upon receipt of each segment, and prior to routing each segment, the Switch module validates the segment header and changes the origination address to the destination address.

Upon routing the segment by changing the segment address, the Switch module transmits the segment on the FBUS. The segment is received simultaneously on the FBUS by all the modules on the switching complex. Only the matching destination module accepts the segment.

Connectionless Service

For connectionless service there is no virtual circuit. The source module places the segment on the TBUS with its address as the origination address. Upon receipt of a connectionless segment, the Switch module changes the origination module address to a special connectionless service destination module address, and places the segment on the FBUS.

The connectionless service destination module address is a special, reserved module number. The same reserved destination module address is used for all connectionless traffic, regardless of the intended destination. The connectionless group address is the equivalent of a common broadcast address to a connectionless network interface module on the node.

All connectionless modules pick up the segment on the FBUS with the special reserved connectionless destination module address and perform the next level of destination address matching by examining the data field.

Inside the connectionless data unit are fields indicating the source and destination E.164 addresses for the data unit. The receiving module screens the connectionless segment based on the E.164 address in the segment. If the connectionless module is responsible for routing the E.164 address, it will deliver the segment. Otherwise, the segment will be discarded by this connectionless module. This process is cyclic and repeated every contention period. Since the bus is synchronous, it can be 100% utilized with no loss of bandwidth resulting from contention collisions.

Error Detection

Several forms of error detection are used in BNS-2000, depending on the type of interface module to which a communicating device is connected. The undetected error rate in the network will typically be one undetected error in 10^{14} bits transmitted. A segment in which an error is detected is simply discarded, and protocols in the network or at a higher level request retransmission.

The Switch module makes error detection and reporting possible on nodes. The Switch module provides capabilities that simplify the task of isolating faults within a node by capturing the source module number and channel number of any segment that causes an error. This source address is reported in the Switch status segment, ultimately allowing the network administrator to isolate a module that is generating bad segments. The Switch module monitors the parity of every octet it receives on the TBUS and verifies the segment.

The Switch also provides the capability to inhibit the control function of any command segment received that has a detected parity error. This prevents erroneous segments from accessing the control functions of the Switch module.

The Switch module's normal response to a detected error is to discard the erroneous segment and report the error type and its possible source. When an error occurs during a testing cycle, a command segment read of the RAM control memory, a segment count increment cycle, or a

hardware audit, the errors are reported but the segment is not discarded.

The Switch module also provides the ability to detect and report when the segment count for calls of long duration rolls over (returns to zero after reaching the maximum).

Resource Capacities

See the *Planning Guide* for node and network planning and engineering guidelines.

Power Supplies and Options

BNS-2000 offers various power arrangements, based on modular units that provide power for all possible system configurations. These arrangements include redundant supplies. Additional power options are available with the base power unit, which is used in AC-powered installations only. The –48 VDC CO frame has its own power arrangements.

Each shelf in a BNS-2000 Series M1 or Series M2 Cabinet has a power entry module that connects the input power to the shelf wiring. This wiring distributes the power to the power supplies in each shelf.

Power Entry Modules

Power entry module are provided on each shelf to converts input power to the +5, +12, and –12 VDC needed to operate modules housed in the cabinet. There are four types of power entry modules for:

- AC-powered Series M2 Shelves
- AC-powered Series M1 Shelves
- DC-powered Series M2 Shelves
- DC-powered Series M1 Shelves.

Each Series M1 Control and Port Cabinet comes with two primary power supply units and a third redundant power supply. Each Series M2 Switch and Extension Cabinet comes with three primary power supply units and a fourth redundant power supply.

Alarm Relay Unit (ARU)

The ARU is used only in the CO frame to provide connection to audible critical alarms through alarm relay contacts. This alarm unit is mounted in the top of frame 0 (the frame containing a Control Cabinet).

Base Power Unit

In AC-powered installations, a base power unit is required. It provides power for four Series M1 or M2 Cabinets. The unit is equipped with casters and leveling feet, and has the following options:

- ***AC distribution (ACD) system*** provides AC power distribution and double-pole circuit breakers for each cabinet. It is available for 200 to 240 VAC only. Distribution cords attach the ACD System to modular cabinets equipped with power entry modules.
- ***Battery backup unit*** provides power distribution and double-pole circuit breakers for each cabinet. This unit accepts power of 200 to 240 VAC.

  Sealed lead-acid batteries in the base power unit supply power to the node if electrical service fails. The batteries ensure an uninterrupted power supply for a minimum of three minutes. A battery charger unit keeps the battery charged.

CO Frame Power

The CO frame includes an interface to distribute −48/−60 VDC power via wiring to the power entry modules on each Series M1 or M2 Cabinet. It also provides a means to terminate the frame ground, and an overhead cable rack to support power cables.

The −48/−60 VDC CO power is connected to a terminal strip on the top of the CO frame. Individual branch connections and circuit breakers for each installed cabinet are provided and terminate in the Series M1 or M2 Cabinet's power entry module.

Concentrators

Concentrators provide an extension to the node backplane. They are physically connected to the node through links provided by trunk modules in the node and corresponding link modules in the concentrators. In some cases, the same type of module that provides a trunk between nodes can be used in a concentrator to provide a link to the node, hence the reference to trunk/link modules. BNS-2000 provides fault tolerance from facility failures for concentrator links by providing an administrable link timer parameter. This strategy allows ample time for outboard devices, such as call back modems, etc., to reestablish connections between the node and concentrator over alternate routes if the primary link facility fails.

Concentrators contain slots for interface modules for user services and operate by multiplexing user data over the link to the home node. They also extend the distribution limit of network interfaces beyond conventional connection distances. Concentrators cannot network with other nodes and concentrators, i.e., links are supported only between a concentrator and its home node, not between two concentrators.

Concentrator selection is based on such factors as distance between the concentrator and node, services required at the concentrator site, and number and type of connections required. BNS-2000 supports the following three families of concentrators:

- ***Multipurpose Concentrators (MPCs)*** support most of the services available in the node through a subset of the interface modules that can be placed in the node. User connections to the concentrators are through ports located on these interface modules. Both fiber and wire links are supported between Multipurpose Concentrators and the home node. There are two versions: the MPC15, a 15-slot version, and the MPC7, a seven-slot version.
- ***Synchronous/Asynchronous Multiplexers (SAMs)*** come in 504-, 64-, and 16-port versions and support EIA RS-232-C synchronous transport and/or switched asynchronous connections, administrable on a per port basis. The SAM504 and SAM64 can be linked to the home node by either fiber or wire facilities, with a wire dual link provided for the SAM64 only. An integrated wire link is provided for the SAM16.

More information on each type of concentrator follows.

Multipurpose Concentrators

Multipurpose Concentrators are remotely located cabinets that support all connection-oriented services supported by the node. The services supported include the following:

- asynchronous communications
- synchronous transport services
- X.25 and X.75 services
- LAN interconnect services
- special purpose services.

The following two Multipurpose Concentrators are available:

- The MPC15 is a 15-slot version capable of supporting up to 12 interface modules
- The MPC7 is a seven-slot version capable of supporting up to four interface modules.

Multipurpose Concentrators have an *autorestore* feature. If the Control Computer in the node is unable to communicate with the modules in the concentrator (because a link is broken or power has failed, for example), the Control Computer puts the concentrator into a suspended state (instead of removing it from service). The Control Computer attempts, at predetermined intervals, to restore the concentrator to service. If the problem has been resolved within a predetermined interval, the autorestore will succeed. Otherwise, the concentrator remains in the suspended state.

Multipurpose Concentrator 15-Slot (MPC15)

The MPC15 is a modular cabinet 30" wide x 17" high x 28" deep. Cabinet dimensions are identical to those of the node cabinets. By adding Control Computer hardware and BNS-2000 software, the MPC15 can be upgraded to Control Cabinet status, thereby providing node-level functionality. The MPC15 contains slots numbered from 0 to 15. It contains the following:

- power units
- a Clock module
- a Switch module
- a trunk/link module
- slots for the interface modules.

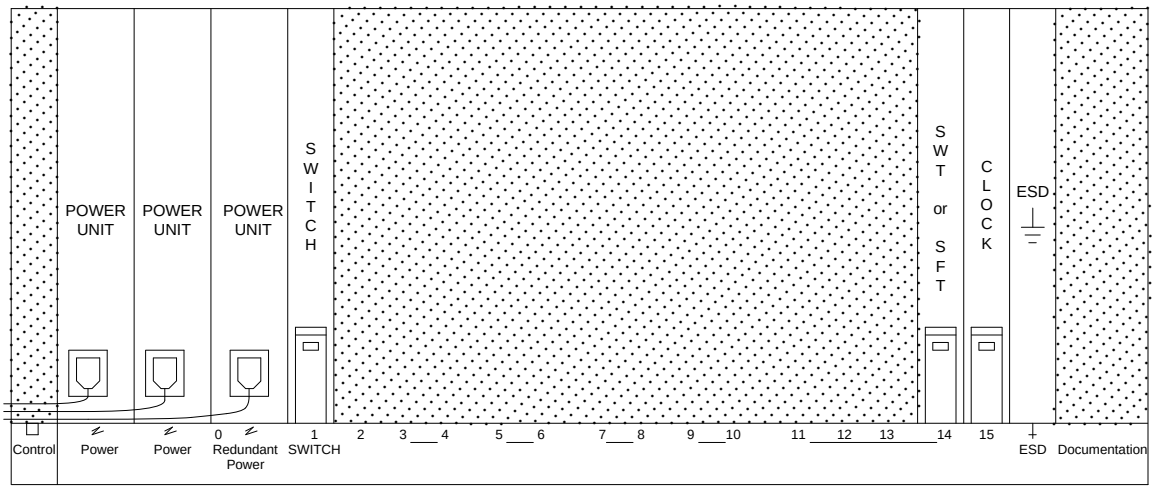

FIGURE 4-14. MPC15

MPC15 Power Units. Three Model 611C or ACX582 AC power units are provided. Stacking three or more MPC15s requires a power base. Model DCX1836 DC power units can also be used for CO applications but require a CO frame.

MPC15 Clock Module (TN1001B). A Clock module (described earlier under Additional Control Modules) is required. It must occupy slot 15 in the concentrator.

MPC15 Switch Module (TN1002B). The TN1002B Switch module is used in the MPC15. The Switch control memory contains information about all existing virtual circuits. This memory is updated by the Control Computer whenever virtual circuits are connected or disconnected. The Switch module can support 3500 simultaneous virtual circuits and 7,000 endpoints.

The Switch module always occupies slot 1 in the concentrator. No redundant Switch module is supported, and no I/O distribution board is required.

MPC15 Trunk/Link Modules. At least one trunk/link module is required to link the concentrator to its home node. Two trunk/link module types can be used in the MPC15:

- the Standard Fiber Trunk (SFT)
- the Standard Wire Trunk (SWT)

Both are explained in detail later under Trunk Modules. The trunk/link module can be placed in slots 2, 3, 13, or 14 in the concentrator.

An administrator has several options for providing wire trunk/link backups. The customer can use modems on the facility link that provide dial backup recovery for the link. These modems detect a link failure and will attempt to reestablish a connection to the partner-modem. The dial-back type modem is used in conjunction with a settable timer so the administrator can configure how quickly a link facility failure is detected. If the modem reestablishes the link successfully

before the concentrator timer parameter expires, calls over the link will not be taken down. If the modems cannot reestablish their link, the calls will come down.

The MPC15 supports a redundant link through a cold standby trunk/link module. If the primary link fails, the network administrator can manually restore the concentrator, establishing a link using the cold standby trunk/link module. BNS-2000 does not support an automatic facility for restoring the concentrator.

MPC15 Interface Modules. The MPC15 has slots numbered from 0 to 15. Three are reserved for the required modules: a Clock module, a Switch module, and a trunk/link module. A fourth slot is for the redundant power module. The remaining 12 slots can accommodate the interface modules, including a trunk/link module used as a cold standby.

Multipurpose Concentrator 7-Slot (MPC7)

The MPC7 is a metal cabinet 19" wide x 6" high x 25" deep. It can be mounted on a flat surface, in a wiring closet, or on an EIA standard rack mount of 19", 23", or 25". It contains seven numbered slots. It contains the following:

- a power unit
- a Clock module
- a Switch module
- a trunk/link module
- slots for interface modules.

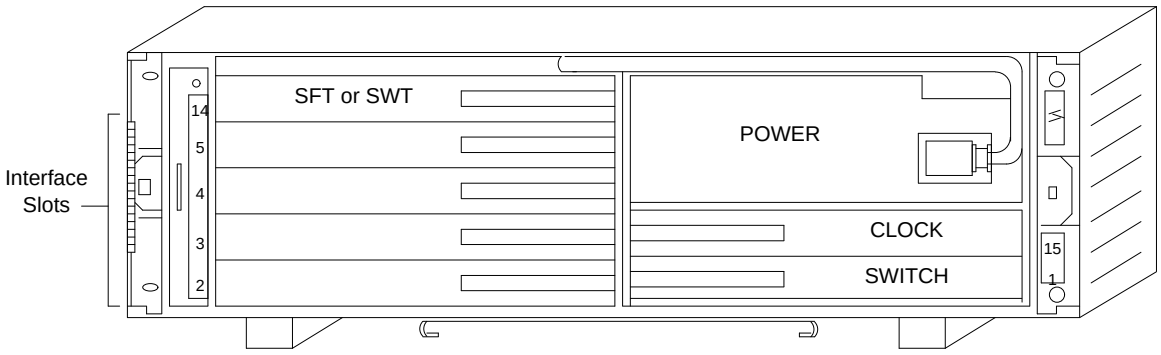

FIGURE 4-15. MPC7

MPC7 Power Unit. One Model 611C or ACX582 AC power unit is provided.

MPC7 Clock Module (TN1001B). A Clock module is required. It must occupy slot 7 in the

concentrator.

MPC7 Switch Module (TN1002B). The TN1002B Switch module is supported in the MPC7. The Switch module always occupies slot 1 in the concentrator.

MPC7 Trunk/Link Modules. At least one trunk/link module is required to link the concentrator to its home node. The following two trunk/link module types can be used in the MPC7:

- the Standard Fiber Trunk (SFT) (MC1P085A1)
- the Standard Wire Trunk (SWT) (TN2092).

Both are explained in detail later under Trunk Modules. The trunk/link module can be placed in slots 2 or 3 in the concentrator.

An administrator has several options for providing wire trunk/link backups. The customer can use modems on the facility link that provide dial backup recovery for the link. These modems detect a link failure and will attempt to reestablish a connection to the partner-modem. The dial-back type modem is used in conjunction with a settable timer so the administrator can configure how quickly a link facility failure is detected. If the modem re-establishes the link successfully before the concentrator timer parameter expires, calls over the link will not be taken down. If the modems cannot reestablish their link, the calls will come down.

The MPC7 supports a redundant link through a cold standby trunk/link module. If the primary link fails, the network administrator can manually restore the concentrator, establishing a link using the cold standby trunk/link module. BNS-2000 does not support an automatic facility for restoring the concentrator.

MPC7 Interface Modules. The MPC7 has 7 numbered slots for circuit boards. Three are reserved for the required modules: a Clock module, a Switch module, and a trunk/link module. The remaining 4 slots can accommodate interface modules, including a trunk/link module used as a cold standby.

Synchronous/Asynchronous Multiplexers (SAMs)

The SAM family of concentrators supports many switched or dedicated asynchronous connections or transparent synchronous connections over a single trunk facility. They use time and channel division multiplexing technology to provide economical access to the BNS-2000 network for large, medium, or small concentrations of endpoints. The following three SAM models in both AC and DC power versions are available:

- ***SAM504*** provides up to 504 individually configurable ports. It can be linked to the node by wire or optical fiber cable.
- ***SAM64*** provides up to 64 individually configurable ports. It can also be linked to the node by wire or fiber cable. A dual wire link is also available.
- ***SAM16*** provides up to 16 individually configured ports. It is linked to the node by an integral wire interface. A dual wire link is also available.

All SAMs support the following features on a per-port basis:

- predefined destination (PDD) protocol support for Bisync, HDLC, SDLC, DDCMP, Burroughs Poll/Select, Uniscope, and asynchronous protocols
- 75 bps to 19.2 Kbps and autobaud full-duplex ASCII and other configured asynchronous data
- 110 bps to 19.2 Kbps full-duplex synchronous data
- switched and PDD connections for asynchronous protocols
- odd, even, and no parity options for async ports and ASCII and variable bit size asynchronous data
- XON/XOFF and EIA flow control in both directions
- permanently active port option — which permits SAM synchronous ports to be "active" as soon as they are put into service, allowing the ports to remain logically connected regardless of EIA lead state changes in network endpoints.

SAM504

The SAM504 provides access to the node for many asynchronous and synchronous ports. (If the SAM504 connects to a SAMML in the node, only 19 ports on the sixteenth TERM32 module can be configured.) Depending on configuration and traffic loads, up to 25 SAM504 units can be connected to a single node.

The SAM504, designed for use in the CO environment only, conforms to CO standards with a –48 VDC power supply and CO framework.

The SAM504 dimensions (26" wide x 84" high x 24" deep) are those of the ESS Switch single-bay frame (ED5A001-70) in which the SAM504 is housed. It weighs about 500 lbs, depending on the number and type of installed modules.

The SAM504 consists of the following four main units:

- Fuse and Alarm Panel
- Multiplexer Shelf
- Fan Unit
- Patch Panel.

Fuse and Alarm Panel. The fuse and alarm panel distributes –48 VDC power to the fans and the multiplexer shelf power supplies. An interface to the CO alarm grid is also provided. Eight fuses protect the power supplies in the multiplexer shelf, fans, and the alarm circuitry in the fuse and alarm panel.

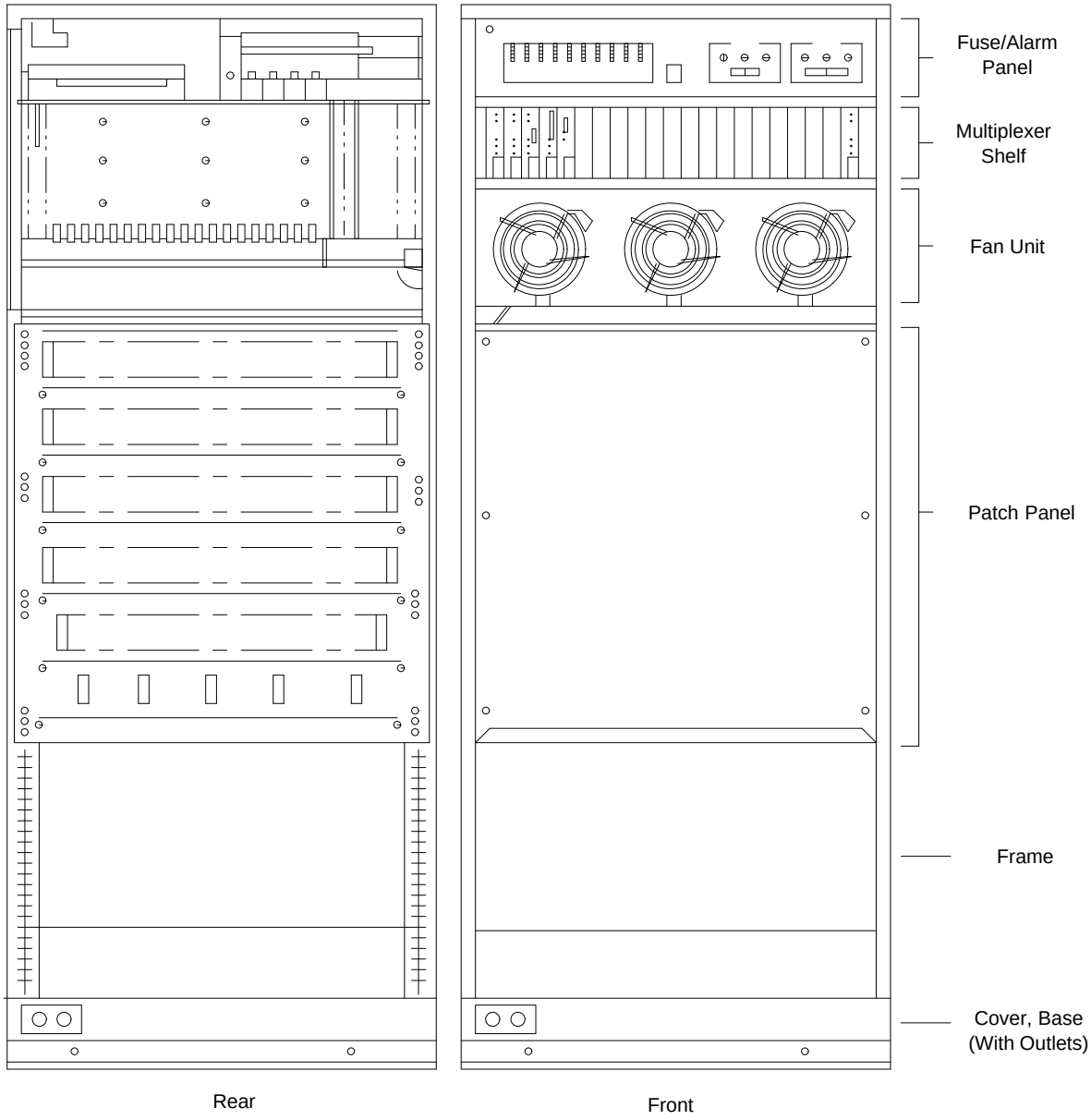

FIGURE 4-16. SAM504

Multiplexer Shelf. The SAM504 multiplexer shelf consists of front and rear card slots that support a maximum of 22 circuit packs.

The multiplexer shelf contains a Time Division Multiplexed (TDM) Bus Controller (TCON) module, a trunk/link module, up to 16 TERM32 interface modules, and power supplies.

The front card slots hold the TCON, a trunk module, the TERM32 modules, and the multiplexer shelf power supplies. The rear of the shelf contains I/O distribution boards for connections to endpoint devices and link facilities.

Four power supply cards can be installed in the multiplexer shelf, depending on how many TERM32 modules are in use.

Fan Unit. The fan unit contains three cooling fans and a filter. It provides cooling to the multiplexer shelf.

Patch Panel. The patch panel is located below the cooling fan unit and provides connections for endpoint devices. It consists of six rows, labeled J1 through J6, of 50-pin connectors. Each connector provides six EIA RS-232-C connections with eight leads. Ribbon cables are used to connect the TERM32 I/O distribution boards (ED2P466-30,G1) to the 50-pin connectors in the SAM patch panel.

SAM504 Control Component (TCON). The TCON module (TN1394C) is the SAM504 controlling element. It occupies the second empty slot in the multiplexer shelf. It emulates the node Clock module, switch module, and Repeater module and controls the three buses on the concentrator backplane. It handles the time slot transformation between the TDM bus and the trunk channels. It includes a microprocessor that performs common functions for the SAM and performs services for individual stations. There is a one-for-one correspondence between each port, each TDM time slot and each channel on the trunk. The TCON initializes the trunk module, downloads control software to TERM32s, translates data between the trunk module and TERM32s, and reports status information.

SAM504 Interface Module (TERM32, UN315). The TERM32 module provides the interface for 32 EIA RS-232-C ports that can be administered independently to support asynchronous or synchronous transport. The TERM32 is covered in detail later under Interface Modules.

SAM504 Trunk/Link Modules. A trunk/link module provides 8 Mbps fiber, or from 9.6 Kbps to 2.048 Mbps wire communication between the SAM504 and a BNS-2000 node. It occupies the first empty slot in the SAM. The trunk/link module can be one of the following:

- ***HS-Trunk*** is the counterpart of a Trunk-HS module in the node. It provides an interface for an 8 Mbps fiber connection to the node.
- ***T1-Trunk*** is the counterpart of the Trunk-T1 module in the node. It provides an interface for a T1 link to the node.
- ***SAMSL*** is the counterpart of a SAMSL or SAMML in the node. It provides a wire interface for an analog transmission facility between the SAM and the node. The SAMML is located in

the node, providing up to eight links to SAM-located SAMSLs.

SAM504 trunk/link modules are covered in detail later under Trunk Modules.

An administrator has the option for providing a wire trunk/link backup. The customer can use modems on the facility link that provide dial backup recovery for the link. These modems detect a link failure and will attempt to reestablish a connection to the partner-modem. The dial-back type modem is used in conjunction with a settable timer so that the administrator can configure how quickly a link facility failure is detected. If the modem reestablishes the link successfully before the concentrator timer parameter expires, calls over the link will not be taken down. If the modems cannot reestablish their link, the calls will come down.

SAM64

The SAM64 supports 64 asynchronous or transparent synchronous EIA RS-232-C connections, in increments of 32 ports, through a trunk to the node. The SAM64 measures 11.25" wide x 13" high x 19.55" deep and weighs approximately 60 lbs. It contains a power supply, integral cooling fans, and a module shelf. Depending on configuration and traffic, up to 100 SAM64 units can be connected to a single node. The SAM64 conforms to central office (–48 VDC) and international (220 VAC, 50˜Hz) power requirements, and supports 120 VAC, 60 Hz.

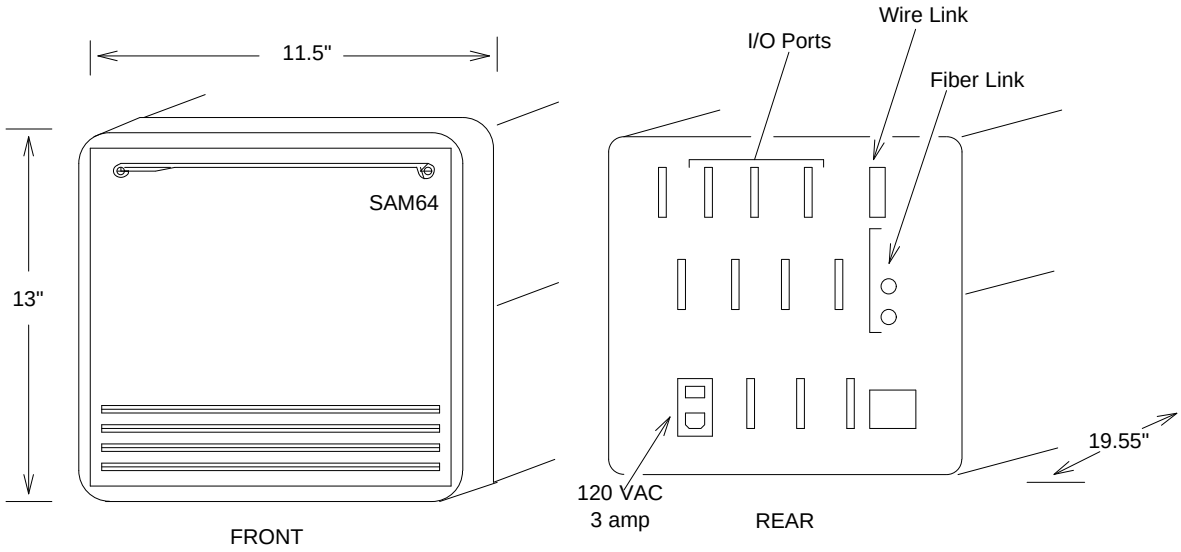

FIGURE 4-17. SAM64

SAM64 Control Module (TCON). The SAM64 controlling element is the TCON module. The TCON was described earlier under SAM504.

SAM64 Interface Module (TERM32). One or two TERM32 modules can be used to provide

interfaces to attached devices. The TERM32 is described later under Interface Modules.

SAM64 Trunk/Link Modules. A trunk/link module provides 8 Mbps fiber, or from 9.6 Kbps to 2.048 Mbps wire communication between the SAM64 and a BNS-2000 node. It occupies the first empty slot in the SAM. The trunk/link module can be one of the following:

- ***HS-Trunk*** is the counterpart of a Trunk-HS module in the node. It provides an interface for an 8 Mbps fiber connection to the node.
- ***T1-Trunk*** is the counterpart of the Trunk-T1 module in the node. It provides an interface for a T1 link to the node.
- ***SAMSL*** is the counterpart of a SAMSL or SAMML in the node. It provides a wire interface for an analog transmission facility between the SAM and the node. The SAMML is located in the node, providing up to eight links to SAM-located SAMSLs.
- ***SAMDL*** provides a dual wire link between the SAM64 and a SAMML in the node, providing a wire interface for an analog transmission facility between the SAM64 and the node. The dual links ensure high reliability by switching data traffic to the active link if the other fails, and provide increased performance by automatically sharing the traffic load between both links.

SAM64 trunk/link modules are covered in detail later under Trunk Modules.

An administrator has another option for providing a wire trunk/link backup. The customer can use modems on the facility link that provide dial backup recovery for the link. These modems detect a link failure and attempt to reestablish a connection to the partner-modem. The dial-back type modem is used in conjunction with a settable timer so the administrator can configure how quickly a link facility failure is detected. If the modem reestablishes the link successfully before the concentrator timer parameter expires, calls over the link will not be taken down. If the modems cannot reestablish their link, the calls will come down.

SAM16 (CPY1)

The SAM16 (CPY1) supports up to 16 asynchronous or transparent synchronous connections, in increments of eight ports, through an integrated V.35 trunk module or RS-232-C trunk module to a SAMSL or SAMML in the node. Each port is configurable to provide any asynchronous or synchronous transport supported service, independent of the configuration of the other ports. SAM16 services are fully compatible with other synchronous and asynchronous ports in BNS-2000, whether they are installed in the node, the SAM, or another concentrator. The SAM16 is a stand-alone unit that measures 17" wide by 13" deep and 4.4" high.

The SAM16 supports an integral dual-link connection to the node for redundancy and load sharing. The two links are to ports on the SAMML. To operate in dual link mode, the SAM16 must be connected to a SAMML; to operate in single link mode it may be connected to either a SAMML or a SAMSL.

External modems are used by the SAM16 at speeds ranging from 1.2 to 56 Kbps. If the modems are dial-back modems, the customer can provide dial backup recovery for the link. These modems detect a link failure and attempt to reestablish a connection to the partner-modem. The

dial-back modem is used in conjunction with a settable timer so the administrator can configure how quickly a link facility failure is detected. If the modem reestablishes the link successfully before the concentrator timer parameter expires, calls over the link will not be taken down. If the modem cannot reestablish the link, the calls will come down.

Depending on configuration and traffic, up to 150 SAM16 units can be connected to a single node.

The SAM16 contains a power supply (AC), integral cooling fans, and a module shelf. It may be ordered with an optional –48 DC power supply, which fits within the existing SAM16 physical enclosure.

The SAM16 can also connect to the SAMML using the following I/O boards:

- AWJ17 multiport RS-232 I/O board
- AWJ32 dual port V.35 I/O board.

In addition, the SAM16 can connect to a SAMSL in the node configured with one of the following two I/O boards:

- AWJ9 single port V.35 I/O board
- AWJ11 single port RS-232 I/O board.

The following two figures show front and back views of the SAM16.

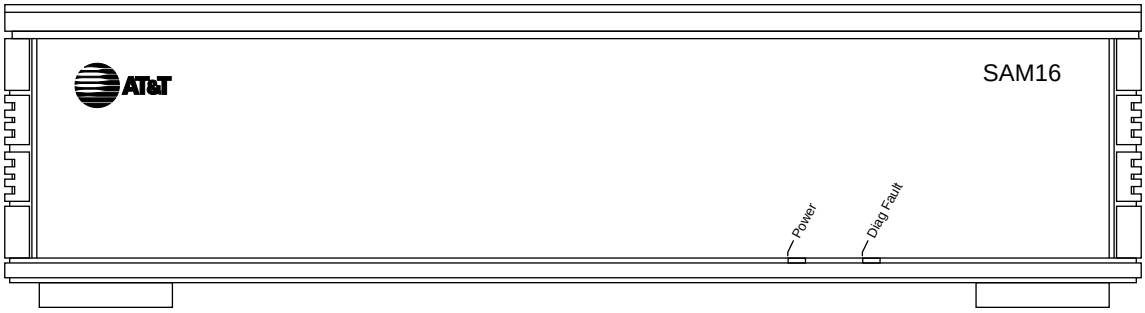

FIGURE 4-18. SAM16: Front View

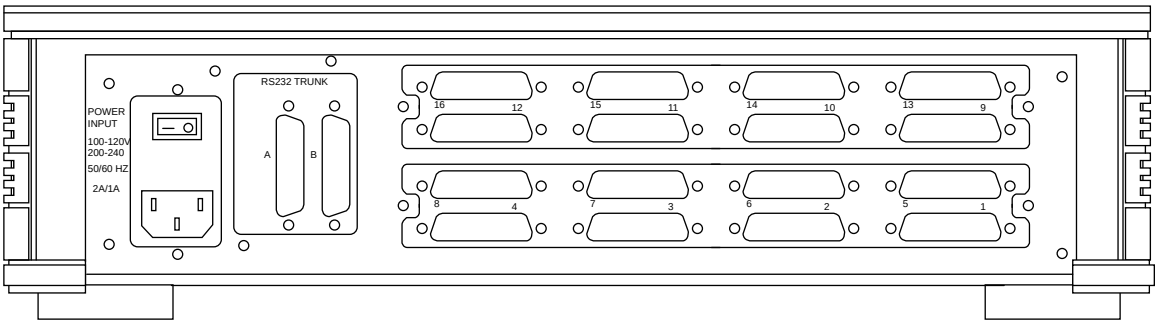

FIGURE 4-19. SAM16: Back View

Interface Modules

Interface modules provide a wide variety of services on the network. These services include the following:

- SMDS
- LAN interconnect
- asynchronous connections
- multiplexed host interfaces
- synchronous transport
- standards compliance for X.25 and X.75 recommendations
- special purpose interfaces
- customer programmable services.

This section contains details on the modules that provide each of these data services via placement in the node, in an MPC, or in a SAM. This section also discusses the I/O distribution boards that are used with each module.

SMDS

SMDS access is provided through AI modules which reside in Series M2 Shelves. The AIs provide SMDS access to the node at either T1/E1 or T3/E3 transmission speeds.

Each AI module communicates via digital transmission facility (DTF) equipment with a compatible terminal adapter (TA) located on the premises of an SMDS subscriber. A TA can be a multiprotocol router, or DSU that supports SMDS interfaces. The TAs are viewed as concentration devices and can provide bridging and routing services for Ethernet, FDDI, Token Ring® (TR), and other IEEE 802-based LANs.

Communication between an AI and a TA takes place across an SNI — the access path between the node and the subscriber's site — using the DQDB access protocol as the SIP. An SNI corresponds to a port on the AI module.

BNS-2000 AI modules support the following SMDS capacity requirements:

- 16 E.164 addresses per SNI
- one individual address screen per SNI
- one group address screen per SNI
- one, 16, or 32 MCDUs
- each E.164 address may be identified by up to 32 group addresses
- each SNI may be identified by up to 48 group addresses.

The AI modules offer an array of features for SMDS network service, interconnection to DTF equipment, diagnostic capabilities, and configurable options.

SMDS is a connectionless protocol — an AI module broadcasts connectionless data segments, equivalent to 53-octet Level 2–Protocol Data Units (L2-PDUs), on the backplane bus of the Series M2 Cabinets. These data segments are read by or routed to other AI modules for transmission across SNIs based on designated source and destination addresses.

The AI modules support E.164 addressing for CLNS traffic. Address screening is by source and destination — for each SNI, individual and group address database tables can be set up by customers to prevent certain subscriber equipment from sending or receiving data from certain specified addresses.

AI modules also support multiple data units in transit — SMDS data units are transferred across the SNI in PDUs of fixed length. The SIP allows PDUs from different data units to be interleaved during transmission across the SNI.

The following SMDS interface modules are supported:

- ***AI-T1*** provides standard connectionless SMDS service interface at speeds up to T1.
- ***AI-E1*** provides standard connectionless SMDS service interface at speeds up to E1.
- ***AI-T3*** provides standard connectionless SMDS service interface at speeds up to T3.
- ***AI-T3P*** provides higher throughput connectionless SMDS service interface at speeds up to T3.
- ***AI-E3*** provides standard connectionless SMDS service interface at speeds up to E3.
- ***GAR*** (Group Address Resolver) is needed only in SMDS networks serving as a GAA (Group Address Agent) for group addresses.

AI-T1 (CMA5)

The AI-T1 is a single-board module that has four ports. The AI-T1 module provides IEEE 802.6 SMDS access to node services. The AI-T1 supports the North American ANSI DS1 standard electrical interface. Each port on the AI-T1 can function independently and supports an SNI at the full rate of 1.544 Mbps.

The AI-T1 can obtain its clock synchronization from the facility or from an SSM4 DS1 Clock on the node. If the reference source, or "master clock" used to synchronize the timing of transmit and receive data signals, is not used (or fails), the SSM4 will maintain accuracy with ± 32 parts per million (ppm) at T1 rates. Only port 1 on the AI-T1 supports 8 kHz timing; ports 2, 3, and 4 support the Stratum 4 timing reference or facility timing.

The AI-T1, when located in a CO node, connects with a variety of DTF equipment, including the following:

- DSX-1
- CSU/DSU

- CSU/DSU connected to a DSX-1
- AT&T DDM1000 digital multiplexer
- AT&T Digital Access Cross-Connect System (DACS)
- AT&T DDM2000 digital multiplexer.

The AI-T1 uses a CMC5B I/O board with a built-in DSU function; it supports DQDB and the Physical Layer Convergence Protocol (PLCP).

AI-E1 (CMA5)

The AI-E1 is a single-board module that has three ports. It provides IEEE 802.6 SMDS access to node services for international applications. The AI-E1 supports CEPT E1 data signals at 2.048 Mbps. Each port on the module can function independently and can support an SNI at the full rate of 2.048 Mbps.

The AI-E1 can obtain its clock synchronization from the facility or from a local clock on the node.

The AI-E1 uses a CMC8 I/O board with a built-in DSU function; it supports DQDB and the PLCP.

AI-T3 (CMA11B)

The AI-T3 is a single-board module that has one port. It provides IEEE 802.6 SMDS access to node services. The AI-T3 supports the North American ANSI Data Signal 3 (DS3) standard electrical interface. The AI-T3 can support Access Class 4 traffic. For very large messages with only ingress traffic, Access Class 5 can be supported. See the AI Module Reference for more information.

The AI-T3 uses a CMC6 or CMC6B I/O board; it supports DQDB and the PLCP.

The AI-T3, when located in a CO node, connects with a variety of DTF equipment. AI-T3 module to DTF connections include the following:

- DSX-3 patch panel
- DDM1000 digital multiplexer
- DACS
- AT&T DDM2000 digital multiplexer.

AI-T3P (CMA17/CMA17)

The AI-T3P is a two board module that resides in the Series M2 Shelf. Its one port provides IEEE 802.6 SMDS access to node services. The AI-T3P supports the North American ANSI DS3 standard electrical interface and can be configured for an access class up to 5. It supports the Distributed Queue Dual Bus (DQDB) access protocol and the Physical Layer Convergence Procedure (PLCP).

Full duplex traffic at Access Class 5 is achieved by having one board dedicated to ingress traffic,

the other board to egress traffic. The egress board of the AI-T3P is a CMA17 circuit pack that uses the CMC6B I/O board; the ingress board is a CMA17 circuit pack that uses a CMC14 I/O board.

AI-E3 (CMA11B)

The AI-E3 is a single-board module that has one port. It provides IEEE 802.6 SMDS access to node services for international applications. The AI-E3 supports CEPT E3 data signals at up to 34 Mbps.

The AI-E3 uses a CMC13 I/O board; it supports DQDB and the PLCP.

GAR (CMA15)

The Group Address Resolver module (GAR) is a single board module that is installed in Series M2 Cabinets only. It works in concert with the TRK-T3I module to provide group-addressed data unit transport across several carriers' networks. The GAR module enables a carrier to serve as a Group Address Agent (GAA) for group addresses that have members outside the carrier's local network. The GAR module is not needed in every network; it is only needed in SMDS networks that are serving as GAAs for group addresses that have members outside the carrier's local network.

The GAR module uses the CMC14 I/O board, however, no external interfaces are used with the GAR module.

LAN Interconnect

BNS-2000 supports a variety of LAN interconnect services. The primary interfaces are provided by the high-speed M2 Frame Relay Module (FRM-M2), the Frame Relay Module (FRM), and the LAN Protocol Module (LPM):

- ***FRM*** provides channelized and non-channelized frame relay interfaces at speeds up to T1/E1.
- ***FRM-M2*** provides frame relay interfaces for six T1/E1 channelized connections.
- ***LPM*** is an Ethernet LAN interface module; it supports up to 2 (full duplex) LAN ports and up to 27 virtual frame relay ports with up to 507 virtual circuits.

FRM (MC1D143A1)

The Frame Relay Module (FRM) is a single-board module that supports either four V.35 ports or a single channelized T1 or E1 port depending on the I/O board selected. Each V.35 connection supports connections ranging in speed from 9600 bps to 2.048 Mbps, subject to the aggregate module throughput of 4 Mbps (2.048 Mbps in each direction).

The FRM is a downloadable module which supports up to a maximum of 507 user channels (Data Link Connection Identifiers). The FRM can be located in a BNS-2000 node on a Series M1 Shelf or in a Multipurpose Concentrator.

The FRM provides frame relay services which are compliant with existing ANSI, ITU-T, and

Frame Relay Forum standards. The FRM supports three PVC management procedures that comply with ANSI T1.617 Annex D, CCITT (ITU-T) Q.933 Annex A, and the local management interface (LMI).

The following I/O distribution boards can be used with the FRM:

- ***AWJ24*** provides four V.35 data terminal equipment (DTE) connections at speeds up to 2.048 Mbps.
- ***CSD1*** is a 4-wire, Digital Signal Cross-Connect, Level 1 (DSX-1) compatible interface based on the ANSI T1.403 standard; it provides a single channelized T1 connection at speeds from 56 Kbps to 1.536 Mbps, and up to 24 virtual ports over that connection. DB-15 connectors must be used for the T1 and external clock connections.
- ***CSD2*** is a 75-ohm board that supports coaxial connections to a single channelized E1 connection at speeds from 64 Kbps to 2.048 Mbps, and up to 31 virtual ports over that connection. DB-15 connectors must be used for the E1 and external clock connections.
- ***CSD3*** is a 120-ohm board that supports twisted pair connections to a single channelized E1 connection at speeds from 64 Kbps to 2.048 Mbps, and up to 31 virtual ports over that connection. DB-15 connectors must be used for the E1 and external clock connections.

FRM-M2 (CTG5)

The high-speed M2 shelf Frame Relay Module (FRM-M2) is a single-board module that supports up to six channelized T1 or E1 ports depending on the I/O board selected. Each channelized T1 connection can support up to 24 independent frame relay interfaces. Each channelized E1 connection can support up to 31 independent frame relay interfaces.

The FRM-M2 is a downloadable module which supports up to a maximum of 2000 user channels (Data Link Connection Identifiers). The FRM-M2 supports 2, 3, or 4 octet addressing. The FRM-M2 can only be located in a BNS-2000 node on a Series M2 Shelf.

The FRM-M2 provides frame relay services which are compliant with existing ANSI, ITU-T, and Frame Relay Forum standards. The FRM supports three PVC management procedures that comply with ANSI T1.617 Annex D, CCITT (ITU-T) Q.933 Annex A, and the local management interface (LMI).

The following I/O distribution boards can be used with the FRM-M2:

- ***CMC17*** is a 4-wire, Digital Signal Cross-Connect, Level 1 (DSX-1) compatible interface based on the ANSI T1.403 standard; it provides six channelized T1 connections at speeds from 56 Kbps to 1.536 Mbps, and up to 24 virtual ports over that connection. DB-15 connectors must be used for the T1 and external clock connections.
- ***CMC18*** is a 75-ohm board that supports coaxial connections to six channelized E1 connections at speeds from 64 Kbps to 2.048 Mbps, and up to 31 virtual ports over that connection. DB-15 connectors must be used for the E1 and external clock connections.
- ***CMC19*** is a 120-ohm board that supports twisted pair connections to six channelized E1 connections at speeds from 64 Kbps to 2.048 Mbps, and up to 31 virtual ports over that

connection. DB-15 connectors must be used for the E1 and external clock connections.

LPM (TN2229)

The LPM is a single BNS-2000 interface module (TN2229) that provides IP router-like functionality over frame relay. It is used with a CSD6 I/O distribution board that contains two RJ-45 connectors for two 802.3 10Base-T (twisted pair Ethernet) ports. The LPM routes IP packets to/from these ports, to equipment connected to the BNS-2000 FRMs, and ports on other LPMs. The LPM can support data traffic at speeds up to 1.544 Mbps per physical port in full duplex mode (simultaneous traffic in both directions).

The LPM supports up to 507 BNS-2000 PVCs to other LPMs and/or to BNS-2000 frame relay ports. Virtual circuits between the LPM and other LPMs and/or BNS-2000 frame relay ports are organized into virtual frame relay ports on the LPM. The LPM supports up to 27 virtual frame relay ports.

The LPM software is downloaded from the Control Computer. The LPM is supported in the BNS-2000 node, and in Multipurpose Concentrators (MPC7/MPC15).

The module is configured and managed from either the BNS-2000 administrative console or the *StarKeeper* II NMS console.

Both on-line and off-line diagnostics are available for the LPM. On-line tests check the communications path and include a loopback test on an LPM physical port and an echo (ping) test for problem isolation between the LPM and any IP endpoint. Off-line diagnostics test various parts of the hardware on the LPM. In addition, the LPM executes a complete self-test each time a reset occurs.

Asynchronous Service

Asynchronous interfaces are provided through the following interface modules: TYs, MSMs, SAMs, and TSM8 (via PDDs only). The TSM8 module is described later under Synchronous Transport.

The following asynchronous interface modules are supported:

- ***MSM*** is most appropriate for support of asynchronous speeds above 19.2 Kbps, but supports the full range of speeds.
- ***TY6*** provides basic asynchronous interface support for most common speeds up to 19.2 Kbps with up to 6 ports.
- ***TY12*** provides basic asynchronous interface support for most common speeds up to 19.2 Kbps with up to 12 ports.
- ***TERM32*** provides basic asynchronous support on SAM64 and SAM504 supporting speeds up to 9.6 Kbps.
- ***CPY1(SAM16)*** provides basic asynchronous interface support on SAM16 for speeds up to 19.2 Kbps.

MSM (TN2111B)

The Multispeed Module (MSM) provides serial asynchronous start-stop protocol transmission to asynchronous devices. These devices can communicate through BNS-2000 with devices connected through another MSM, or a TY12, TY6, CPM-HS, SAM, TSM8, X.25, X.25P, or X.75 module. Options, which are administrable on a per-port basis, include speed conversion, parity translation, flow control protocol conversions, and call processing. The module provides high-speed, remote access from asynchronous devices to devices on local area networks (LANs) and connectivity for higher speed dial-in modem pools. The MSM supports asynchronous communications at speeds from 75 bps to 115.2 Kbps with the reliability provided by Grade of Service 5 (GOS5).

Diagnostics for the MSM are described in the *Multispeed Module Reference*.

The MSM consists of a TN2111B circuit pack and an AWJ4 I/O board that provides the wiring for 12 serial, asynchronous, full-duplex EIA RS-232-C ports. The module and its I/O board can reside in a node, or in a Multipurpose Concentrator 15-slot (MPC15) or Multipurpose Concentrator 7-slot (MPC7). Interface leads provide the physical connection to a DTE or DCE device through the interconnecting cabling. The service type identifies the function of the interface to the connected end device.

TY12 (TN2157 or TN1011C)

The TY12 interface module (TN2157 or TN1011C) communicates with asynchronous terminals, host computer ports, personal computers, printers, or modems. These devices can communicate through BNS-2000 with devices connected through another TY12 or through an MSM, TY6, CPM-HS, SAM, TSM8, DKAP, X.25, X.25P, or X.75 module.

This module provides 12 serial, asynchronous, full-duplex ports. Each of the 12 ports can be individually set to baud rates from 300 bps to 19.2 Kbps and autobaud.

The TY12 module optionally supports XON/XOFF flow control and CTS/RTS (clear to send/request to send) flow control. Odd, even, or transparent parity features are supported. Four types of loopback tests are provided for the TY12, and the module supports connections and diagnostics for AT&T Voice/Data Multiplexers. Administrators can display EIA status of the TY12 leads without removing the module from service. For additional information on diagnostics, refer to the *TY Module Reference*.

A single I/O distribution board can be used with the TY12:

- ***AWJ4*** provides 12 EIA RS-232-C DTE ports.

The TY12 clearly and rapidly passes the BREAK to its attached device when it is received from another BNS-2000 circuit pack.

The TY12 provides immediate detection of end-of-session signaling from a host. It also recovers gracefully from illegally sized block mode transmissions. The port that received the illegal data is automatically reset. It tolerates overspeed conditions from a variety of modems and terminals that occasionally transmit at nonstandard speeds.

TY6 (TN1006)

The TY6 interface module communicates with terminals, host computers, personal computers, printers, and modems. It provides six serial, asynchronous, full-duplex, EIA RS-232-C ports that run at speeds from 75 bps up to 19.2 Kbps. It can interface with devices connected through another TY6, or through an MSM, TY12, CPM-HS, SAM, TSM8, DKAP, X.25, X.25P, or X.75 module.

Supported baud rates are 75, 110, 300, 1200, 1800, 2400, 4800, 9600, and 19200 bps. The TY6 can serve a limited number of ports when operating on a continuous flow of data at the higher bit rates. Many user terminals do not operate in this way, transmitting in small bursts and then sitting idle. The TY6 module can usually support six ports operating at 9600 bps. Frequently, even six ports at 19.2 Kbps can be supported. Applications that need high-speed continuous data flow can mix high-speed and low-speed interfaces or leave one or more ports unused.

The TY6 module optionally supports XON/XOFF flow control. It also supports odd, even, mark, or transparent parity. As a special feature, the TY6 supports several specific options that are necessary for certain applications, such as TNM logging lines.

The TY6 module's behavior is controlled by firmware (ROM), and does not require a reload after a power failure.

Four types of loopback tests are provided for the module. All four diagnostics interrupt service to only one port on the module.

A single I/O distribution board is used with the TY6:

- ***ED5P066-30,G1*** provides 6 RS-232-C DTE connections.

TERM32 (UN315)

TERM32 modules can only be placed in the SAM504 and the SAM64. Each TERM32 module provides the interface for 32 EIA RS-232-C ports that can be administered independently to support asynchronous transport. Each group of four ports is controlled by a single microcomputer station. The stations support call services for their individual ports, including call setup, data transmission, and diagnostic functions. Each port on a station is treated totally independently regarding port options and status. Each port has one dedicated TDM channel to send/receive data and supervision messages. The TERM32 module interfaces with terminals, host computers, personal computers, printers or modems, and can interface through BNS-2000 with devices connected through a SAM, or a TY12, MSM, TY6, CPM-HS, TSM8, DKAP, X.25, X.25P, or X.75 module. Features include odd, even, or no parity, and 5, 6, 7 or 8 bits per character.

When configured for asynchronous service, the 32 full-duplex ports can run at speeds of 75, 110, 150, 300, 1200, 2400, 4800, 9600, 14400, and 19200 bps. The module also supports autobaud, or automatic adjustment to the speed of the connected endpoint, at speeds up to 9600 bps.

The TERM32 module has eight processors, or stations, each supporting four EIA RS-232-C ports. Each port has a dedicated 19.2 Kbps full-duplex channel through the SAM. However, throughput is constrained by processor (station) capacity, as well as the capacity of the trunk that connects the SAM to the node.

- ***Port Capacity*** — Asynchronous ports can be configured at speeds up to 19.2 Kbps. SAM ports can accept data from attached devices at the maximum rate, independent of other activity on the SAM. Initially, data received from attached devices is stored in buffers. Each port has 1827 bytes of buffer available for collection of data from attached devices.
- ***Station Capacity*** — A TERM32 station supports four adjacent ports on the TERM32 module. These processors collect data from the SAM ports in buffers, transport this data across the BNS-2000 network, and transmit the data from the TERM32 port to the attached device. Data is transmitted from the TERM32 station using GOS5. This provides error detection and retransmission, ensuring that the SAM provides reliable transmission across the network. For asynchronous traffic, each TERM32 station can support a total throughput of about 62 Kbps.
- ***Board Capacity*** — The capacity of the TERM32 module is simply the aggregate of the capacities of the eight stations on the TERM32 module.

The stations on a TERM32 module have insufficient capacity to transmit data at the total of the configurable port speeds over extended periods of time. To meet the needs of devices requiring high sustained throughput, it may be necessary to reduce the number of active ports on a single TERM32 station, or carefully configure the TERM32 stations to assure that devices requiring high sustained throughput are connected to ports on different TERM32 stations.

Five types of loopback tests are provided for the TERM32, all of which interrupt service to only one of its ports. Diagnostic procedures are described in the Troubleshooting chapter of the *Data Networking Products Synchronous/Asynchronous Multiplexer Reference*.

The TERM32 is used with the following I/O distribution board:

- ***ED2P466-30,G1*** is used with the TERM32 in the SAM504. No I/O distribution board is required with the TERM32 in the SAM64.

TERM32 support for synchronous communications is described later under Synchronous Transport.

CPY1

The CPY1 module can only be placed in the SAM16. It supports eight EIA RS-232-C ports. Each port can be administered independently to support asynchronous transport. The CPY1's asynchronous interface also provides call services for the individual ports, including call setup, data transmission, and diagnostic functions. Each port is treated independently regarding port options and status.

The CPY1 interfaces with terminals, host computers, personal computers, printers or modems, and can interface through BNS-2000 with any channel on another SAM, or on a TY12, MSM, TY6, CPM-HS, DKAP, TSM8, X.25, or X.75 module. Features include odd, even, or no parity, and 5, 6, 7 or 8 bits per character.

Five types of loopback tests are provided for the CPY1's asynchronous interface, all of which interrupt service to only one of its ports. Diagnostic procedures are described in the *Data Networking Products Synchronous/Asynchronous Multiplexer Reference*.

The CPY1 has integrated I/O boards. The CRA1 V.35 trunk module provides the link connection for V.35. The CRA2 RS-232-C trunk module provides the link connection for RS-232.

CPY1 support for synchronous communications is described under Synchronous Transport.

Multiplexed Host Interfaces

In addition to the RS-232-C asynchronous host connections, BNS-2000 provides multiplexed fiber connections to AT&T hosts and servers and certain computers from other vendors through a Computer Port Module (CPM). Hosts/servers connected via CPMs require CommKit software or compatible networking software. Each BNS-2000 connection requires an interface in the target host as well as in the BNS-2000.

CPM-HS (TN1009)

The CPM-HS provides a high-speed, serial optical fiber connection from BNS-2000 nodes to currently supported AT&T host computer systems and the host computer systems of other vendors. One or two host connections are supported up to 1 km from the node. CommKit software is required for the connections. Connections from BNS-2000 to the host are multiplexed over the fiber link.

The CPM-HS uses an AWJ2 I/O board.

Synchronous Transport

In BNS-2000 nodes and MPCs, synchronous interfaces are provided by the TSM8, TSM-T1, SYNC8, X.25, X.25P, and X.75 modules. Additionally, ports on the TERM32 module, located in SAM504s and SAM64s, and any of the SAM16 ports can be administered to support synchronous communications. The X.25, X.25P, and X.75 modules are described in later sections.

The following synchronous interface modules are supported:

- ***TSM8*** is the primary synchronous interface module for speeds up to 64 Kbps.
- ***TSM-T1*** is the primary synchronous interface module for speeds up to T1/E1.
- ***SYNC8*** provides support for switched 3270 service.
- ***TERM32*** provides basic synchronous support on SAM64 and SAM504 supporting speeds up to 9.6 Kbps.
- ***CPY1(SAM16)*** provides basic synchronous interface support on SAM16 for speeds up to 19.2 Kbps.

TSM8 (MC1D088A1)

The TSM8 module allows various synchronous and asynchronous devices to communicate through the BNS-2000 network over PVCs. As its primary service, it provides nonswitched synchronous transport service for synchronous terminals, hosts, front-end processors, and cluster controllers. The module can communicate simultaneously with host ports and cluster controllers.

The TSM8 supports block mode Bisync, HDLC, SDLC, DDCMP, Burroughs Poll/Select, or Uniscope service in transparent mode in point-to-point or multipoint configurations. It supports speeds of 2.4, 4.8, 9.6, and 19.2 Kbps for DCE or DTE, and 48, 56, or 64 Kbps for DTE configurations only. With the DDCMP protocol, speeds can be 2.4, 4.8, 9.6 or 56 Kbps. The module provides clocking for DCE ports; external clocking is required for all DTE ports.

One or more single or multipoint Bisync or SDLC lines can be multiplexed onto one host multipoint line. This multipoint bridging capability is enhanced by pipelining for improved performance. Pipelining allows transmissions of synchronous data as it arrives at the network interface, without waiting until a frame is filled.

Synchronous transport is appropriate for interactive and batch-oriented devices using EIA RS-232-C or V.35 interfaces. This service is achieved through an administered predefined destination between two EIA RS-232-C or V.35 endpoints.

The TSM8 does not provide terminal-handling functions; it serves as a transport mechanism for the synchronous protocols above, removing all extraneous fill and sync characters from the data stream.

The TSM8 serves as the interface between the protocol of the external device and the internal packet protocol, providing buffering and flow control of the data. Users should follow engineering guidelines specified in the *Planning Guide* to set flow control mechanisms within the protocols to limit the amount of data sent to the TSM8 and thus eliminate buffer overruns.

This module downloads software from the Control Computer. The software version number is selected when the module is administered.

In addition to the TSM8 board, six boards are available for I/O distribution. By using the appropriate I/O distribution board, the module can be configured as DCE or DTE. The following I/O distribution boards can be used with the TSM8:

- ***AWJ5*** provides one DTE V.35 connection and three DCE EIA RS-232-C connections for lines operating at 2.4, 4.8, 9.6, or 19.2 Kbps (sync and async); 48, 56 or 64 Kbps (sync DTE); or 1.2 Kbps (async only). Clocking is provided for the DCE ports only. The bottom 50-pin connector is used to access port 1 (V.35) and the top 50-pin connector is used to access ports 2, 3 and 4 (EIA RS-232-C).
- ***AWJ6*** provides one DTE V.35 connection and three DTE EIA RS-232-C connections for lines operating at 2.4, 4.8, 9.6 or 19.2 Kbps (sync and async); 48, 56 or 64 Kbps (sync DTE); or 1.2 Kbps (async only). External clocking is required for all ports. The bottom 50-pin connector is used to access port 1 (V.35) and the top 50-pin connector is used to access ports 2, 3, and 4 (EIA RS-232-C).
- ***AWJ7*** provides eight DTE EIA RS-232-C connections with NRZI encoding for lines operating at 2.4, 4.8, 9.6, or 19.2 Kbps (sync and async); or 1.2 Kbps (async only). External

clocking is required.

- ***AWJ8*** provides eight DCE EIA RS-232-C connections with NRZI encoding for lines operating at 2.4, 4.8, 9.6, or 19.2 Kbps (sync or async) or 1.2 Kbps (async only). Clocking is provided.
- ***AWJ17*** provides eight DTE EIA RS-232-C connections for lines operating at 2.4, 4.8, 9.6 or 19.2 Kbps (sync and async); or 1.2 Kbps (async only). External clocking is required.
- ***AWJ18*** provides eight DCE EIA RS-232-C connections for lines operating at 2.4, 4.8, 9.6 or 19.2 Kbps (sync and async) or 1.2 Kbps (async only). Clocking is provided.

TSM-T1 (MC1D149A1)

The TSM-T1 provides high-speed transparent transport, up to rates of 2.048 Mbps, for the SDLC and HDLC protocols, including such HDLC-based traffic as TCP/IP. Messages sent from customer-based devices in the format of SDLC or HDLC frames are broken into packets for high-speed transport across the network to another TSM-T1 or TSM-T1-compatible module. On receipt, the packets are re-assembled into frames and transmitted to the designated customer-based device.

The TSM-T1 supports up to four V.35 DTE ports that can be configured at any line speed from 9600 bps to 2.048 Mbps, although the performance of the module is limited to an aggregate throughput of 3 Mbps.

The module interworks with a number of other synchronous endpoints, including endpoints on the module itself, the TSM8, and all protocol-compatible SAM endpoints. The TSM-T1 also supports multipoint bridging for 3270 SNA/SDLC, where a single port can receive multiple calls from other TSM-compatible ports. In addition, the TSM-T1 supports *synchronous only* connections to and from the TSM8, and can consolidate lines that carry traffic at 56/64 Kbps through the TSM8.

Fanout and broadcast are multipoint bridging options for the TSM-T1.

The TSM-T1 uses an AWJ24 I/O board, which provides connections for four V.35 DTE devices.

SYNC8 (MC1D089A1)

The SYNC8 (BSC3270) module interfaces with the *Teletype*® 4540/5540 family and IBM® families of 3270-type control units (CUs), printers, and terminals as well as IBM 3705/3725 Front-End Processors and Comten® Front-End Processors that use Basic Telecommunications Access Method (BTAM) and Virtual Telecommunications Access Method (VTAM) access methods with Information Management System (IMS), Customer Information Control System (CICS), and Time Sharing Operation (TSO) application subsystems. Bisync 3270 protocol is supported using ASCII/odd, ASCII/CRC, and or EBCDIC codes. Both half-duplex and full-duplex transmissions are supported by the EIA RS-232-C and V.35 communication channels.

This downloadable module accepts software from the Control Computer.

A SYNC8 module cannot be used simultaneously for host and terminal service. When used for terminal and CU connections, the CUs view the module as a 3270-type host. When used for host connections, the host views the module as a CU. When configuring the module to interface to a

host, it is necessary to define virtual CUs and terminals. The number of virtual CUs and terminals must be equal to or greater than the number of physical CUs and terminals. This will allow all users wishing to call the host the ability to do so. The SYNC8 module interfacing to a synchronous host should be configured following the configuration of the host.

The SYNC8 module is made up of a SYNC8 board (MC1D089A1) and one of four available I/O distribution boards. By using the appropriate I/O distribution board, customers can configure the module as a DCE or DTE. The following I/O distribution boards can be used with the SYNC8 module:

- ***AWJ5*** provides one DTE V.35 connection for a line operating at 56 Kbps, and three DCE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6, or 19.2 Kbps. Clocking is provided for the DCE ports only. The bottom 50-pin connector is used to access port 1 (V.35) and the top 50-pin connector is used to access ports 2, 3 and 4 (EIA RS-232-C).
- ***AWJ6*** provides one DTE V.35 connection for a line operating at 56 Kbps, and three DTE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6 or 19.2 Kbps. External clocking is required for all ports. The bottom 50-pin connector is used to access port 1 (V.35) and the top 50-pin connector is used to access ports 2, 3, and 4 (EIA RS-232-C).
- ***AWJ17*** provides eight DTE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6 or 19.2 Kbps. External clocking is required.
- ***AWJ18*** provides eight DCE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6 or 19.2 Kbps. Clocking is provided.

The SYNC8 module can occupy any slot on a shelf except where precluded by other requirements. Diagnostics available for the SYNC8 include five types of on-line loopback tests and off-line component diagnostics that are started by the administrator's command.

TERM32 (UN315)

A TERM32 can be placed only in the SAM504 and SAM64. The TERM32 module provides the interface for 32 EIA RS-232-C ports that can be administered independently to support synchronous transport. When configured for synchronous service, speeds of 110, 300, 1200, 2400, 4800 and 9600 bps are supported. SAM ports can accept data from attached devices at the maximum rates, independent of other activity on the SAM. For synchronous traffic the throughput per station is about 50 Kbps.

The synchronous protocols supported by SAM ports are all windowing protocols, including ALC, SDLC, HDLC, Bisync, DDCMP, LAPB/X.25, Burroughs Poll/Select, and Uniscope. For Bisync it supports ASCII and EBCDIC coding. For ASCII coding, NRZI signaling is supported. For most SAM applications the window size will be less than the 1827 byte SAM buffer. As a result, most devices connected to SAM ports would stop transmitting data because of their own windowing protocol before they would overflow the SAM buffers.

Users should follow engineering guidelines specified in the *Planning Guide* to set flow control mechanisms within the protocols to limit the amount of data sent to the TERM32 and thus eliminate buffer overruns.

The TERM32 is used with the following I/O distribution board:

- ***ED2P466-30,G1*** is used with the TERM32 in the SAM504. No I/O distribution board is required with the TERM32 in the SAM64.

More information on the TERM32 is provided earlier under Asynchronous Service.

CPY1

The CPY1 module can only be placed in the SAM16. It supports eight EIA RS-232-C ports. Each port can be administered independently to support synchronous transport.

When configured for synchronous service, the sixteen full-duplex ports can run at speeds of 110, 300, 1200, 2400, 4800, 9600, and 19200 bps, and can accept data from attached devices at the maximum rates, independent of other activity on the CPY1.

The synchronous protocols supported by CPY1 ports are all windowing protocols, including ALC, SDLC, HDLC, Bisync, DDCMP, and Uniscope. For Bisync the CPY1 supports ASCII and EBCDIC coding. For ASCII coding, NRZI signaling is supported. For most CPY1 applications the window size will be less than the 3683-byte SAM buffer. As a result, most devices connected to CPY1 ports will stop transmitting data as a result of their own windowing protocol before they overflow the CPY1 buffers.

Users should follow engineering guidelines specified in the *Planning Guide* to set flow control mechanisms within the protocols to limit the amount of data sent to the CPY1 and thus eliminate buffer overruns.

CPY1 support for asynchronous communication is described under Asynchronous Service.

X.25 and X.75 Interfaces

Compliance with 1988 CCITT recommendations for X.25 and X.75 services is accomplished through the X.25, X.25P, and X.75 modules. The X.25 and X.25P modules provide transport of X.25 traffic for both SVCs and PVCs, as well as an integral asynchronous PAD service, which supports CCITT Recommendations X.3, X.28, and X.29. Both X.25 modules interwork with each other, with the X.75 module, and with all supported asynchronous modules in PAD mode.

The following interface modules are provided:

- ***X.25*** is the basic X.25 interface for speeds up to 64 Kbps.
- ***X.25P*** is the enhanced X.25 interface for speeds up to T1/E1.
- ***X.75*** is the standard X.75 interface at speeds up to T1/E1.

X.25 Module (TN2094)

The X.25 module consists of an X.25 board and one of four available I/O distribution boards. By using the appropriate I/O distribution board, customers can configure the module as DCE or DTE. Each X.25 module supports up to 100 virtual circuits. Lines operate in full-duplex transmission. The module provides clocking for DCE ports; external clocking by a modem or a DSU is required

for DTE ports. Diagnostics available for this module are described in the *X.25 and X.25P Module Reference.*

Throughput on the X.25 module can be engineered through several user facilities available via administration. User facilities support configuring the module to support nonstandard default packet and window sizes for all logical channels on a module for both switched and permanent virtual circuit calls. Packet sizes of 128 and 256 octets are supported, with 128 the default, constrained to the same value for both directions of data transmission. Window sizes of 1 through 3 are supported, with 2 the default, constrained to the same value for both directions of data transmission.

In addition, some optional user facilities are supported, including the following:

- incoming/outgoing calls barred
- packet and window size negotiation (to lowest common value)
- T1 timer and N2 parameter configuration.

The following I/O distribution boards can be used with the X.25 module:

- ***AWJ5*** provides one DTE V.35 connection for a line operating at 48, 56, or 64 Kbps, and three DCE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6, or 19.2 Kbps. Clocking is provided for the DCE ports only. The bottom 50-pin connector is used to access port 1 (V.35) and the top 50-pin connector is used to access ports 2, 3 and 4 (EIA RS-232-C).
- ***AWJ6*** provides one DTE V.35 connection for a line operating at 48, 56, or 64 Kbps, and three DTE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6 or 19.2 Kbps. External clocking is required for all ports. The bottom 50-pin connector is used to access port 1 (V.35) and the top 50-pin connector is used to access ports 2, 3, and 4 (EIA RS-232-C).
- ***AWJ17*** provides four DTE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6 or 19.2 Kbps. External clocking is required. The top 50-pin connector only is used to access ports 1 through 4.
- ***AWJ18*** provides four DCE EIA RS-232-C connections for lines operating at 1.2, 2.4, 4.8, 9.6 or 19.2 Kbps. Clocking is provided. The top 50-pin connector only is used to access ports 1 through 4.

X.25P Module (MC1D153A1)

The X.25P module is a single-board interface that supports either four V.35 DTE ports or eight RS-232 DCE/DTE (configurable on a per port basis) ports, depending on the I/O board chosen. The X.25P is a downloadable module which supports a maximum of 507 channels. It can reside in a node or in an MPC15 or MPC7.

All of the 1988 CCITT X.25 Recommendation mandatory facilities are supported. In addition, many optional facilities are supported, all configurable on a per port basis. Among them are the following:

- packet sizes of 128, 256, 512, and 1024 octets

- Level 3 window sizes of 1-7
- throughput classes from 75bps to 64Kbps
- segmentation (packet sizes can be different in each direction of transmission)
- window sizes can be different in each direction of transmission
- support of modulo 128 and modulo 8 numbering at Level 2
- support of D-bit for end-to-end acknowledgement
- hunt group address substitution.
- X.25 SVC-to-PVC connectivity

In addition, certain application-specific capabilities are available as part of the X.25 or asynchronous PAD service, including the following:

- the ability for a switched asynchronous user to call an X.25 PVC
- default calling address substitution
- configurable channel "offset" for the SVC channel range — indicates the "offset" for the logical channel number (LCN), according to Annex A of the CCITT X.25 Recommendation.

Diagnostics for the X.25P module are described in the *X.25 and X.25P Module Reference*. An ISO-compliant test frame test is provided. When a test command frame is received, a test response frame, containing the same information field as the command frame, is returned to the module.

The following I/O boards can be used with the X.25P module:

- ***AWJ24*** has up to four data terminal equipment (DTE) ports that can be configured for V.35 connections for lines operating at 48, 56, or 64 Kbps. For speeds greater than 64 Kpbs, 1 to 2 ports (depending on packet size) can be configured for speeds up to E1 rate. See the *Data Networking Products Planning Guide* for more information. The AWJ24 I/O board can be used with an external conversion device (such as a modem) for G.703 connections. External clocking is required for all ports.
- ***CSD4*** has eight ports that can be configured independently for RS-232-C connections as DTE or DCE for lines operating at 1.2, 2.4, 4.8, 9.6, or 19.2 Kbps. Internal clocking is provided for all DCE ports, and external clocking is required for all DTE ports.

X.75 Module (MC1D143A1)

The X.75 is a single-board interface module that consists of the MC1D143A1 main circuit pack and the AWJ24 I/O distribution board. The module and its I/O board can reside in the node, or in a 7- or 15-slot Multipurpose Concentrator (MPC7 or MPC15). The X.75 module conforms to the 1988 CCITT X.75 Recommendation.

X.75 module ports function as national or international gateways for switched virtual circuit (SVC) or permanent virtual circuit (PVC) service between BNS-2000 and other PSPDNs. The X.75 module thus allows BNS-2000 to serve as a public national network or as an originating or

destination network when connected to an international network. BNS-2000 supports calls to an unlimited number of national networks and up to 256 international gateways.

Connections between synchronous endpoints are implemented as SVCs or PVCs. Connections to asynchronous endpoints are handled by the X.75 module's integrated Packet Assembler/ Disassembler (PAD).

The AWJ24 I/O board supports up to four data terminal equipment (DTE) ports that can be configured for V.35 connections. The board can also be used with an external conversion device (such as a modem) for G.703 connections. Up to 507 logical channels are available per module.

Special Purpose Interfaces

Two special purpose interface modules provide services for the CO OSN environment. The E2A module supports asynchronous communications; the SLM module supports synchronous communications.

The following special purpose interface modules are supported:

- ***E2A*** is a special purpose module dedicated to telemetry service for SCCS/TNM.
- ***SLM*** is a two-board, special-purpose module dedicated to BX.25 service.

E2A (TN1012)

The E2A module provides E2A telemetry service for the Total Network Management (TNM) Operations System. The code for the E2A module is stored in EPROM on the board. Two types of loopback tests are provided for the E2A module. Both types of diagnostics interrupt service to the port.

The code for the E2A module has been customized to meet the needs of the TNM and is not available for other applications. E2As can receive calls from CPM-connected devices only. E2A endpoints cannot originate calls. E2A modules are supported in nodes and in the MPC15. The ED5P074-30,G1 I/O distribution board is used with the E2A module.

SLM (MC5P025A1/UN221)

The SLM provides BX.25 Issue 2 service for several OSs, including the TNM and the Traffic Data Management System (TDMS). The SLM provides the interface to four BX.25 Issue 2 synchronous data links, each operating at 2400 bps or 9600 bps. The hardware used for the SLM module is a two-board set consisting of a single-board processor (MC5P025A1) and an SC/DKI interface board (UN221). These boards must occupy two adjacent, addressable slots. The software for the SLM module is downloaded from an OS host. The SLM module performs the BX.25 Issue 2 processing for Levels 1, 2, and 3. The SLM can only receive calls from a CPM-connected TNM or TDMS host processor. The SLM cannot originate calls. The SLM is supported in nodes and in the MPC15. It uses two I/O distribution boards:

- ***ED5P077-30,G1*** for the SC/DKI

- ***ED5P080-30,G1*** for the single-board processor.

Customer Programmable Interface

Networks that have special communications processing needs can use the BNS-2000 integrated applications feature. This feature allows AT&T-provided applications to be programmed in the Portable Development Environment (PDE) for use on a module called the DKAP module. Examples of these applications include context switching, protocol conversion, and security protection. AT&T can implement specialized application programs to satisfy your needs. Contact your AT&T account representative for details.

The DKAP is a plug-in module that includes a processor, 64 KB of ROM, 2 MB of RAM, and an interface to the node backplane. The DKAP is not equipped with an I/O distribution board. It provides customized protocol support within the node. The DKAP, which is a downloadable module, cannot be used without customized programming.

Trunk Modules

BNS-2000 networks that include concentrators, have more than one node, or interwork with other kinds of nodes depend on trunk transmission lines. BNS-2000 provides trunk modules for coaxial, fiber and wire trunks.

Coaxial Trunk Modules

Coaxial trunk modules are available for Series M2 cabinets and support both CLNS and CONS services. Coaxial trunks operate at T3 or E3 speeds (44.74 Mbps or 34.368 Mbps).

The following coaxial trunk modules are available:

- ***Trunk-T3S*** carries traffic between two BNS-2000 nodes at T3 speeds (44.736 Mbps).
- ***Trunk-E3S*** carries traffic between two BNS-2000 nodes at E3 speeds (34.368Mbps).
- ***Trunk-T3I*** carries CLNS traffic between a BNS-2000 node and another carrier's network and supports ICI-LEC, ICI-IC, and ICI-SA at T3 speeds.
- ***Trunk-T3A*** can connect two BNS-2000 Series M2 Shelves either directly or through an ATM network.
- ***Trunk-E3A*** can connect two BNS-2000 Series M2 Shelves either directly or through an ATM network.

Trunk-T3S (CMA13)

The Trunk-T3S is a downloadable module. It supports the North American ANSI DS3 standard interface. The Trunk-T3S carries both connectionless and connection-oriented traffic for speeds up to 44.736Mbps. The Trunk-T3S also supports CIR for frame relay traffic.

The Trunk-T3S provides communication between two BNS-2000 Series M2 Shelves.

The Trunk-T3S uses the CMC6B I/O board, which provides one DS3 transmission facility interface.

Trunk-E3S (CMA13)

The Trunk-E3S is a single port DS3 trunk module that supports both connectionless and connection-oriented traffic between two BNS-2000 Series M2 Shelves. The Trunk-T3S also supports CIR for frame relay traffic. It operates at speeds of up to 34.368Mbps. The Trunk-E3S supports the European E3 standard interface. Its interface is a BNC coaxial cable; its distance limit to the node is 900 feet.

The Trunk-E3S provides communication between two BNS-2000 Series M2 Shelves.

The Trunk-E3S is a downloadable module. It uses the CMC13B I/O board, which has two micro-coaxial cable connectors, one for transmit and one for receive.

Trunk-T3I (CMA14/CMA16)

The Trunk-T3I is a two-board downloadable module. It supports the North American ANSI DS3 standard interface. The Trunk-T3I carries only connectionless traffic at speeds up to 44.736 Mbps consistent with the Bellcore ICI specification TR-TSV-001060. Using a BNC coaxial cable, the Trunk-T3I connection limit is 900 feet.

The Trunk-T3I provides an ICI connection between a BNS-2000 node and another carrier's network.

The Trunk-T3I consists of an egress module (CMA14) and an ingress module (CMA16). The CMC6B (egress) and CMC14 (ingress) I/O boards provide the connection between the two modules and the facility DS3 line interface.

Trunk-T3A (CMA18)

The Trunk-T3A supports both connectionless and connection-oriented traffic. The Trunk-T3A also supports CIR for frame relay traffic.

The Trunk-T3A can directly connect two BNS-2000 Series M2 Shelves, or can connect two Series M2 Shelves through an ATM network.

The Trunk-T3A is a single port DS3 trunk module that uses the CMC15 I/O board.

Trunk-E3A (CMA18)

The Trunk-E3A supports both connectionless and connection-oriented traffic. The Trunk-E3A also supports CIR for frame relay traffic.

The Trunk-E3A can directly connect two BNS-2000 Series M2 Shelves, or can connect two Series M2 Shelves through an ATM network.

The Trunk-E3A uses the CMC16 I/O board.

Fiber Trunk Modules

Fiber trunk modules are available that support internodal connections and connections between most concentrator types and the home node. Fiber trunks operate at the 8 Mbps backplane speed of the Series M1 Shelf.

The following fiber trunk modules are available:

- ***Trunk-HS*** provides a fiber interface for transport of CONS traffic between nodes. It also can be used to connect nodes to SAM64 and SAM504.
- ***SFT*** is a fiber interface for transport of CONS traffic between nodes.

Trunk-HS (TN1010)

The Trunk-HS module resides in a Series M1 Shelf and provides a limited-distance high-speed point-to-point communication link between a BNS-2000 node and

- a BNS-2000 node,
- a *Datakit* II VCS node, or
- a SAM504 or SAM64. Its SAM counterpart is the HS-Trunk module.

The high-speed link runs at 8 Mbps on optical fiber to a maximum length of 3 km. The Trunk-HS module supports a maximum of 2042 virtual circuits for end users.

The Trunk-HS module uses CRC error-checking to identify bad frames, which are then discarded. Error correction is the responsibility of higher-level protocols.

The AWJ2 I/O distribution board is used with the Trunk-HS module.

Standard Fiber Trunk (SFT) (MC1D085A1)

The SFT module resides in a Series M1 Shelf and provides a limited-distance high-speed point-to-point communication link between a BNS-2000 node and:

- a BNS-2000 node,
- *Datakit* II VCS nodes, or
- Multipurpose Concentrators.

The maximum cable length of the SFT is 3 km. Fiber extenders can be used with the SFT to increase this distance to 15 km. SFT trunks operate at standard speeds up to 8 Mbps, and support up to 2042 user channels. The SFT module is used with the AWJ3 I/O distribution board.

Wire Trunk Modules

Wire trunks are available for internodal connections operating at speeds from 2.4 Kbps to 2.048 Mbps, including T1 and Fractional T1 (F-T1) speeds. They reside in Series M1 Shelves and are used for connection-oriented traffic.

The following wire trunk modules are supported:

- ***SWT*** provides a wire connection supporting up to 506 virtual circuits, at speeds from 2.4 Kbps to 2.048 Mbps.
- ***Trunk-T1*** provide long-distance, high-speed, point-to-point communication over a T1 digital transmission facility.
- ***Trunk-PQ*** is a single port wire trunk for facilities at speeds of 56 Kbps to 2.048 Mbps.
- ***Trunk-64*** provides a wire trunk interface at speeds of 9.6 Kbps to 64 Kbps.
- ***SAMSL*** is used for a single link trunk from a node to a SAM8, SAM16, SAM64, or SAM504. It supports facility speeds of 9.6 Kbps to 64 Kbps.
- ***SAMDL*** is used for a dual link trunk from a node to a SAM64. It supports two EIA RS-232-C connections at a combined throughput of 9.6 or 19.2 Kbps.

- ***SAMML*** is a multiple link interface from a node to SAM16s, SAM64s, or SAM504s. It supports a total link bandwidth of 128 Kbps.

Standard Wire Trunk (SWT) (TN2092B)

The SWT module in a Series M1 Shelf provides a wire trunk interface between BNS-2000 nodes and:

- a BNS-2000 node,
- a *Datakit* II VCS node, or
- Multipurpose Concentrators.

The SWT can have up to 506 channels and operates at the following configurable standard speeds: 2.4, 4.8, 9.6, 19.2, 48, 56, or 64 Kbps; or up to T1/E1 speeds. It uses HDLC framing, provides bit and byte stuffing, and has a high- and low-priority queuing algorithm. The connections between nodes and the equipment listed above include DSUs located at either end of a T1 trunk facility.

A variety of connections can be made by selecting one of the three appropriate I/O distribution boards:

- ***AWJ9*** provides a V.35 DTE interface to the SWT with or without NRZI encoding.
- ***AWJ10*** provides an EIA RS-422/449 DTE interface with or without NRZI encoding.
- ***AWJ11*** provides an EIA RS-232-C DTE interface to the SWT. It is connected to a data service unit (DSU) that interfaces to a channel service unit (CSU).
- ***AWJ33*** provides a G.703 interface for use in international applications.

Trunk-T1 (TN1015)

The Trunk-T1 module provides a long-distance high-speed point-to-point communication link between a BNS-2000 node and the following:

- a BNS-2000 node,
- a *Datakit* II VCS node, or
- a SAM504 or SAM64. Its counterpart in the SAM is the T1-Trunk module (TN1392).

The Trunk-T1 supports a maximum of 2042 virtual circuits and presents a V.35 type (34-pin) or EIA RS-449 type (37-pin) connection through an AWJ4 I/O distribution board.

Most applications will require the use of a DSU/CSU to provide network protection, automatic loop equalization, and maintenance loopback testing between the DSU and the T1 network.

The Trunk-T1 module uses CRC error-checking to identify bad frames, which are then discarded. Higher-level protocols are responsible for the correction of bad frames.

Loopback tests are provided for the Trunk-T1 module. Diagnostic procedures are described in the *Trunk Module Reference*.

Trunk-PQ (MC1D152A1)

The Trunk-PQ (MC1D152A1) is a single-port wire interface that provides fair queuing and enhanced buffering for multi-protocol traffic, and support of CIR for frame relay traffic at up to T1/E1 rates throughout the network.

The Trunk-PQ provides communication between a BNS-2000 node and the following:

- a BNS-2000 node, or
- a *Datakit* II VCS node.

Various parameter options can be configured to avoid congestion and data loss over the Trunk-PQ. The Trunk-PQ module supports a maximum of 2038 user channels for non-CIR traffic, or a maximum of 502 channels when **`TRAFFIC TYPE`** is configured for *cir* or *both*.

The **Troubleshooting** chapter of the *Trunk Module Reference* describes the diagnostic tests provided for the Trunk-PQ.

The Trunk-PQ uses an AWJ24 I/O distribution board, which provides a V.35 DTE connection from the Trunk-PQ to the external device.

Trunk-64 (MC1D105A1)

The Trunk-64 module provides communication over a Digital Data Service (DDS) line between a BNS-2000 node and:

- a BNS-2000 node (at 64 Kbps and below), or
- a *Datakit* II VCS node.

The Trunk-64 operates at speeds up to 64 Kbps, and supports up to 504 virtual circuits. The module can also operate as an interface to an analog carrier up to 9.6 Kbps, using modems, or 19.2 Kbps, using duoplexors. The module can be configured for either an EIA RS-232-C or a V.35 interface.

The Trunk-64 module consists of single board processor (TN2165B).

The Trunk-64 uses a CRC to detect bad frames, which are then discarded. Error correction is the responsibility of higher level protocols.

Loopback tests are provided for the Trunk-64. The *Trunk Module Reference* describes diagnostics.

The following two I/O distribution boards can be used with the Trunk-64:

- ***AWJ9*** provides two V.35 DTE ports, of which only one is used. An external DSU is required.
- ***AWJ11*** provides two EIA RS-232-C DTE ports, of which only one is used. It is connected to a DSU that interfaces to a CSU.

The Trunk-64 can communicate with a Trunk-DDS on another node. The Trunk-64 has replaced the Trunk-DDS, which is discontinued.

Synchronous/Asynchronous Multiplexer Single Link (SAMSL) (MC1D090A1B)

The SAMSL module is the wire interface at each end of an analog transmission facility connecting a BNS-2000 node and a SAM. It supports EIA RS-232-C connections at 9.6 or 19.2 Kbps and V.35 connections up to 64 Kbps, and provides up to 504 user channels. This module provides software for boot-up diagnostics, loop diagnostics, and channel selection.

The SAMSL is used with the following I/O distribution boards:

- ***AWJ9*** provides two V.35 DTE ports when placed in the node, of which only one is used. This connects to a CEY2 I/O distribution board in the SAM64, which provides one V.35 DTE port, or to an EAA2 single-port V.35 DTE I/O distribution board in the SAM504. An external DSU is required.
- ***AWJ11*** provides two EIA RS-232-C DTE ports when placed in the node, of which only one is used. This connects to a CEY3 I/O distribution board in the SAM64, which provides one EIA RS-232-C DTE port. An external DSU is required.

Synchronous/Asynchronous Multiplexer Dual Link (SAMDL) (MC1D106A1)

The SAMDL module is the dual wire interface located in a SAM64 that provides connections over an analog transmission facility to a SAMML in the BNS-2000 node. The SAMDL supports two EIA RS-232-C connections at a combined throughput of 9.6 or 19.2 Kbps.

The two links connect to the same SAMML module in the node and provide dynamic load sharing of user traffic. This feature improves end-to-end network performance delay.

Control software in the node monitors the status of the links. If one of the links goes down for a period of time that is equal to a failure detection threshold, all user channels are automatically routed to the other link. When the failed link comes up for a period of time equal to a recovery detection threshold, the link is automatically restored and all user channels are redistributed according to the load sharing scheme. Both thresholds can be administered by the network administrator.

The SAMDL provides software for boot-up diagnostics, loop diagnostics, and traffic and status measurements. Service diagnostics include the ability to remove and restore individual links, with traffic rerouted to the link remaining up when the other link is removed from service.

The SAMDL uses the following I/O distribution board:

- ***CEY4*** provides circuits for two RS-232-C DTE ports through a single female RS-232-C port. This port supports two trunks via an ED5P055-31,G219 "Y" cable that connects via its common end to the CEY4 I/O distribution board while the split ends connect to the modems/DSUs for the two trunks.

Synchronous/Asynchronous Multiplexer Multiport Link (SAMML) (MC1D091A1)

The SAMML module provides wire connections from the BNS-2000 node to up to eight remote SAMs. It supports up to 507 user channels to the SAM. It can be installed in the node only, where it takes up only one slot while providing ports for links to eight SAMs. Its counterpart in the SAM is the SAMSL or the SAMDL in the SAM64.

The SAMML is used with the following I/O distribution boards:

- ***AWJ9*** provides two V.35 DTE ports, of which only one is used, at speeds of 56 or 64 Kbps.
- ***AWJ17*** provides eight EIA RS-232-C DTE ports. They can be configured as follows: eight lines operating at 9.6 Kbps (full-duplex), or four lines operating at 19.2 Kbps, with a total bandwidth of 128 Kbps.
- ***AWJ32*** provides one V.35 DTE port for a line operating at a speed of 56 or 64 Kbps.

Software Packaging and Configuration

Software Packaging and Configuration

This chapter contains information about BNS-2000 software packaging and distribution, the mechanics of adding optional Feature Packages, the centralized release download feature, and basic system software organization for each of the two standard control configurations — single Control Computer configuration and dual Control Computer configuration.

Software Packaging

The operating system software comes on a cartridge tape. For each right-to-use fee, the customer is shipped a tape containing the release and a set of documentation.

The operating system software is then read from the release tape to the fixed disk. In dual Control Computer configurations, the software must be copied to the secondary disk as well as the primary disk.

Feature Selection

Feature packaging allows customers to select and purchase, via the software right-to-use (RTU) fee, modular BNS-2000 software packages that support services appropriate for specific environments. Services are grouped into software feature packages that provide selectivity ranging from basic node support to full data services and special capabilities.

- ***Basic Feature Package*** offers standard support for the node and basic asynchronous and synchronous interfaces, multiplexed host interfaces, X.25 and X.75 interfaces, special purpose interfaces, the integrated applications processor, internodal trunks (except ATM), and concentrators.
- ***Optional Feature Packages*** can be added to the Basic Feature Package through supplementary packages, as follows:
  - Frame Relay Feature Package
  - SMDS Feature Package
  - ATM Feature Package
- ***Full Feature Package*** includes support for all features and services. It is equivalent to the Basic Feature Package and all optional packages listed above.

Table 5-1 lists the complete line of modules supported in the Full Feature Package as well as in the optional packages.

TABLE 5-1. Feature Packages

Components[1]	Base Feature Package	Optional Feature Packages		
		SMDS	Frame Relay	ATM
AIs/GAR		√		
Multiplexed Host Interface	√			
FRM-M2/FRM/LPM			√	
Asynchronous Interfaces	√			
MPCs/SAMs	√			
Trunks (except ATM)	√			
ATM Trunk				√
Synchronous Interfaces	√			
X.25/X.75 Interfaces	√			
Special Purpose Interface	√			
StarKeeper II NMS Interface	√			

1. Capabilities are activated by the packages checked; all are activated with the Full Feature Package.

System Software Organization

The fixed disk is organized in partitions or areas. Various Control Computer configurations use these partitions differently.

Single Control Computer Configuration

In a single Control Computer configuration, the processor is connected to its disk and tape devices via its primary SCSI bus. The Control Computer uses the following disk resources:

- *Active file system* — partition 0 contains the release software and configuration information used by the Control Computer. The Control Computer boots from the active file system.
- *Staging file system* — partition 1 is used for loading a new software release and for backing out of the active release to an old release; this partition can contain another full release.
- *Auxiliary file system* — partition 2 contains scheduled measurements data readable by *StarKeeper* II NMS.
- *Backup area* — Node configuration database files are copied to this partition with the backup command. A retrieve command copies configuration database files from the tape, save area, or host into this partition.

  When the system is booted, if there is configuration information in the backup partition of the disk, the Control Computer loads the backup information into the active file system.
- *Save area* — An off-line copy of disk configuration information can be stored in this partition. The network administrator can specify this area as the target or source of optional commands that backup and retrieve the database. One backup command copies configuration information from the active file system to the specified save area partition. A parallel retrieve command copies configuration information from the specified save area partition to the backup area partition on the disk currently used by the active Control Computer. The system does not automatically write to or read from the save area.

Dual Control Computer Configuration

For nodes optioned with high availability, the basic configuration is backed up by a redundant basic configuration: two Control Computer configurations. In a typical configuration, one Control Computer configuration resides in any Series M1 cabinet, and the second interconnected Control Computer configuration resides in the next higher-numbered Series M1 cabinet. For a CCM only, both Control Computer systems can reside in the same Series M1 cabinet.

The (required) MRC function, which ensures that one processor (either CC0 or CC1) is the *active* Control Computer and the other processor is the *standby* Control Computer, is required in the lower-numbered cabinet or slot.

The Control Computers use the following disk resources:

- *Active file system* — Partition 0 contains the release software and configuration information used by the currently active Control Computer. The active Control Computer boots from the active file system on its primary disk; that is, if CC0 is active, it boots from the active file system on disk 0. If the primary disk fails, the active Control Computer will use the active file system on its secondary disk; that is, disk 1 for CC0. If CC1 is active, it boots from Disk 1; if disk 1 fails, it boots from disk 0.
- *Staging file system* — Partition 1 is used for loading a new software release and for backing out of the active release to an old release; this partition can contain another full release.
- *Auxiliary file system* — Partition 2 contains scheduled measurements data readable by *StarKeeper* II NMS.
- *Standby file system* — Partition 3 contains a subset of the release software used by the current standby Control Computer. The standby Control Computer boots a diagnostic program called *bstat* from the standby file system on its primary disk; that is, if CC1 is standby, it boots from the standby file system on disk 1. If the primary disk fails, the standby Control Computer will use the standby file system on its secondary disk; that is, disk 0 for CC1.
- *Backup area* — Node configuration database files are copied to this area using a backup command. A retrieve command copies database files from the tape, save area, or host into this partition of the active disk. When the system is booted, if there is configuration data in the backup partition of the active disk, the Control Computer loads the backup data into the active file system and uses it to configure the node.

  When automatic backup is enabled, the active Control Computer periodically copies the current configuration information to the backup area on the non-active disk; that is, when active CC0 has been booted on disk 0, it copies configuration changes to the backup area on disk 1. If automatic backup is not enabled, the network administrator can use a backup command to perform the same operation manually.

  When the system is booted, if the configuration information in the backup partition of the currently active disk is newer than the information in the active file system, the Control Computer loads the backup information into the active file system.
- *Save area* — An off-line copy of disk configuration information can be stored in this partition. A separate save area exists on disk 0 and on disk 1. The node administrator can specify either area as the target or source of optional backup and retrieve commands. One backup command copies configuration information from the active file system to the specified save area partition. A parallel save command copies configuration information from the specified save area partition to the backup area partition on the disk currently used by the active Control Computer. The system does not automatically write to or read from the save area.

Upgrading Capability

An existing BNS-2000 database can be upgraded to the current release using procedures detailed in the *BNS-2000 Node Reference*.

Upgrades to existing databases will occur independently of the current release feature package arrangement. That is, all modules in an existing database will be upgraded to the current release and will be usable, as long as the relevant feature packages have been installed on the node.

Users have choices for upgrading their networks to take advantage of the current BNS-2000 features and services as follows:

- *StarKeeper* II NMS can be used to upgrade the network database to the current release
- A database transfer service is provided (see **Support and Services**).

Centralized Release Download

New generic or maintenance release software can be downloaded to geographically dispersed BNS-2000 nodes from a *StarKeeper* II NMS core system host. This feature is already enabled if upgrading from Release 3.0. For pre-3.0 nodes, the centralized release download feature will be enabled after the node is upgraded to Release 4.0 by present methods.

After the node's initial conversion to Release 4.0, any release can be downloaded to it while the node is running. Then a cutover to the new release can be executed remotely. *StarKeeper* II NMS must have sufficient disk space to store each release. If a cutover is not successful, the node can be reverted to the previous release within minutes.

Control Computer hardware upgrades cannot use this procedure.

Related Products

Related Products

This chapter describes a range of products that are manufactured by AT&T Network Systems and are in the BNS-2000 product family, products manufactured by AT&T that are compatible with BNS-2000, and products manufactured by external vendors that are certified to work with BNS-2000.

Billdats Network Server

Together with BNS-2000, the Billdats Network Server provides usage-sensitive billing for intra-LATA SMDS, in compliance with Bellcore specifications. The Billdats Network Server receives billing data from the BNS-2000 switch, processes the data, and transmits the processed data to a centrally located billing collector in a Revenue Accounting Office (RAO). It features a high reliability duplex configuration, with two identical, connected systems. If one system fails, the other takes over processing with no loss of data. Redundant disks also provide on-line backup of data.

The Billdats Network Server is part of a billing teleprocessing network comprising the following three main components:

- the BNS-2000 node is the billing source or network element
- the Billdats Network Server provides the Automatic Message Accounting Transmitter (AMAT) function
- the host collector (a Billdats II® Collector or other Automatic Message Accounting Teleprocessing System (AMATPS).

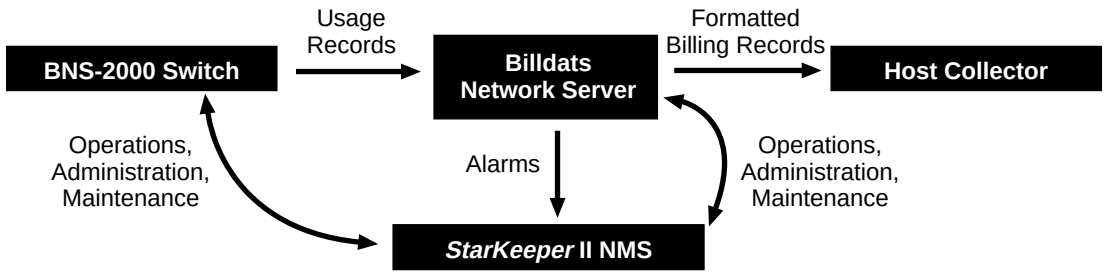

FIGURE 6-1. Billing Teleprocessing Network Systems

The billing source, or BNS-2000 node, collects raw billing data from the SMDS network and generates usage records for the Billdats Network Server.

The node counts the number of packets successfully transmitted over the network, and aggregates them into usage records for a unique source-destination address pair over a specific time period. This period is called the Stage 1 aggregation interval; in Release 1, the interval is 15 minutes.

The Billdats Network Server receives the usage records from the Stage 1 aggregation interval. The customer, however, can specify a time interval, called the Stage 2 aggregation interval, based on the customer's billing system. The Billdats Network Server can merge the Stage 1 intervals into a longer Stage 2 interval.

The Stage 2 interval must be a multiple of the Stage 1 interval. With the Stage 1 interval of 15 minutes, for example, and a Stage 2 interval of 45 minutes, the Billdats Network Server merges records from three Stage 1 intervals into one Stage 2 interval.

The Billdats Network Server formats the aggregated billing records, also called Automatic Message Accounting (AMA) data, in Bellcore Automatic Message Accounting Format (BAF), and stores the data, called *primary* data, on disk until it is requested by the host collector.

Upon request, the Billdats Network Server transmits the data to the host collector and retains a copy. The copy, designated *secondary* data, is stored on disk until overwritten by new primary data.

Operations, Administration, and Maintenance

System operations, administration, and maintenance, including alarm monitoring, is performed through *StarKeeper* II NMS. Once the Billdats Network Server is installed and set up, its billing aggregation, formatting, and transfer functions are performed automatically. An operator needs to monitor the system only if an alarm occurs.

Bellcore Requirements Compliance

The Billdats Network Server complies with Bellcore specifications needed to support SMDS billing, as follows:

- ***Usage-sensitive billing requirements*** — TR-TSV-000775, *Usage Measurement Generic Requirements in Support of Billing for Switched Multi-megabit Data Service*
- ***Format of billing records sent to the collector*** — TR-NWT-001100, *Bellcore Automatic Message Accounting Format (BAF) Requirements*
- ***AMATPS protocol for collector interface*** — TR-TSY-000385, *Automatic Message Accounting Teleprocessing System (AMATPS) Generic Requirements*
- ***Equipment standards for central offices*** — TR-NWT-000063, *Network Equipment Building System (NEBS) Generic Equipment Requirements*.

Ordering Information

The Billdats Network Server can be ordered with a BNS-2000 node, or as an add-on to an existing node. Consult your AT&T Account Executive.

LCS60 Network Interface for Ethernet

The LCS60 Network Interface for Ethernet (LCS60) provides high-speed connectivity between Ethernet LAN endpoints and AT&T data switches, including BNS-2000 VCS. The LCS60 is a replacement for the LCS50E.

The LCS60 provides TCP/IP, Serial Line IP (SLIP), and Point to Point Protocol (PPP) gateway services over a high-speed multiplexed fiber interface. *StarKeeper* II NMS and/or an SNMP manager provide central monitoring and control of a network of LCS60s. A high-performance processor card (Motorola 50 Mhz 197LE card based on the 88110 RISC processor) running SVR4 UNIX software, and a high-capacity hard disk drive (520 MB), allow up to 80 simultaneous sessions, which is a fifty percent improvement over the LCS50E. Other features include security through the AT&T Network Access Control System, Domain Network Server (DNS) support, and remote backup/restore and upgrade.

There are two TCP/IP gateway services: asynchronous-to-TCP and TCP-to-asynchronous. These features allow older and less expensive asynchronous devices or emulators to have access to LAN resources through Telnet services. Devices on TY, MSM, X.25, CPM, or SAM modules can access LAN resources through the LCS60.

For remote LAN services, there are also two services supported: SLIP and TCP/IP-over-PPP. These services allow a remote PC to have access to all TCP/IP services on a remote LAN through the LCS60 as long as SLIP or PPP is running on the remote PC. Telecommuters can now dial in to the AT&T packet network and exercise TCP/IP commands as ftp, telnet, or ping on their remote PC as if their PC were directly connected to the LAN at the main work location. PPP is a standard that will allow multiple protocols (TCP/IP, AppleTalk, IPX) to be multiplexed together. TCP/IP is the initial LCS60 offering over PPP. AppleTalk services over AppleTalk Remote Access Protocol (ARAP) and PPP are supported in Release 2.0. IPX is supported in Release 3.0.

Central network management of a network of LCS60s is easily accomplished through *StarKeeper* II NMS or an SNMP manager. Either can monitor status of LCS60s at a centralized location. *StarKeeper* II NMS provides the ability to configure and control a network of LCS60s at one location through one interface. One LCS60 can also back up and restore configuration files of other LCS60s over the BNS-2000 network. This capability eliminates the need for hands-on backups on each machine. Local tape drives are provided for an extra level of backup security.

Complete network security is achieved through the AT&T Network Access Control System. A predefined destination (PDD) can force users connected on the AT&T data switches to connect to the Network Access Controller (NAC) for authentication. Once authenticated, the user can request a TCP gateway session or a remote access session (such as SLIP) with an LCS60. From the LAN, all sessions bound for the AT&T data switches can also be forced to be authenticated by the NAC.

The LCS60 can be configured as a Resolver in the Domain Name Server (DNS), allowing the LCS60 to access a DNS Server for the translation of symbolic names into IP addresses. This configuration reduces the administration required for translating symbolic names to IP addresses; it is a more efficient mechanism for this translation than a static administered file on each LCS60.

Hardware-software kits for upgrading an LCS50E to an LCS60 are available.

Network Access Control System

The Network Access Control System augments the basic security of a BNS-2000, BNS-1000, or *Datakit* II VCS network. Release 5.0 consists of a server software package that runs on a Hewlett Packard 9000 Model 700 Series platform and converts the host into a Network Access Controller (NAC). Access controls, user identification and authentication, and auditing functions are implemented on the NAC. When users attempt to gain access to the network, the calls are directed to the NAC, which authenticates the user and then establishes connections to permitted destinations.

User Access, Identification, and Authentication

Users are given access through a unique identifier (UID) and a personal authenticator, either a password or a personal user authentication device. Once authenticated, the user can be connected only to hosts for which access is allowed.

An additional layer of security is provided through compatible hand-held authentication devices, which require a user to possess a personal identification number (PIN). The Network Access Control System supports Security Dynamics SecurID® devices. The SecurID card generates a one-time password based on a proprietary synchronized time algorithm.

The NAC disconnects calls after an excessive number of failed access attempts. When a call exceeds a threshold number of attempts, the NAC suspends the user's UID and sends an alarm to the security administrator, and, if configured to receive it, to *StarKeeper* II NMS.

User Features

Network user features include the following:

- easy access to available hosts or services through printouts of names of hosts the user is permitted to access
- the ability to use the same SecurID card in several different Network Access Control Systems, as determined by the administrator
- no need for re-authentication as long as the user maintains the same connection to the network
- firewall security for TCP/IP networks. In addition to the conventional approach to controlling access based on protocol and source/destination address, the firewall provides user-level authentication and audit trails. It supports four TCP/IP application services: Telnet Proxy, a service which enables terminal access to hosts; FTP Proxy, which enables file transfers; Relay

Proxy, which enables the relaying of certain protocols to a predefined destination; and Password-Update Proxy, which enables users to change their passwords or PINs.

Security Administration

The security administrator selects the type of authentication appropriate for the network, sets security threshold levels, and controls the full range of security-related activities.

Administration Features

Administration features include the following:

- Disconnection, suspension, and alarm thresholds can be selectively administered
- Authentication methods for the NAC can be set up globally or individually
- Users, or groups of users, can easily be added to or removed from security access control lists
- Network security auditing can be selectively scheduled for the NAC. Auditing of access attempts, violations, and password changes are all under the administrator's control
- TCP/IP dial-in security server add-on packages support TACACS authentication protocols
- Full command set restriction allows the NAC system administrator to control the command privileges of NAC subadministrators
- Database verification and synchronization allows the NAC system administrator to verify CSAC and RAC databases (for *Datakit* II VCS, BNS-1000, and BNS-2000-connected RACs only) and synchronize them if discrepancies are found
- Real-time monitoring for incoming and outgoing NAC call traffic, as well as historical data, is provided
- Point-of-origin information is passed to the destination host
- Network access restrictions for individual NAC users can be based on time of day or point of origin.

Customized System

The Network Access Control System is a modular system that offers customers a variety of options and controls. Starting with one processor that provides network access control and security administration (the stand-alone NAC), the system can easily be expanded. Multiple NACs can function independently, or a distributed system can include from two to 25 Remote Access Controllers (RACs) under the control of a Central Security Administration Controller (CSAC). The CSAC can control RACs connected to a *Datakit* II VCS/BNS-1000/BNS-2000 network as well as RACs connected to a TCP/IP network.

Support Services and Documentation

AT&T offers a full range of support services and documentation for the Network Access Control System. Consult your AT&T Account Representative for more information.

DSUs/CSUs

Data service units and channel service units are available for use in many different applications, including internodal trunks, frame relay, SMDS, ATM, 64 Kbps, T1, E1, T3 and E3. See the *Data Networking Products Ordering Guide* for more information on the DSU/CSU products currently available.

Voice/Data Multiplexers

Adding a BNS-2000 node to a CO (along with the appropriate compatible equipment) provides support for either data transmission only, or simultaneous voice and data transmission. AT&T voice/data multiplexers (VDMs) connect to all BNS-2000 nodes via local loops:

- *AT&T VDM* — These point-to-point multiplexers support CO-LAN and customer premises data networking, allowing end users simultaneous, independent voice and data communication through their current telephone lines. A multiplexer at the customer premises, known as a Remote VDM (R-VDM), and a complementary multiplexer at the CO (C-VDM) are used to multiplex and demultiplex the voice and data signals. Voice and data are combined at the customer's location and transported over the existing nonloaded local loop. The C-VDM, located near the BNS-2000 node, is a cabinet containing circuit cards, power units, a fan unit, and an alarm unit. It can be powered by 115/220 VAC or –48 VDC. The C-VDM circuit cards multiplex/demultiplex voice and data signals, with the voice signals going over cables to a Main Distribution Frame (MDF) for cross-connection to the voice switching network. Data signals are sent to asynchronous or synchronous ports on the BNS-2000 node.

  The R-VDM uses 110 VAC power (220 VAC, international). For each R-VDM, there is one complementary C-VDM card.

  The AT&T VDM can transmit asynchronous or synchronous data up to 19.2 Kbps, half-duplex or full-duplex, over nonloaded 2-wire twisted pair lines.

  Five test modes are available for troubleshooting and fault isolation, two are user-initiated, the other three are initiated from the BNS-2000 administrative console or the *StarKeeper* II NMS.

Modem Eliminators

Modem eliminators connect RS-232 and V.35 standard interface DTEs together without modems and monitor the connection with RS-232 test equipment. VIR, Inc. provides the following features in their MOD Series equipment:

- standalone and rackmount models
- data rates between 2.4 Kbps and 6.144 Mbps
- internal/external clock or no clock
- modem handshaking emulation to both DTEs
- front panel loopback switch
- 110–220 VAC, 47–63 Hz, and -48 VDC models

Switched Network Modems

Modem pools can be established on BNS-2000 for either dial-in or dial-out purposes. BNS-2000 ports are dedicated for either answering or originating calls, but not for both at the same time. Thus a separate modem pool would have to be established for each purpose. The dial-in option allows fixed or autobaud connection between the external modem and BNS-2000. For dial-out purposes, the autodialer option provides an integral, automatic dialer that accepts the number dialed from stored memory or from the user's keyboard.

Dial-in Service

BNS-2000 ports arranged for answering calls have an autobaud capability of preselected baud rates up to 19.2 Kbps. The following AT&T modems are recommended for these applications:

- AT&T Dataphone II 2212C (300/1200 bps)
- AT&T Dataphone II 4024 (300/1200/2400 bps)
- AT&T Dataphone II 2224CEO (300/1200/2400 bps)
- AT&T Dataphone II 2248A (4800 bps)
- AT&T Dataphone II 2296A (4800/9600 bps).
- AT&T Paradyne 3800 (V.32, 14.4 Kbps)

Dial-out Service

The autodialer feature supports, via TY modules, certain AT&T dial-out modems at speeds of 300, 1200, 2400, 4800, and 9600 bps.

The supported two-wire, full-duplex, dial-line modems provide FCC-certified originate/answer transmission and reception of serial binary data over switched or leased telephone networks:

- AT&T 2212C/FDX
- AT&T Dataphone II 2224B
- AT&T Dataphone II 4024
- AT&T Dataphone II 2248
- AT&T Dataphone II 2224CEO
- AT&T Dataphone II 2224G
- AT&T Dataphone II 2296A
- AT&T Dataphone II 2296A with an optional Microcom™ Networking Protocol (MNP) plug-in board. MNP allows two modems to communicate error-free over the switched network. This error control method is similar to that of the AT&T 2296A.
- Penril® Autodata 1200, Model 8216
- Penril Datalink 2400®.
- AT&T Paradyne 3800 (V.32, 14.4 Kbps)

AT&T Systimax PDS

BNS-2000 networks can be used with an AT&T Systimax Premises Distribution System (PDS) wiring arrangement. The Systimax PDS is a specific cabling plan for a building or campus that connects telephones, data processing equipment, PCs, PBXs, LANs, and office equipment to each other and to outside networks in a total information transport system. The PDS consists of copper and optical fiber cable, electrical protection and grounding, and splicing facilities.

Support and Services

Support and Services

This chapter discusses support provided for BNS-2000. It contains information on training, documentation, customer assistance, maintenance, and support agreements.

Training

AT&T provides practical, hands-on training courses, available through the following organization:

AT&T Network Systems Customer Education and Training Center
5151 Blazer Memorial Parkway
Dublin, Ohio 43017-1392

1-800-TRAINER (872-4637)
1-800-221-1647 (In Canada)

When you call the toll free number, a voice service will explain the numbers to press on a touch-tone telephone for training information:

- Press 1 for information on UNIX System Education.
- Press 2 for AT&T telecommunications products and services training — **Press this number twice for BNS-2000 information.**
- Press 3 for Technical Education Center Services.
- Press 4 for AT&T School of Business, Management, and Virtual Workplace Education.
- Press 5 for all other training and education services.

Training courses for BNS-2000 and *StarKeeper* II NMS are listed below, with their recommended prerequisites. Other training may be useful for working with BNS-2000, for example, INFORMIX. Consult your AT&T sales representative on the appropriate courses for your BNS-2000 staff.

BNS-2000 Training Courses		
Number	**Course Title**	**Recommended Prerequisite**
UC4113	Data Communications I	None
NT3521*	Data Network Management via StarKeeper II NMS	NT3526, NT3505, NT3510, NT3511 or NT3513
NT3526	Introduction to BNS-2000	UC4113
NT3527	BNS-2000 Installation, Administration and Maintenance	NT3526, NT3505, NT3510, NT3511, NT3513, or NT3522

* Required for BNS-2000 system administrators.

Documentation

Documentation for the BNS-2000 product line includes installation guides and aids, user guides, trouble analysis guides, system administration guides and aids, and training documentation. Customer documents describing BNS-2000 and compatible products and equipment are orderable from the AT&T Customer Information Center (CIC); see the inside front cover of this *System Description* for ordering information.

BNS-2000 Customer Documentation

BNS-2000 customer documents provide the necessary information to plan, install, administer, maintain, and use the network efficiently. They contain detailed reference information on the system and its capacities, on network communications, and on all commands and error messages. A complete set of BNS-2000 customer documentation is provided with each system on delivery.

Customer documentation is described in the brochure *Data Networking Products Publications*, which briefly explains the contents of documents and points out titles appropriate to various audiences.

BNS-2000 Release 4.0 Customer Documentation		
CIC Select Code	**Issue Number**	**Title**
255-100-020	**Issue 1**	*Data Networking Products Ordering Set: Cabling Guide, Ordering Guide, Quick Reference*
255-100-021	**Issue 1**	*Data Networking Products Ordering Guide*
255-100-022	**Issue 1**	*Data Networking Products Quick Reference*
255-100-025	**Issue 4**	*Data Networking Products Cabling Guide*
***255-184-140**	**Issue 1**	*BNS-2000 Customer Documentation Library (paper plus CD-ROM)*
***255-184-141**	**Issue 1**	*BNS-2000 Customer Documentation Library (CD-ROM only)*
255-100-233	**Issue 1**	*Data Networking Products Administration Quick Reference*
255-100-235	**Issue 1**	*Data Networking Products Publications*
255-100-236	**Issue 1**	*Data Networking Products Terminal User Guide*
255-100-230 ISS 2	**Issue 2**	*Data Networking Products Planning Guide*
255-100-209	**Issue 1**	*Data Networking Products Session Maintenance Guide*
255-184-142	**Issue 1**	*BNS-2000 System Description*
255-184-104	**Issue 1**	*BNS-2000 SMDS Guide*
255-184-143	**Issue 1**	*BNS-2000 Node Reference*
255-100-234	**Issue 1**	*Data Networking Products Commands Reference*
255-100-228	**Issue 1**	*Data Networking Products Multipurpose Concentrator Reference*
255-100-203	**Issue 1**	*Data Networking Products Synchronous/Asynchronous Multiplexer Reference*
255-184-107	**Issue 1**	*BNS-2000 Access Interface Module Reference*
255-100-204	**Issue 1**	*Data Networking Products Computer Port Module Reference*
255-100-205 ISS 3	**Issue 3**	*Data Networking Products Frame Relay Module Reference*
255-100-237	**Issue 1**	*Data Networking Products Frame Relay Module–M2 Reference*
255-100-206	**Issue 2**	*Data Networking Products LAN Protocol Module Reference*
255-100-231	**Issue 1**	*Data Networking Products M2 Trunk Module Reference*
255-100-207	**Issue 1**	*Data Networking Products Multispeed Module Reference*
255-100-211	**Issue 1**	*Data Networking Products Special Modules Reference*
255-100-212	**Issue 1**	*Data Networking Products SYNC8 Module Reference*
255-100-213	**Issue 1**	*Data Networking Products Trunk Module Reference*
255-100-214	**Issue 1**	*Data Networking Products Transparent Synchronous Module Reference*
255-100-215	**Issue 1**	*Data Networking Products TY Module Reference*
255-100-216 ISS 2	**Issue 2**	*Data Networking Products X.25 and X.25P Module Reference*
255-100-217	**Issue 1**	*Data Networking Products X.75 Module Reference*
255-100-210	**Issue 5**	*Data Networking Products Messages Reference*
255-100-201	**Issue 4**	*Data Networking Products Terminology*

* Includes all of the following titles.

StarKeeper II NMS Customer Documentation

StarKeeper II NMS customer documents provide the necessary information to plan, install, manage, and monitor the BNS-2000 network. These documents are orderable from the AT&T CIC; see the inside front cover of this *System Description*.

***StarKeeper* II NMS Customer Documents**	
Number	**Title**
255-114-730	*StarKeeper II NMS Planning Guide*
255-114-731	*StarKeeper II NMS Core System Guide*
255-114-732	*StarKeeper II NMS Graphics System Guide*
255-114-022	*StarKeeper II NMS Proxy Agent Guide*

Marketing Documentation

Marketing documentation for BNS-2000 provides general descriptive information on a variety of specific products and services. These documents present a high-level view of the BNS-2000 product and service line. Marketing documentation is available from your AT&T representative.

Customer Assistance

AT&T offers a Hotline Technical Support Service for customers needing technical assistance in the administration, operation, maintenance, and problem analysis of BNS-2000 networks. The Hotline Technical Support Service can be obtained on a contract or Time and Materials basis. Time and Material billing can be established with a running or per-event Purchase Order.

See the *Node Reference* for more information, including what account and technical information you should have available when you call, and what hotline number you should use.

To establish an account, contact your AT&T Account Representative, or call the appropriate hotline number listed in the *Node Reference*.

Maintenance and Support Services

The following maintenance and support service agreements are available from AT&T:

- ***Remote Technical Support Service Agreement*** — The Remote Technical Support Service provides complete software and consultative support, including expert remote assistance and timely software updates. It is recommended if you perform your own hardware maintenance and maintain your own inventory of spare parts.

- ***Full System Support Service Agreement*** — The Full System Support Service provides software, hardware, and consultative support. It provides both remote and on-site expert assistance, timely software updates, and prompt replacement of defective parts. It is recommended if you do not have an extensively trained maintenance staff or maintain your own inventory of spare parts.

The features provided by each service are described in detail in the following sections.

Remote Technical Support Service Agreement

The *Remote Technical Support Service Agreement* is designed for customers who choose to perform their own maintenance on their BNS-2000 node. It includes the following remote technical services, which are provided by the Customer Assistance Center (CAC):

- ***Technical Consultation*** — Technical consultation includes providing information about equipment and release compatibilities and incompatibilities, giving telephone support to customers who are installing, operating, administering, or maintaining a product at a site. Technical consultation may also include support in understanding the product interfaces as they relate to a specific application, and explaining or clarifying product functionality.
- ***Problem Diagnosis and Cause Isolation*** — Troubleshooting activities isolate the cause of a problem and determine whether it is associated with software, hardware, or firmware. These activities may include analysis of system-generated reports, remote access to your system, the use of special diagnostic software, and the re-creation of the problem in the CAC test lab.
- ***Trouble Resolution*** — Once a problem has been diagnosed and its cause has been isolated, solutions are recommended. These may include database or data table changes, reinstallation procedures, hardware or software replacements or upgrades, and temporary workarounds in cases where the problem cannot be resolved immediately.
- ***General Consultation*** — General consultation involves nontechnical information, such as the estimated availability date of a maintenance release or a new generic, the identification numbers that correspond to product parts, or instructions for completing the requirements of administrative processes such as product and service ordering, or the repair, service, and return of defective equipment.
- ***Call Referral and Redirection*** — When calls for assistance or information that is not available from the CAC are received, the CAC will put you in contact with the responsible AT&T organization via a three-way call. If the request involves another vendor, you will be referred to that vendor's hotline. When appropriate, the CAC consultant will work with other AT&T or vendor support groups to resolve your problem.
- ***Problem Management*** — The CAC will manage the resolution of all requests for assistance. If necessary, the CAC may engage other AT&T support groups or other vendors' support groups for additional expert assistance on your behalf. In this case, the CAC will serve as the problem manager for these different support groups until the problem is resolved or until there is mutual agreement that the resolution belongs to another support group.

- ***Software Maintenance Updates*** — Software updates are available that contain changes made to correct or enhance your system's functionality or performance. *This service feature does not apply to older software generics.* Contact your AT&T sales representative for the current Data Networking Supported Software List.
- ***Cumulative Software Maintenance Updates*** — Periodically, you may receive software updates that contain all previously developed corrections and selected enhancements. *This service feature does not apply to older software generics.* Contact your AT&T sales representative for the current Data Networking Supported Software List.

The two standard coverage options available are shown in Table 8-1.

TABLE 7-1. Remote Technical Support Service Agreement Options

Option	Effective Hours
Basic	8:00 A.M. - 5 P.M., Monday-Friday, excluding holidays
Unlimited	Total coverage (all hours, all days)

NOTE: The following holidays are excluded for Basic Service: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, the day after Thanksgiving Day, and Christmas.

Full System Support Service Agreement

The *Full System Support Service Agreement* provides the most complete software, hardware, and consultative support, including both remote and on-site expert assistance, timely software updates, and prompt replacement of defective parts. It is designed for customers who do not choose to maintain an extensively trained maintenance staff or maintain their own spare parts inventory. It includes the following remote and on-site technical services:

- ***Technical Consultation*** — Provides help in the installation, operation, administration, or maintenance of your data networking system. Technical consultation also includes providing information about equipment and release compatibilities and incompatibilities, clarifying product functionality, and support in understanding product interfaces as they relate to a specific application.
- ***Problem Diagnosis and Cause Isolation*** — Troubleshooting activities isolate the cause of a problem and determine whether it is associated with software, hardware, or firmware. These activities may include analysis of system-generated reports, remote access to your system, the use of special diagnostic software, and the re-creation of the problem in the CAC test lab.
- ***Trouble Resolution*** — Once a problem has been diagnosed and its cause has been isolated, solutions are recommended. These may include database or data table changes, reinstallation procedures, hardware or software replacements or upgrades, and temporary workarounds in cases where the problem cannot be resolved immediately.

- ***General Consultation*** — General consultation involves nontechnical information, such as the estimated availability date of a maintenance release or a new generic, the identification numbers that correspond to product parts, or instructions for completing the requirements of administrative processes, such as product and service ordering, or the repair, service, and return of defective equipment.
- ***Call Referral and Redirection*** — When calls for assistance or information that is not available from the CAC are received, the CAC will put you in contact with the responsible AT&T organization via a three-way call. If the request involves another vendor, you will be referred to that vendor's hotline. When appropriate, the CAC consultant will work with other AT&T or vendor support groups to resolve your problem.
- ***Problem Management*** — The CAC will manage the resolution of all requests for assistance. If necessary, the CAC may engage other AT&T support groups or other vendors' support groups for additional expert assistance on your behalf. In this case, the CAC will serve as the problem manager for these different support groups until the problem is resolved or until there is mutual agreement that the resolution belongs to another support group.
- ***Software Maintenance Updates*** — Software updates are available that contain changes made to correct or enhance your system's functionality or performance. *This service feature does not apply to older software generics.* Contact your AT&T sales representative for the current Data Networking Supported Software List.
- ***Cumulative Software Maintenance Updates*** — Periodically, you may receive software updates that contain all previously developed corrections and selected enhancements. *This service feature does not apply to older software generics.* Contact your AT&T sales representative for the current Data Networking Supported Software List.
- ***Remedial Hardware Maintenance*** — In response to a hardware failure, an SSC or CSC Customer Engineer will perform tests, take measurements, make adjustments, and replace defective parts to return the system to its proper operating condition.
- ***Preventive Hardware Maintenance*** — Periodically, an AT&T Customer Engineer will perform tests, take measurements, make adjustments, and replace certain parts in order to minimize the possibility of a system failure. Preventive maintenance is performed on a mutually-agreed schedule.
- ***Resident On Site*** — This optional service feature provides a resident customer engineer at the customer's designated service location for the selected hours of coverage.
- ***Out-of-hours Remote Assistance*** — Remote technical support is available from the CAC for severity 1 and severity 2 assistance requests outside the hours covered by your service contract. Out-of-hours support is billed on a time and materials basis.
- ***Out-of-hours On-site Service*** — On-site service is available from your local SSC or CSC outside the hours covered by your service contract. Service is provided on an as-available basis at the prevailing local out-of-hours rate. For service requests initiated outside the normal coverage period, charges apply from the time of dispatch and include travel and living expenses for dispatches over 100 miles.

The three standard coverage options are shown in Table 8-2.

TABLE 7-2. Full System Support Service Agreement Options

Option	Effective Hours
Basic	8:00 A.M. - 5:00 P.M., Monday-Friday, excluding holidays
Extended	8:00 A.M. - 9:00 P.M., Monday-Saturday, excluding holidays
Unlimited	Total coverage (all hours, all days)

NOTE: The following holidays are excluded for Basic and Extended Service: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, the day after Thanksgiving Day, and Christmas.

Value-Added Services

Value-added services are available from AT&T for BNS-2000 and *StarKeeper* II NMS customers. Contact your AT&T Account Executive for ordering information and availability. Value-added services are available in the following categories:

- Database Transfer Services
- Start-up Services
- *StarKeeper* II NMS Tools.

Start-up Services

These services are designed to help customers get their systems operational as soon as possible with a minimum of work and planning. After a Start-up Service is scheduled, a technical representative from the Operations System Technical Center will come on-site to your location and install all operating system and application software, customize the system to your requirements, provide hands-on training for systems administration personnel, check the performance of system back-ups, and verify the entire installation.

In addition, the technical representative will demonstrate the features of the product and provide opportunities for your administrator to ask questions and learn more about the product.

Start-up Services are available for the following products:

- *StarKeeper* II NMS
- LCS60
- Network Access Control System.

Start-up Services can be ordered from AT&T Account Executives.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X